Received 9/30/2021 9:17:11 AM Commonwealth Court of Pennsylvania

Filed 9/30/2021 9:17:00 AM Commonwealth Court of Pennsylvania
310 MD 2021

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

SENATOR JAY COSTA, SENATOR ANTHONY H. WILLIAMS, SENATOR VINCENT J. HUGHES, SENATOR STEVEN J. SANTARSIERO and SENATE DEMOCRATIC CAUCUS, Petitioners, v. SENATOR JACOB CORMAN III, SENATE PRESIDENT PRO TEMPORE, SENATOR CRIS DUSH and SENATE SECRETARY-PARLIAMENTARIAN MEGAN MARTIN, Respondents.	:	No. 310 MD 2021

ANSWER TO APPLICATION FOR SPECIAL RELIEF BY RESPONDENTS SENATOR JACOB CORMAN III AND SENATOR CRIS DUSH

Petitioners' Application for Special Relief should be denied for several reasons. First, there is no party to this action against whom the Court can enter effective relief, since several indispensable parties are missing (which likewise deprives the Court of jurisdiction). Second, Petitioners lack standing to pursue their claims. Third and finally, Petitioners have failed to satisfy the elements necessary for injunctive relief. Accordingly, Respondents Senator Jacob Corman III and Senator Cris Dush urge the Court to deny the pending Application.

I. ARGUMENT

A. The proper parties are not before the Court.

Petitioners have not established a clear right to relief, *Com. ex rel. Corbett v. Snyder*, 977 A.2d 28, 43 (Pa. Cmwlth. 2009), because they have failed to name all indispensable parties to the Petition for Review (PFR), and consequently, any meaningful relief requested by the Application cannot be granted. To illustrate, in the Application, Petitioners ask the Court to extend the response deadline for the subpoena at issue and to also enjoin "Respondents and/or the Committee" from entering into a certain third-party contract. *See* Appl. ¶ 21. But both requests—on their face—request relief from the Intergovernmental Operations Committee, the non-party who issued the subpoena, *see* PFR, Ex. J, and the non-party who, according to the Petitioners' allegations, would enter into the speculated contract. *See* Appl. ¶ 6; PFR ¶ 110.

"A party is indispensable when his rights are so connected with the claims of the litigants that no decree can be made without impairing those rights." *Pilchesky v. Doherty*, 941 A.2d 95, 101 (Pa. Cmwlth. 2008). Applied here, the Committee is not, of course, a named

Respondent. Yet as set forth above, Petitioners seek relief that would impair the Committee's rights. This makes the Committee an indispensable party. This not only deprives the Court of the ability to grant special relief, but also deprives it of subject matter jurisdiction. *See Church of Lord Jesus Christ of Apostolic Faith, Inc. v. Shelton*, 740 A.2d 751, 755 (Pa. Cmwlth. 1999).

The Committee is not the only indispensable party that Petitioners failed to name. The Senate, the Acting Secretary of the Commonwealth, and the Auditor General are all also similarly vital parties who have not been named.

As to the Senate, Petitioners demand that this Court declare, as a matter of law, that the Senate as an institution lacks certain powers of inquiry. *See, e.g.*, PFR, Prayer for Relief ¶¶ (b), (d). Once again, like the Committee, Petitioners have failed to name the Senate as a Respondent, despite claims for relief that expressly seek an impairment of the Senate's institutional authority. Thus, the Senate is an indispensable party.

Further, despite the subpoena being issued to Acting Secretary of the Commonwealth Veronica Degraffenreid, Petitioners have failed to

name her as a party. This is also despite making various claims on her behalf (i.e., quashal), and despite seeking various declarations under, and interpretations of, the Election Code, *see, e.g.*, PFR Count III, the statutory scheme under which she has various duties. *See* 25 P.S. § 2621. Thus, the Acting Secretary is an indispensable party.

Finally, Count II of the PFR seemingly seeks various conclusions regarding the duties and powers of the Auditor General, *see* PFR ¶¶ 82-94, who is also not a party to the PFR. Moreover, the PFR appears to seek relief that would limit the Auditor General's powers in at least two ways: first, by seeking a declaration that only the Judiciary can determine "audits" under the Constitution and Election Code, *see* PFR Prayer for Relief ¶ (b); and second, by seeking a declaration that certain data is exempt from audit by most parties, seemingly including the Auditor General. *See* PFR Prayer for Relief ¶ (d). Thus, the Auditor General is an indispensable party.

Therefore, the Application fails on this ground alone.

B. Petitioners lack standing to pursue their claims.

Petitioners are also not entitled to relief because they lack the requisite legal interest—either as legislators, or as individual voters—

relative to any of their three claims and, thus, cannot establish their standing.

It is axiomatic that "[p]rior to judicial resolution of a dispute, an individual must as a threshold matter show that he has standing to bring the action." *Pittsburgh Palisades Park, LLC v. Com.*, 888 A.2d 655, 659 (Pa. 2005). To establish standing, the party must have an interest in the cause of action that is: (1) "substantial," so as to "surpass[] the common interest of all citizens in procuring obedience to the law[,]"; (2) "direct," which means that the "asserted violation and the harm complained of" are causally linked; and (3) "immediate," such that "the causal connection is not remote or speculative." *Phantom Fireworks Showrooms, LLC v. Wolf*, 198 A.3d 1205, 1215 (Pa. Cmwlth. 2018) (*en banc*).

1. Petitioners lack standing in their legislative capacities.

In terms of Petitioners' standing in their respective legislative capacities, because there is no "special category of standing for legislators[,]" legislators who bring an action in their official capacity must satisfy the same criteria as any other litigant. *Markham v. Wolf*, 136 A.3d 134, 140 (Pa. 2016). Bearing in mind that Petitioners'

membership in the General Assembly does not alter the standing analysis, Petitioners cannot satisfy the elements of standing with respect to any of their claims and, thus, are not entitled to relief.

With regard to Count I, which alleges that Respondents are seeking to hold a "*de facto* election contest" in violation of the Judiciary's exclusive jurisdiction over contested elections, *see* PFR ¶ 81, Petitioners' averments fall far short of meeting the requisite standard for standing. Specifically, even assuming *arguendo* a review of the materials enumerated in the subpoena could somehow constitute an "election contest"—which it cannot—it would affect the interests of the Judiciary, whose powers are allegedly going to be usurped, and/or the specific elected officials, whose election would purportedly become the subject of the contest. Petitioners, of course, are members of the Legislative Branch—not the Judiciary. As such, insofar as they seek relief in their legislative capacities, Petitioners have failed to explain how any of the interests unique to them, as legislators, would be affected—let alone impaired.

Nor do Petitioners allege that their election—or, in the case of the Senate Democratic Caucus, the election of any of its members—would

be the subject of the "*de facto* election contest." Accordingly, setting aside the absence of any factual allegation to support this assertion, Petitioners have failed to allege a concrete and particularized interest in the purportedly forthcoming "*de facto* election contest." In short, Petitioners' interest in forestalling the purported election contest is indistinguishable from "the common interest of all citizens in procuring obedience to the law[,]" *Phantom Fireworks*, 198 A.3d at 1215, and, thus, cannot confer standing. *Accord Fumo v. City of Philadelphia*, 972 A.2d 487, 501 (Pa. 2009) (holding legislators lack standing "in actions seeking redress for a general grievance about the correctness of governmental conduct").[1]

Turning to Count II, which alleges that the subpoenas invade the exclusive authority of both the Auditor General and the Secretary of the Commonwealth to conduct "audits," Petitioners similarly lack standing. Setting aside, once again, the untenable definition of "audit" on which this claim is predicated, insofar as the authority of either the Auditor General or the Secretary has been usurped or diminished, the injury is

[1] Although Petitioners' failure to satisfy the principal element of standing renders further discussion unnecessary, even if some generalized harm to Petitioners' legislative powers could be gleaned from their generalized allegation, given the remote nature of their claim, the injury is neither direct nor immediate.

to those respective offices—not Petitioners' legislative powers and responsibilities. As such, much like their first claim, Petitioners are seeking nothing more than "redress for a general grievance about the correctness of governmental conduct[,]" which is insufficient to confer standing on anyone. *See Fumo*, 972 A.2d at 501 (holding legislators, like all other litigants, lack standing in cases involving such generalized grievances)

Similarly, even assuming *arguendo* that compliance with the subpoena in question would violate the statutory provisions referenced in Count III, *see* 25 Pa.C.S. §§ 1101, *et seq.*, Petitioners' legislative interests would not be impacted. Specifically, that statutory scheme concerns the relationship between counties and the Pennsylvania Department of State; it does not touch or concern the legislative power. *Compare id.* at § 1103 ("This part applies to all counties."), *with id.* at § 1108 ("The [D]epartment [of State] shall administer this part."). As such, Petitioners have failed to allege *any* injury to the legislative power, let alone one that is "a discernible and palpable infringement on their authority as legislators" that would afford them standing. *Fumo*, 972 A.2d at 501.

2. Petitioners lack standing in their personal capacities.

Next, Petitioners also lack standing to maintain this action in their individual capacities. Assuming Petitioners seek to rely (in whole, or in part) on taxpayer standing in pursing this action as voters, under this narrow exception to the general rule of standing a taxpayer may be able to challenge a governmental action even without having a substantial, direct, and immediate interest if: (1) conduct would otherwise go unchallenged; (2) those directly and immediately affected by the complained-of matter are beneficially affected and not inclined to challenge the action; (3) judicial relief is appropriate; (4) redress through other channels is unavailable; and (5) no other persons are better situated to assert the claim. *See Stilp v. Com., Gen. Assembly*, 940 A.2d 1227, 1233 (Pa. 2007).

Applying *Stilp* to Count I, which alleges the subpoena is subterfuge for an unconstitutional "*de facto* election contest," Petitioners cannot satisfy any of the elements of taxpayer standing. First, given the perennial election-related litigation involving specific candidates—many of them commenced in this Court—it is unfathomable that not a single elected official (whose election would,

under Petitioners' theory, be jeopardized by a "*de facto* election contest") would elect to challenge an unconstitutional attempt to undo a duly certified election. Nor is it likely that such a usurpation of judicial authority would go unaddressed by the Judicial Branch. Indeed, where a legislative act has threatened the Judiciary's independence, the Supreme Court has not hesitated in the past to address such a violation *sua sponte*—in the absence of a case or controversy. *See In re 42 Pa.C.S. § 1703*, 394 A.2d 444, 446 (Pa. 1978) (relaying, in a published opinion in the form of a letter addressed to the General Assembly, that a statute violated the State Constitution as applied to the Judiciary).

Turning to the second requirement, as the PFR itself makes clear, those directly and immediately affected by an unconstitutional election contest—*i.e.*, the Judicial Branch and elected officials whose election would be in peril—would not be beneficially affected if the purported *de facto* contest proceeded, and would therefore be inclined to challenge the contest and eliminate the need for general taxpayer-initiated litigation. Along these same lines, the fifth factor is also not satisfied, since the Judiciary and/or an impacted official would be best situated to challenge any unauthorized de facto contest. As for the third

requirement, judicial relief is inappropriate for the multitude of reasons set forth herein. And finally, redress through other channels—namely, the branch to which Petitioners belong—is available, since Petitioners can take a variety of legislative actions to prevent the constitutional crisis that they allege.

Petitioners also fail to satisfy the minimum requirements of taxpayer standing for Count II. As it relates to the alleged encroachment on the Auditor General's exclusive powers, the Supreme Court has previously held that taxpayer standing does not exist to advance the Auditor General's interest because "the Auditor General, an elected official, is a far-better situated party to bring an action seeking a declaratory judgment that the Department of the Auditor General does, or does not, have the authority to audit the financial accounts of the General Assembly." *See Stilp*, 940 A.2d at 1234 (holding taxpayer standing did not exist to vindicate the Auditor General's power to audit the Legislative Branch). But even analyzed anew, none of the five requirements are satisfied, since (1) it strains credulity that a constitutional officer like the Auditor General would forgo a challenge to a genuine encroachment of his powers; (2) the Auditor General, based

on Petitioners' own allegations, would not be benefitted by the complained-of diminution of his authority; (3) judicial relief is inappropriate, as developed throughout this submission; (4) redress through the legislature is available; and (5) per *Stilp*, the Auditor General is better situated to assert the claim.

Similarly, to the extent Petitioners are seeking to vindicate the interests of the Secretary of the Commonwealth, taxpayer standing is inappropriate. In this regard, this Court need look no further than its own docket to be satisfied that the purported interference with the Secretary's powers will not go unchallenged and that she is better-positioned to advance such claims. Specifically, in a seven-count Petition for Review, captioned *Commonwealth of Pennsylvania, et al. v. Dush, et al.*, docket no. 322 M.D. 2021, the Secretary is seeking declaratory and injunctive relief that subsumes Petitioners' claims—at least as it pertains to the Secretary's power of administering elections.

Finally, with regard to Count III, as noted above, the duty of administering the voter registration statutory scheme is vested exclusively in the Department of State. *See* 25 Pa.C.S. § 1108. Indeed, Chapter 18 of the statute in question, aptly titled "Enforcement," *see id.*

at §§ 1801-1804, sets forth a specific enforcement mechanism, generally vesting the Department of State authority to take any action necessary to secure compliance with the statute, *see id.* at §§ 1803-1804, and delineating the respective powers of the Attorney General, *see id.* at § 1801, and District Attorneys, *see id.* at § 1802, in prosecutions for criminal violations. As this Court has explained, "where the General Assembly commits the enforcement of a regulatory statute to a government body or official, this precludes enforcement by private individuals." *Lerro ex rel. Lerro v. Upper Darby Twp.*, 798 A.2d 817, 822 (Pa. Cmwlth. 2002) (holding no private right of action exists for seeking enforcement of the State Dog Law, where that power is expressly vested in the Secretary of the Agriculture); *see also Quirk v. Schuylkill Cty. Mun. Auth.*, 422 A.2d 904, 905 (Pa. Cmwlth. 1980) (holding individual lacked standing to obtain injunctive relief to secure compliance with a statute because, under the relevant provisions, "when any violation of the [enactment] occurs, the Commonwealth is the only party authorized to enforce the requirements of [its provisions]"); *Elizabeth Twp. v. Power Maint. Corp.*, 417 A.2d 1285, 1289 (Pa. Cmwlth. 1980) (same).

Accordingly, Petitioners lack standing to seek enforcement of 25 Pa.C.S. §§ 1101, *et seq*.

Moreover, even if this Court were to overlook this settled precedent, the injury Petitioners allege—*i.e.*, access to their private information—is insufficient to confer standing. To begin, given that nearly all of the information in question can be accessed by the general public at any time, *see, e.g.*, 25 Pa.C.S. § 1207, the "harm" from allowing a coequal branch of government to review those materials available to all citizens is not only insubstantial, but it is nonexistent. Furthermore, to the extent the alleged injury arises out of the possibility that the Respondents—or someone connected to the Senate—may, at some point in the future, provide this information to a third-party contractor for review and analysis, that harm is both remote and speculative, since the vendor, as Petitioners acknowledge in their pleading, has not yet been identified.

In sum, Petitioners' interest in this action is not "substantial," so as to "surpass[] the common interest of all citizens in procuring obedience to the law." *Phantom Fireworks*, 198 A.3d at 1215. Rather, it is precisely the type of "action[] seeking redress for a general grievance

about the correctness of governmental conduct[,]" *Fumo*, 972 A.2d at 501, which is insufficient to establish standing for any litigant—legislative or otherwise.

C. Petitioners have not satisfied the factors necessary for injunctive relief.

Finally, even if the Application could survive the above challenges, it still fails because Petitioners have failed to satisfy the factors necessary for injunctive relief.

As to irreparable harm, Petitioners have posited nothing more than a series of speculative injuries. First, Petitioners speculate the Acting Secretary will respond to the subpoena on October 1. *See* Appl. ¶ 28. But given that the Acting Secretary has filed a petition in this Court seeking to quash the subpoena, *see Com. v. Dush*, No. 322 M.D. 2021, a response at all, let alone one by October 1, is highly unlikely. Second, Petitioners speculate that Respondents will soon enter into a contract with an unidentified vendor to release unknown information in an unidentified way. *See* Appl. ¶ 29. But even if such a contract is entered into, as of today, and for the foreseeable future (*see Com. v. Dush*), there will be nothing to give to this vendor. And critically, the notion that a private vendor cannot see election data is patently absurd,

since the Commonwealth, through the Department of State, is ***currently*** in a multi-year contract with a ***private*** vendor (from South Dakota) who has comprehensive access to election data. *See* BPro, Inc. Contract with Dep't of State, at 4 of 603 (Dec. 28, 2020) ("**THIS CONTRACT** is for the provision of **Statewide Uniform Registry of Electors (SURE) System**…") (attached as Exhibit A); *id.* at 353 of 603 (describing project); *id.* at 357 of 603 ("BPro's proposed solution for Pennsylvania is a complete replacement of the SURE system with BPro's TotalVote suite of products."); *id. at* 389 of 603 ("Our plan for Pennsylvania is to extract as much data as possible from the state repository and then fill in any missing pieces from each of your 67 county databases. Data that may only reside in county systems would include images, signatures, and transactional history."), *available at* https://patreasury.gov/transparency/e-library//ContractFiles/588822_DGS_4400023325_ContractFile.pdf.[2] There is no reason to believe or

[2] Additionally, Pennsylvania is a member state of the Electronic Registration Information Center (ERIC), which is a non-profit corporation "with the sole mission of assisting states to improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens." *See Electronic Registration Information Center*, https://www.ericstates.org, (last visited Sept. 28, 2021). ERIC advises that each member, like Pennsylvania, submits to ERIC "at a minimum its voter registration and motor vehicle licensee data. The data includes names, addresses, date-of-birth, last four digits of the social security number." *Id.*

suggest that any contract with a third party vendor to review this information as part of the Committee's investigation, would not contain the same types of protections against unlawful disclosure as would any contract entered into by the Department of State as it relates to this information.

As to clear right to relief, Petitioners lack standing, *see supra*, and thus have no likelihood of success. Further, the claims on their merits fail for a host of reasons. To begin, the Pennsylvania Constitution sets forth a foundational principle about our government: "The legislative power of this Commonwealth shall be vested in a General Assembly, which shall consist of a Senate and a House of Representatives." Pa. Const. art. II, § 1. The "legislative power" referenced in the Constitution, "in its most pristine form," is "the power 'to make, alter and repeal laws.'" *Blackwell v. Com., State Ethics Commn.*, 567 A.2d 630, 636 (Pa. 1989), *on reargument*, 589 A.2d 1094 (Pa. 1991). An "essential corollary" of this power to legislate is the "power to investigate." *Com. ex rel. Carcaci v. Brandamore*, 327 A.2d 1, 3 (Pa. 1974); *see also Lunderstadt v. Pa. H.R. Select Commn.*, 519 A.2d 408, 410 (Pa. 1986). The power to so inquire "extends to every proper subject

of legislative action." *Carcaci*, 327 A.2d at 3. And that power to investigate can be exercised by the legislature through, among other means, subpoenas. *See* Pa. Const. art. II § 11; 46 P.S. § 61; 18 Pa.C.S. § 5110; *see also Annenberg v. Roberts*, 2 A.2d 612, 616 (Pa. 1938); *Camiel v. Select Comm. on State Contract Practices of H.R.*, 324 A.2d 862, 865-66 (Pa. Cmwlth. 1974); *Examination of Reports of Insurance Companies*, 64 Pa. D. & C.2d 627, 631-32 (Office of Att'y Gen. 1973).

In this matter, all parts of the foregoing foundational principles are present. To begin, the Senate, through the Committee, is analyzing whether to make, alter, or repeal election laws. PFR ¶ 50. It is doing so through a factual investigation. PFR ¶ 54. That investigation is being conducted in part by subpoena. PFR, Ex. J. And the subject matter of the investigation—elections—is not only *arguably* within the Senate's power, but also *constitutionally committed* to the Senate's (and House's) purview in multiple sections. *See* Pa. Const. art VII, §§ 1, 2, 3, 4, 6, 9, 11, 13, 14.

Against the foregoing basic laws and facts, the central thesis of Petitioners' claims—that a committee of the Senate is attempting to do something unusual, unlawful, or impermissible—is flawed. In turn,

Petitioners are unlikely to succeed on the merits of their claims and have not shown a clear right to relief.

In particular, Count I is premised on the notion that a mere Senate committee investigation is somehow an impermissible election contest. Not so. Nothing about the Committee's attempt to investigate existing election laws or the need for new ones transforms the inquiry into a proceeding that will declare some candidate the winner of some election. Simply put, there is not an unlawful election contest at stake.

Next, Count II posits that "audits" can only be done by parties other than the Senate. But this flies in the face of settled principles about the General Assembly's constitutionally committed power to legislate, which carries with it the corollary power to investigate. *See supra.*

Finally, as to Count III, Petitioners posit that the Senate is somehow subject to various statutory provision and regulations, but Petitioners have not shown that whatever privacy concerns those statutes are designed to protect is not already accounted for in the normal operations of government. Indeed, the free sharing of public and "confidential" data among constituent parts of the Commonwealth, of

which the Senate is a part, is consistent with the dictates of the Administrative Code and guidance from the Pennsylvania Attorney General, and, frankly, ordinary agreements among Commonwealth agencies. *See* 71 P.S. § 182 (Admin Code § 502); *Examination of Reports of Insurance Companies*, 64 Pa. D. & C.2d 627, 631-32 (Office of Att'y Gen. 1973); *see also* Auditor General, *Performance Audit Report—Pennsylvania Department of State, Statewide Uniform Registry of Electors (SURE)*, at 130 (Dec. 2019) (describing non-disclosure agreement involving Department of State and Auditor General) (attached as Exhibit B), *available at* https://www.paauditor.gov/Media/Default/Reports/Department%20of%20State_SURE%20Audit%20Report%2012-19-19.pdf.[3] [4] In other words, the mere presence of

---

[3] 71 P.S. § 182 (Admin Code § 502):

> Whenever, in this act, power is vested in a department, board, or commission, to inspect, examine, secure data or information, or to procure assistance, from any other department, board, or commission, a duty is hereby imposed upon the department, board, or commission, upon which demand is made, to render such power effective.

[4] *Examination of Reports of Insurance Companies*, 64 Pa. D. & C.2d at 631-32 (internal citation removed):

> A duly constituted legislative committee should, of course, be given any record which is a public record or which is not otherwise prohibited by law, and you should, as we are certain you do, cooperate with such a committee so that it may appropriately carry on its legal functions. …. If, however, such a committee requests a report of examination which has not yet been finalized

confidential information is not an insurmountable barrier to access, as Petitioners posit in Count III.

As to the balance of injunction factors, Petitioners' request fares no better. Greater harm would not result from denying relief than from granting it: if the Court does nothing, none of the "harms" claimed by Petitioners will come to pass. This is so chiefly because the Acting Secretary has signaled she does not intend to respond, and absent a response, there is no data that can be revealed to anyone, let alone a private vendor in some purportedly injurious way. *See supra*. Moreover, Respondents have no intent to violate the rights of any Commonwealth citizen. Next, the relief requested is not reasonably suited to abate the offending activity, since the relief, even if entered, will not bind the Committee or the Acting Secretary, both of whom are non-parties but who are both necessary parties. *See supra*. Finally, the balance of factors (status quo and public interest) are neutral, since, again, Petitioners have not sought relief through viable claims or against

---

> and is, therefore, not public, we believe, and it is our opinion, that you should require a subpoena from such committee and specifically advise such committee of the confidential nature of such material so that it will not make it public to the detriment of the company involved. Once the subpoena has been properly issued and is otherwise legal and proper, you should obey it[.]

viable parties, so neither the status quo nor the public interest will be impacted.

II. CONCLUSION

Wherefore, the Court should deny the Application for Special Relief.

Respectfully submitted,

Dated: September 30, 2021

s/ Matthew H. Haverstick
Matthew H. Haverstick (No. 85072)
Joshua J. Voss (No. 306853)
Shohin H. Vance (No. 323551)
Samantha G. Zimmer (No. 325650)
KLEINBARD LLC
Three Logan Square
1717 Arch Street, 5th Floor
Philadelphia, PA 19103
Ph: (215) 568-2000
Fax: (215) 568-0140
Eml: mhaverstick@kleinbard.com
jvoss@kleinbard.com
svance@kleinbard.com
szimmer@kleinbard.com

Attorneys for Respondents Senator Jacob Corman III and Senator Cris Dush

Exhibit A

FULLY EXECUTED
Contract Number: 4400023325
Original Contract Effective Date: 12/28/2020
Valid From: 12/28/2020 To: 12/27/2024

All using Agencies of the Commonwealth, Participating Political Subdivision, Authorities, Private Colleges and Universities

Your SAP Vendor Number with us: 347081

Supplier Name/Address:
BPRO INC
102 E 6TH AVE
FORT PIERRE SD 57532-2270 US

Supplier Phone Number: 605-224-8114
Supplier Fax Number: 605-224-1665

Contract Name:
19_Statewide Uniform Reg of Electors Sys

Purchasing Agent
Name: Roadcap Sara
Phone: 717-425-5446
Fax: 717-783-2724

Please Deliver To:

To be determined at
the time of the Purchase Order
unless specified below.

Payment Terms
NET 30

Solicitation No.: Issuance Date:

Supplier Bid or Proposal No. (if applicable): Solicitation Submission Date:

This contract is comprised of: The above referenced Solicitation, the Supplier's Bid or Proposal, and any documents attached to this Contract or incorporated by reference.

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
1	Maintenance & Support	0.000	Month	0.00	1	0.00

Item Text
Maintenance, Support, and Hosting

Maintenance & Support
- Year 1 = $60,000
- Year 2 = $61,000
- Year 3 = $62,000
- Year 4 = $63,000

Hosting
- Year 1 & 2 = $25,000
- Year 3 & 4 = $27,500

Information:

Total Amount:
SEE LAST PAGE FOR TOTAL OF ALL ITEMS

Currency: USD

Supplier's Signature _____ Title _____

Printed Name _____ Date _____

FULLY EXECUTED
Contract Number: 4400023325
Original Contract Effective Date: 12/28/2020
Valid From: 12/28/2020 To: 12/27/2024

Supplier Name:
BPRO INC

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
2	Election Night Reporting	0.000	Each	0.00	1	0.00

Item Text
Optional Service on RFP Cost Matrix

3	Automated Testing	0.000	Each	0.00	1	0.00

Item Text
Optional Service on RFP Cost Matrix

4	Enhancements	0.000	Each	0.00	1	0.00

Item Text
Not a guarantee for work to be performed or payment of services. DOS will be charged for actual hours of work performed through approved Change Order.

5	Stress & Load Testing	8.000	Each	0.00	1	0.00

Item Text
Semi Annual Test

6	Initial License Fee	0.000	Each	0.00	1	0.00

7	Implementation Planning	0.000	Each	0.00	1	0.00

Item Text
Deliverable A.1 - Final Implementation Plan

8	Implementation of the Solution	0.000	Each	0.00	1	0.00

Item Text
Deliverables for:
- Requirements Package
- Configuration Confirmation Report for all agreed to environment reviewed and approved by DOS
- Detailed Solution and Interface Design Document and Interface Delivery Specification
- Fully Configured Solution and Interfaces reviewed and accepted by DOS
- Test Plan and Test Scenarios
- Final Implementation Report

9	Data Conversion & Validation	0.000	Each	0.00	1	0.00

Information:

Total Amount:
SEE LAST PAGE FOR TOTAL OF ALL ITEMS

Currency: USD

FULLY EXECUTED
Contract Number: 4400023325
Original Contract Effective Date: 12/28/2020
Valid From: 12/28/2020 To: 12/27/2024

Supplier Name:
BPRO INC

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
	Item Text Deliverable for: - Data Conversion & Validation Plan approved by DOS - Data Conversion Schedule - Final Conversion Test Results - Final Data Conversion Report					
10	Training	0.000	Each	0.00	1	0.00
	Item Text Deliverable for: - Finalized Training Plan - Training Documentation - County User Training Sessions(s) - DOS User Training Session(s)					
11	Exit from Hosting	0.000	Each	0.00	1	0.00
	Item Text Deliverable for: - Hosting Transition Plan - Test Plan - Test Results - Final Hosting Migration Results Report					
12	Outgoing Transition	0.000	Each	0.00	1	0.00
	Item Text Deliverable for: - Outgoing Transition Plan Reviewed and Accepted by DOS - Final Report Showing the Successful Completion of Turnover Activities					

General Requirements for all Items:

No further information for this Contract

Information:

Total Amount:
10,689,890.91

Currency: USD

Contract Number: 4400023325

CONTRACT
FOR
STATEWIDE UNIFORM REGISTRY OF ELECTORS (SURE) SYSTEM

THIS CONTRACT for the provision of **Statewide Uniform Registry of Electors (SURE) System** ("Contract") is entered into by and between the **Commonwealth of Pennsylvania,** acting through the **Department of State**, and **BPro, Inc. ("Contractor").**

WHEREAS, the Department of General Services (DGS) issued a Request For Proposals for the provision of **Statewide Uniform Registry of Electors (SURE) System** for the Commonwealth, RFP No. **6100044816** ("RFP"); and

WHEREAS, Contractor submitted a proposal in response to the RFP; and

WHEREAS, Contractor's proposal was selected for the Best and Final Offer ("BAFO") phase of the RFP process; and

WHEREAS, in response to the DGS BAFO request, Contractor submitted a BAFO Cost Submittal; and

WHEREAS, DGS determined that Contractor's proposal, as revised by its Final Negotiated Cost Submittal, was the most advantageous to the Commonwealth after taking into consideration all of the evaluation factors set forth in the RFP and selected Contractor for contract negotiations; and

WHEREAS, **Department of State** and Contractor have negotiated this Contract as their final and entire agreement in regard to providing **Statewide Uniform Registry of Electors (SURE) System** to the Commonwealth.

NOW THEREFORE, intending to be legally bound hereby, **Department of State** and Contractor agree as follows:

1. Contractor shall, in accordance with the terms and conditions of this Contract, provide **Statewide Uniform Registry of Electors (SURE) System** as more fully defined in the RFP, to the Commonwealth.

2. Contractor agrees to provide the **Statewide Uniform Registry of Electors (SURE) System** listed in its Final Negotiated Cost Submittal, which is attached hereto as Exhibit C and made a part hereof, at the prices listed for those items in Exhibit C.

3. The Contractor shall meet and maintain the commitments to small diverse businesses made in its Final BAFO Small Diverse Business and Small Business Submittal, which is attached hereto as Exhibit D and made a part of this Contract. The Contractor shall submit any proposed change to a small diverse business

commitment to the Department of General Services' Bureau of Diversity Inclusion and Small Business Opportunities ("BDISBO"), which will make a recommendation as to a course of action to the Agency's Contracting Officer. The Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Contracting Officer and BDISBO within 10 workdays at the end of each calendar quarter that the Contract is in effect.

4. This Contract is comprised of the following documents, which are listed in order of precedence in the event of a conflict between these documents:

a. The Contract document contained herein.

b. The negotiated Contract Terms and Conditions, which are attached hereto as Exhibit A and made part of this Contract.

c. The Final Negotiated Technical Proposal Documents and Clarifications, which is attached hereto as Exhibit B and, with any referenced Attachments, made part of this Contract.

d. The Contractor's Final Negotiated Cost Submittal which is attached hereto as Exhibit C and made a part hereof.

e. The Contractor's Final BAFO Small Diverse Business Participation Submittal, which is attached hereto as Exhibit D and made a part hereof.

f. The RFP, including all of the referenced Appendices and as revised by all Addenda issued thereto, which is attached hereto as Exhibit E and made a part hereof.

g. The Contractor's Technical Submittal, which is attached hereto as Exhibit F and made a part hereof.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the parties have signed this Contract below. Execution by the Commonwealth is described in the Contract Terms and Conditions.

Witness:

By: 
Vice President

Abbey Campea 12/11/2020
Printed Name/Date

CONTRACTOR:

By: 
President

Brandon Campea 12/11/2020
Printed Name/Date

46-0446113
Federal I.D. Number

COMMONWEALTH OF PENNSYLVANIA
Department of State

By: To be obtained electronically
Agency Head/Designee Date
Title

APPROVED AS TO FORM AND LEGALITY:

To be obtained electronically
Office of Chief Counsel Date

To be obtained electronically
Office of General Counsel Date

To be obtained electronically
Office of Attorney General Date

APPROVED:

To be obtained electronically

Comptroller Date

APPENDIX A
Current State

The Department of State (DOS) is responsible for the administration of approximately 8.5 million active and inactive voter registrations for the state of Pennsylvania. Voter registration is a joint state-county effort.

SURE Systems

As referenced throughout the document, "SURE Systems" includes the following applications: SURE Portal, Election and Campaign Finance System, Campaign Finance Online System, Election Night Returns, Public Portal (PA Voter Services), Online Civilian Absentee Application, Dynamic Import Process Interface, Kiosk Portal, Voter Registration, PennDOT and DOS IDs application, verification, and related processes, Lobby Disclosure Reporting and the SURE Phone System ("SURE Systems"). Below is a brief explanation of what each of these systems do and the technology that allows them to operate.

Platform and language	.NET/XML SQL Stored Procedures
Interdependent/peripheral applications impacted	SUREPortal – Administrative interface for many of the SURE functions SUREReports – Reporting interface for SURE data and processes OVR/OVRDrive/OVR WebAPI – electronic voter registration application submission ECF – Elections and Campaign Finance Administration ENR – Election Night Returns (voter history and poll books)
Integrated applications	SUREPortal – Administrative interface and voter query for both County and Agency user groups KOFAX (KTA) – eSignature image enhancement system for all electronic submissions of voter applications Campaign Finance/ECF – Election Administration Administrative interface Keystone Login – voter authentication for absentee ballot retrievals (UMOVA) and voter specific queries Web API – a secure public facing webservice to allow properly vetted entities by the Department (such as 3rd party registration drives) to submit voter registration applications (new or changes) on their behalf using Department-approved customized applications
High demand times/volumes	Just prior to voter registration deadlines and poll book generation the volumes increase
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election and associated voter registration deadline approaches.
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes

SURE (SURE SYSTEMS) System

APPENDIX A
Current State

The SURE SYSTEMS system is the voter registration system for the Commonwealth of Pennsylvania. This system grants election users in all 67 counties the ability to enter and process voter registration applications. The system is written in Microsoft VB.NET on Visual Studio 2005 and Visual Studio 2008 as a client server application. The application resides on multiple Windows Server 2012 servers with a Citrix Xen App rendering layer. An active/passive SQL Server 2012 cluster houses databases that drive the application's data store. A second active/passive SQL Server 2012 cluster houses SQL Server Reporting Services (SSRS) where the application generates various election-required reports. A third active/passive SQL Server 2012 cluster houses services that provide replication distribution to the SSRS cluster as well as to a SQL Server 2012 cluster located in the Department's server farm.

Each county office leverages Wyse Z90D7 thin client as the access point to the SURE SYSTEMS system. These devices are running a locked down version of Windows 7. The user utilizes the Citrix ICA client to connect to the SURE application servers by way of the Commonwealth to County Network (CCN). Connections to most of the counties are by way of T1 circuits. Each county has at least one Wyse Z90D7 thin client with a USB connected DVD burner. This allows the county to burn DVDs of exported report data. Counties also have USB connected Strobe 400 scanners which are used to take images of voter registration applications. Bar code readers are also connected to the Wyse Z90D7 thin client to allow users to scan various correspondences.

Each county election office contains one or more Kyocera 3920 DN/9350 DN printers. Some counties also have other county owned printers attached to the SURE environment for printing of reports, ID cards, and poll books. Printing is accomplished through the Citrix environment.

Each county also has a secure FTP site for exporting and retrieving data.

SURE Data Warehouse

The SURE Data Warehouse is located on one of the previously mentioned SQL Server 2012 clusters. SQL Server Analytical Services (SSAS) is leveraged to build various cubes of data, which will be used by the Department. Some SURE reports may also leverage this data.

SURE Portals

The SURE Portals are made up of a client/server and a web application. The client server application, also known as the Entity Portal, resides in county offices as well as in offices within the Department. The Entity Portal allows users to enter into and query the voter registry, administer information that is rendered on the web application, record and report on provisional ballots, submit voter registration statistics, and generate various statistical reports. The entity portal is built with Visual Studio 2005 as a Microsoft VB.NET Click Once application. Smart Client Software Factory and the Commonwealth's BSCoE enterprise blocks are leveraged as the underlying architecture. C# is also found in some remote areas of the code. The client communicates over the CCN to common web services that are found as the logic layer between

the client/server part of the application, the public web application, and the SQL Server 2005 database. The web services and databases are found in the Department's server farm.

The public web portal provides constituents with various pieces of information. Voters may query the Polling Place Locator to find directions and the location of their polling place. An election calendar, frequently asked questions, and news items are available for both county specific and state specific areas. The status of a provisional ballot can be found on this site. In addition, UOCAVA voters can access their approved absentee ballots for download and submission via mail. UOCAVA voters also have the ability to review status of their absentee ballot. The public web portal is built as a VB.NET ASP.NET application. The front facing portion of the application resides in the Commonwealth's Data Power House. Calls from the public site are routed to the common web services at the Department.

PA Voter Services (PAVS)

This web site was designed to support the needs of voters, election services and other associated election services. Voters can apply for absentee ballots, find voter application and/or registration status, polling place, Voter Hall of Fame, etc. Authenticated voters can also find county contact information, absentee ballot status, modify own voter record and report complaints.
Election services include Election Events, links, news, voting systems information and complaints.

Platform and language	.NET/XML SQL Stored Procedures
Interdependent/peripheral applications impacted	PAVS uses the same database (ELVS) as SUREPortal and SURE VR for both Voter and Election Services.
Integrated applications	Voter applications are captured and integrated into the current SURE VR system for application processing. Authentication is currently integrated with Keystone Login. Payment processing for Full Voter Export data is integrated with the Commonwealth Payeezy system. Self-service account management is performed through the Keystone Login portal.
High demand times/volumes	Increase just prior to voter registration deadlines.
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election voter registration deadline approaches
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes

PA Online Absentee Application

This web site was designed to support the needs of civilian absentee voters and streamline the processing of these applications by the county within the SURE VR system. Until recently, voters were required to download (or obtain) the form, fill it out and mail the PA Absentee Ballot Application, to the corresponding county election office. The form is located on the PAVS website. Civilian voters wishing to apply to vote absentee, can now apply online by providing the required

and optional information, as in the paper form, and submit their application electronically. The online application will be automatically assigned to the voter's county (as specified on the application) within the SURE VR application batches. Currently, the online absentee ballot application is limited to those civilian voters with a valid PA Driver's License.

Platform and language	.NET SQL Stored Procedures
Interdependent/peripheral applications impacted	Online Absentee Ballot Application is modelled after OVR Drive in UI design and processing. It utilizes the same data elements as its paper form predecessor, leverages integration points, eSignature services (KOFAX KTA), basic workflows, etc. of OVR Drive. The approval process for the applications leverage existing processes and features used by the county in SURE VR.
Integrated applications	Voter absentee ballot applications are captured and integrated into the current SURE VR system for application processing.
High demand times/volumes	Civilian absentee ballot application deadlines from the Election Calendar.
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election voter absentee ballot deadline approaches
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes, but minimal

PA Online Voter Registration (Web API)

This web service was designed to support on line voter registration efforts by NVRA (National Voter Registration Act) organizations and other third party registration drive organizations that support development of their own application yet would provide data exchange via web-based API for the Department the necessary tracking for monitoring and management of participating organizations and the respective voter applications. Utilization of the web service starts with a registration and approval process (BEST).

Platform and language	.NET SQL Stored Procedures
Interdependent/peripheral applications impacted	OVR WebAPI is modelled after the current OVR website in utilizing the same data elements, integration points, eSignature services (KOFAX KTA), basic workflows, etc. The registration process uses a feature within SUREPortal for approvals for the various levels of access into the STAGING and PROD environments.
Integrated applications	Voter applications are captured and integrated into the current SURE VR system for application processing. Web API utilization metrics are captured and reported within SUREPortal. Self-service account management is performed through the OVR WebAPI portal with internal account approvals being managed within SUREPortal.

APPENDIX A
Current State

High demand times/volumes	Increase just prior to voter registration deadlines.
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election voter registration deadline approaches
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes

PA Online Voter Registration Drive

This site was designed to support on line voter registration drives for organizations that could not financially support development of their own application yet would provide the Department the necessary tracking for monitoring and management of participating organizations and the respective voter applications. Utilization of the website starts with a registration and approval process (BEST).

Platform and language	.NET SQL Stored Procedures
Interdependent/peripheral applications impacted	OVR Drive is modelled after both OVR and OVR WebAPI in utilizing the same data elements, integration points, eSignature services (KOFAX KTA), basic workflows, etc. The registration process uses a feature within SUREPortal for approvals for the various levels of access into the STAGING and PROD environments.
Integrated applications	Voter applications are captured and integrated into the current SURE VR system for application processing. OVR Drive utilization metrics are captured and reported within SUREPortal. Self-service account management is performed through PALogin services with internal account approvals being managed within SUREPortal.
High demand times/volumes	Currently awaiting registrations and promotions.
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election voter registration deadline approaches
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes, but minimal

eSignature Service

One of the key elements in voter registration applications is the ability of the perspective voter to show his/her identity for application processing and later processes such as poll books. The Commonwealth has standardized on several methods of the voter supplying his/her identification. The most reliable method has and continues to be the PennDOT Driver's License (PADL). With the voter providing a valid PADL, the Department has developed an interface (and associated agreements) with the Pennsylvania Department of Transportation (owner of the

PADL product) to allow standard/structured requests via a secure webservice to validate the PADL product and return a copy of the applicant's signature on the PADL product. This webservice provides validation of the applicant's identification and an associated digital signature that is attached to the voter registration application and eventually to the voter record (and subsequently the appropriate poll book). The proposed system must utilize this webservice for identification validation and eSignature retrieval on all interfaces for voter registration application submissions.

HAVA Interface

Various requirements are placed on the processing of voter registration and absentee ballot applications. One of those requirements is verification of an applicant's driver's license number (DL), photo ID number, or last four digits of their social security number (SSN) for new registrants. The HAVA Interface is the mechanism that accomplishes this process. Voter registration and absentee ballot transactions that are required to be verified are placed into a SQL Server 2005 database where a Biztalk 2006 application utilizes the SQL Adapter to pick up these transactions. The Biztalk application processes these transactions and passes them on to the MQ Series Adapter where the Department's MQSeries server at the Enterprise Data Center sends them to PennDOT. PennDOT's MQSeries system then either processes the DL transactions or sends them on to the American Association of Motor Vehicle Administrators (AAMVA) for SSN verification. Validation responses are sent back through the interface and logged back into SURE where the user posts the transactions appropriately. This system is used to meet Voter ID requirements for both voter registration and absentee ballots.

SURE Phone System

The Department is required to provide voters with the status of Provisional Ballots that were cast in an election. The SURE Entity Portal is the mechanism where most county election offices data enter the status. The SURE Public Portal allows voters to query and visualize the status of their vote using the Twilio application. The SURE Phone System allows voters to query and hear the status of their vote.

Platform and language	Twilio .NET/XML
Interdependent/peripheral applications impacted	SUREPortal
Integrated applications	SUREPortal Database
High demand times/volumes	Minor until Election day
Black-out periods for maintenance	It is anticipated higher volumes as the Primary/General election approaches
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes

APPENDIX A
Current State

Lobbying Disclosure Registration and Reporting System

The Department is required to provide a system in which lobbyists are required to register and provide details of the organizations for which they are working. The system is web based and provides interfaces for lobbyists to enter quarterly reports and for the public to search the database. Records are entered into a web application hosted in IIS 7 and stored in a SQL Server 2012 database. The Lobbying Disclosure Registration and Reporting System was developed using Visual Studio 2013 and is hosted in the Commonwealth's Data Center. Registrations and quarterly expense reports can now be filed and reviewed online 24 hours a day, seven days week. The management of the application by Commonwealth users is completed within the same interface as non-Commonwealth users.

Platform and language	.NET SQL Stored Procedures
Interdependent/peripheral applications impacted	Minimal sharing of data with the ECF database.
Integrated applications	Authentication is performed via Keystone Login for non-Commonwealth users, CWOPA AD for Commonwealth users. Electronic payments utilize the Commonwealth's PAYEEZY service for credit card payments.
High demand times/volumes	Lobbying firms input data for registration and reporting compliance directly to the website. Most activity is performed around the quarterly deadlines. There are many public users that query the database, especially around the quarterly deadline timeframes (~1000s per day).
Black-out periods for maintenance	Quarterly reporting deadlines, defined by the Election calendar. Quarterly Expense Report Due Dates: 1st Quarter January 1-March 31 Report Due April 30th 2nd Quarter April 1-June 30 Report Due July 30th 3rd Quarter July 1-September 30 Report Due October 30th 4th Quarter October 1-December 31 Report Due January 30th
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes, but minimal

Elections and Campaign Finance System (ECF)

The Elections and Campaign Finance System provides the Bureau of Elections and Notaries and the Bureau of Campaign Finance and Civic Engagement a system to manage campaign finance filings and election results. This system has an interface for the counties that utilize it to enter elections results and to certify elections. This system is hosted in the Commonwealth's Data Center, leveraging a SQL Server 2012 cluster.

Campaign Finance Online System

APPENDIX A
Current State

Campaign Finance System provides for online filing and searching of campaign contributions. Candidates for statewide, legislative and judicial offices and political committees are able to upload their filings as a text file, use an online from to create their filing or submit them to the Bureau of Campaign Finance and Civic Engagement to have them uploaded into the system. This system is hosted in the Commonwealth's Data Center, leveraging a SQL Server 2012 cluster. Campaign Finance reports can now be filed and reviewed online 24 hours a day, seven days a week.

Platform and language	.NET SQL Stored Procedures
Interdependent/peripheral applications impacted	ECF which controls the parameters by which reporting periods are measured (aka election cycle). Petition Filing and the Candidate Database control the list of candidates required to report.
Integrated applications	ECF and Petition Filing/Candidate integrate at the backend/database level via background processes. Authentication is performed via PALogin (near future Keystone Login) for non-Commonwealth users, CWOPA AD for Commonwealth users.
High demand times/volumes	Depending on the election cycle and the number of candidates currently running for offices. Offices and candidates vary within in Municipal, Gubernatorial and Presidential elections, but usually hovering in the several hundred. There are many public users that query the database, especially around the quarterly deadline timeframes (~1000s per day).
Black-out periods for maintenance	Quarterly reporting deadlines, defined by the Election calendar.
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes, but minimal

Campaign Finance Third-Party Transmittal

As a part of the Campaign Finance submission and reporting requirements, the current system allows for sending uploaded CF reports to a third-party vendor for data entry. The system will allow this assuming that the candidate status is approved, and the candidate has the CF-Cycles populated. The system uses unique barcodes to track the CF Report and allows electronic upload or scanning of reports by the Department. The uploaded reports are then assigned to a batch. From this collection/batch, the reports can be electronically sent to vendor, who currently is contracted for this data entry, for further processing. Once the vendor inputs/files the report information into the CFOnline module, the reports are then earmarked for the Department for final upload/publishing on the CFOnline website.

Petition System

APPENDIX A
Current State

The Petition system automates the process of candidates filing petitions to run for state-level offices. Petitions are received by the Bureau of Elections and Notaries staff and scanned into a SQL 2012 database. The system utilizes OCR technology to identify the required information on each line of the petitions. The signatures are then tallied to meet the various requirements for the appropriate office. The technologies utilized for this system include ImagXpress OCR software, SQL Server 2012, IIS 7 and it was developed in Visual Studio 2012. Petition filer information is also shared with other areas like campaign finance.

PA Portal Locator
This website was designed for specific reporting/data exports to election-based geographies relating to election polling places accessible to the general public.

Former website was GetCityList. Returns the list of cities that are within the boundaries of a single specified county.

- GetCountyList Returns the Returns the list of counties from the database of the SURE Portal.
- GetHouseNumbers Returns a list of house numbers that are valid for the specified street, city and county. This returned list is located in the DataSet supplied by referend.
- GetPollingPlaceForAddressAJAX Returns Polling Place Information for a given address query that is sent to the function.
- GetStreetList Returns a list of streets given a specific county and city name. The returned lists are contained in the dataset that is sent along.

Platform and language	.NET/XML SQL Stored Procedures
Interdependent/peripheral applications impacted	This reporting website extracts its information from SUREPortal database.
Integrated applications	None
High demand times/volumes	Unknown
Black-out periods for maintenance	Higher volumes are expected during high seasons of canvassing.
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Yes, but minimal

Dynamic Import Process Interface
The Dynamic Import Process Interface is used by County Boards of Election to bulk process voter registration forms during high volume periods. The process pushes application data from public facing sites to the County Boards of Elections for processing.

Voter Information Project Interface
As an integral partnership of providing transparency and accessibility to voters in Pennsylvania, the Department works with the Voter Information Project (VIP) to provide polling place

information from the SURE system (polling place data is managed and updated by the counties) as an extract and uploaded to the VIP website. The data extracted follows the VIP 5.1 Specification, which makes data interoperable across platforms and applications, and ultimately more easily disseminated to voters. The delivery method of the XML based information involves a configurable scheduler for recurring updates to the VIP website. The information is available through websites, like gettothepolls.com, and other tools available from www.votinginfoproject.com.

Electronic Registration Information Center (ERIC) Interface

List maintenance is the process by which the Department uses various sources of information to update and maintain voter records, their information and status. One of the key agreements that the Department has engaged with is the non-profit corporation governed by a board made up by member states, ERIC. Their mission is to help state and local election officials improve the accuracy of their voter rolls, register more eligible citizens to vote, reduce costs, and improve the voting process. Through its membership agreements, ERIC outlines the various reporting requirements of the member states, member states' responsibilities in using and processing ERIC reports/data for major list maintenance activities and the results of each. The proposed system must comply with the Department's current ERIC membership agreement and its deliverables.

PA Campaign Finance (CF) Export

The Department of state generates 5 campaign finance .txt files through system request, which is then uploaded to a public facing SharePoint site hosted by Pennsylvania Interactive (PAI). The site address is www.dos.pa.gov. The CF export files are manually updated by program staff. The five (5) .txt files are: 1) Contributions; 2) Debts; 3) Expenses; 4) Filers; and 5) Receipts. Together, the files illustrate current or historical candidate or committee reporting. Additionally, a readme file is provided for export users to understand the data contained within.

DOH Interface

The Department of Health interface is utilized by the SURE systems to retrieve a list of death certificates that have been issued to purge those names from the active voter list. This process utilizes FTP to transport the data between the two departments' systems. There is also a separate import process related to this interface.

PennDOT Interface

The Department of State interfaces with the Department of Transportation to receive voter registrations via the MotorVoter process. This process utilizes FTP to transport initial and change application data between the two departments' systems. There is a separate import process related to this interface.

Kiosk Portal

The Kiosk Portal is a limited access interface to the SURE system which counties can use to have citizens register electronically in the Bureau of Elections offices. It's also used by public users for

voter searches. This is built on the SURE Portal platform. It's used by Commonwealth, County Boards of Elections, and public users. This interface is also used by the Commonwealth court in areas of candidate and/or voter litigation involving voter information.

Election Night Returns (ENR) System

The Election Night Returns system provides the counties with a means to upload their returns for state-wide races to the Department of State. The Department of State then compiles that data and presents the state-wide and county level results on the election night returns website for public consumption. This application is built using the .Net Framework and is hosted on IIS 7 and utilizes a MS SQL 2012 database. Through recent efforts, the Department has developed a standard data format for the upload file. The XML format is also a standard by which voting system vendors must comply with. The application also provides a dashboard for monitoring county reporting progress during election night. The ENR application is a Click ONCE DB application. The ENR website utilizes .NET and has a reporting component which includes a Reporting Center for reports and an RSS Feed of the results to the general public to subscribe to. In addition to the reporting website and dashboard, the ENR Ballot Data Entry application allows a secure manual entry of ENR results for the counties if the electronic upload is not possible. This application is available only to the Department assigned staff.

Platform and language	.NET SQL Stored Procedures XML
Interdependent/peripheral applications impacted	Just the integration between the modules. Counties use the data for election certification (precinct and county). After counties have certified their results, the ENR website is manually updated by the Bureau of Elections and Notaries. ENR is primarily a reporting dashboard.
Integrated applications	Some modules authenticate with the CWOPA, MUSER and USER domains (ENR Dashboard and ENR Ballot Data Entry), while the ENR website does not integrate with other modules.
High demand times/volumes	Highest volumes from the general public are during election day (primary and general) and the days that follow. For the 2016 Presidential election, 40.4m hits on the ENR website. ENR Dashboard would have < 200 users.
Black-out periods for maintenance	Blackout periods are usually from Voter Registration Deadline through Election day (Primary and General) … ~ 30 days per election.
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Adequate, especially on the Reporting website

County Extranet

APPENDIX A
Current State

The County Extranet is a central location for the Department of State to interact with the county users. This tool will allow the Department to share information with the counties as well as provide an easy to use repository of that information.

Platform and language	SharePoint Site
Interdependent/peripheral applications impacted	The County Extranet has pointers/links to the other SURE and CF applications that are applicable to the county. SURE VR Exports are available only from this website/document library.
Integrated applications	SURE VR Exports are available only from this website/document library. Authentication is performed via Keystone Login for non-Commonwealth users, CWOPA AD for Commonwealth users.
High demand times/volumes	Users from the 67 counties comprise the bulk of the demand, especially around Voter Registration and Election deadlines and reports. Typical demand would be < 150 users.
Black-out periods for maintenance	Voter Registration and Election events (poll books), deadlines (VR deadline) and reports (VR certification, annual report).
Environments	Development, Staging, Production, Disaster Recover (DR)
Existing System Documentation	Adequate, especially on the Reporting website

APPENDIX B
Project References

Name of Client & Project Title	[Client – Project Title]	
Contract Value	[approximate contract value]	
Nature and Scope of Project:	Describe the project in sufficient detail to explain it is similar to the Commonwealth's project. How does this project compare in size, scope, complexity and/or duration? What is it specifically about this project that makes it a good representative project of the vendor's work?	
Project Duration:	**Start Date Year: [**YEAR]	**End Date Year:** [YEAR or on-going]
Nature of the Client:	[Description of client and organizational unit that project was managed by.]	
Nature of Client Audience:	[Description of project users and/or client/customer audience.]	
Number of Users:	[Number of business users assigned to the project]	
Data Migration:	[explain whether data migration was involved, duration, and general scope of migration]	
# & Composition of Vendor Employees & Consultants Assigned:	Vendor Project Manager/Key Consultant on Project Team: [Describe start-up, peak and ongoing level of vendor's efforts.]	
Client Contact Information:	[Provide the name, title, address and telephone number of at least two references or contact persons that the Commonwealth can contact to inquire about the vendor's performance and indicate the role these individuals had in relation to the assignment or project. The references/contact persons should be individuals who were key stakeholders or project leaders and who can validate the vendor's role and responsibilities and who can comment on the quality of the vendor's performance. (**Minimum 3 contacts required.**)] **Reference Contacts:** Name: Title: Department: Full Address: Telephone: E-mail: Relation/Role to Project: Name: Title: Department: Full Address: Telephone: E-mail: Relation/Role to Project: Name: Title: Department: Full Address: Telephone: E-mail:	

APPENDIX B
Project References

	Relation/Role to Project:

APPENDIX C

Glossary of Terms

1	API	Application Programming Interface is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.
2	Commonwealth	The Commonwealth of Pennsylvania
3	DOS	The Pennsylvania Department of State
4	Department	Refers to the Pennsylvania Department of State.
5	NVRA	National Voting Rights Act of 1993.
6	ERIC	The Electronic Registration Information Center is a non-profit organization with the sole mission of assisting states to improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens.
7	RFP	Request for Proposal - All documents, including those either attached or incorporated by reference, utilized for soliciting proposals.
8	Offeror	The person/entity that is submitting the proposal for this RFP.
9	Subcontractor	An individual, business, university, governmental entity, or nonprofit organization contracting to perform part, or all, of another entity's contract.
10	Small Business	A business in the United States which is independently owned, is not dominant in its field of operation, employs no more than 100 full-time or full-time equivalent employees, and earns less than $38,500,000 in gross annual revenues.
11	Small Diverse Business	A Department of General Services-certified minority-owned business, woman-owned business, service-disabled veteran-owned business or veteran-owned business, or United States Small Business Administration-certified 8(a) small disadvantaged business concern, that qualifies as a small business.
12	Election Infrastructure Information (EII, or EI Information)	Information or data of any type, that describes, discusses or contains details concerning Election Infrastructure.
13	Election Infrastructure (EI)	Includes but is not limited to the following items: voter registration databases and associated information technology (IT) systems; IT infrastructure and systems used to manage elections (such as the counting, auditing and displaying of election results, post-election reporting to certify and validate results); any non-public data included in any of the above; Electronic Voting Systems, as defined in the Pennsylvania Election Code, section 1101-A (25 P.S. § 3031.1), and related equipment; storage facilities for election and Electronic Voting Systems; information on polling places that could create vulnerabilities; all cyber security factors relating to the above, and any other information that could create risk or harm for the electoral process.
14	Critical Infrastructure	The physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety.
15	Multijurisdictional Implementation	Of or pertaining to more than one jurisdiction. Regarding this RFP, multijurisdictional refers to implementing a solution that crossed multiple

		jurisdictions. (e.g. a top-down solution that serviced both state, county, or local jurisdictions)

APPENDIX D

PERSONNEL EXPERIENCE BY KEY POSITION

TION st one row for identified as in V(H) of the ell as any sitions you've ntegral to the ated in your osal.)	PERSONNEL NAME (Identify by first/last name the person who will fulfill this position.)	Personnel Location (Identify the location and facility of the named person who will fulfill this position)	COMMITMENT (Provide the percentage of this person's time to be committed to the proposed project.)	# YEARS PRIOR EXPERIENCE IN POSITION (List the number of years this person has acted in the same role on prior projects similar in nature to the proposed project. This should not include academic experience).	OTHER RELEVANT EXPERIENCE (Provide a brief narrative of other experience this person has had that may be relevant to his/her role in the proposed project.)	EDUCATION (List all postsecondary degrees completed for this person.)	C PROF QUALI (List ar and/o membersh that may p

APPENDIX D

PERSONNEL EXPERIENCE BY KEY POSITION

APPENDIX G
IT Contract Terms and Conditions

1. DEFINITIONS.

(a) Agency. The department, board, commission or other agency of the Commonwealth of Pennsylvania listed as the Purchasing Agency. If a COSTARS entity or external procurement activity has issued an order against this Contract, that entity shall also be identified as "Agency."

(b) Commonwealth. The Commonwealth of Pennsylvania.

(c) Contract. The integrated documents as defined in **Section 11, Order of Precedence**.

(d) Contracting Officer. The person authorized to administer this Contract for the Commonwealth and to make written determinations with respect to the Contract.

(e) Data. Any recorded information, regardless of the form, the media on which it is recorded or the method of recording.

(f) Days. Calendar days, unless specifically indicated otherwise.

(g) Developed Works. All of the fully or partially complete property, whether tangible or intangible prepared by the Contractor for ownership by the Commonwealth in fulfillment of the requirements of this Contract, including but not limited to: documents; sketches; drawings; designs; works; papers; files; reports; computer programs; documentation; data; records; software; samples; literary works and other works of authorship. Developed Works include all material necessary to exercise all attributes of ownership or of the license granted in **Section 46, Ownership of Developed Works**.

(h) Documentation. All materials required to support and convey information about the Services or Supplies required by this Contract, including, but not limited to: written reports and analyses; diagrams maps, logical and physical designs; system designs; computer programs; flow charts; and disks and/or other machine-readable storage media.

(i) Expiration Date. The last valid date of the Contract, as indicated in the Contract documents to which these IT Contract Terms and Conditions are attached.

(j) Purchase Order. Written authorization for Contractor to proceed to furnish Supplies or Services.

(k) Proposal. Contractor's response to a Solicitation issued by the Issuing Agency, as accepted by the Commonwealth.

(l) Services. All Contractor activity necessary to satisfy the Contract.

(m) Software. A collection of one or more programs, databases or microprograms fixed in any tangible medium of expression that comprises a sequence of instructions (source code) to carry out a process in, or convertible into, a form executable by an electronic computer (object code).

(n) Solicitation. A document issued by the Commonwealth to procure Services or Supplies, e.g., Request for Proposal; Request for Quotation; Supplier Pricing Request; or Invitation for Bid, including all attachments and addenda thereto.

(o) Supplies. All tangible and intangible property including, but not limited to, materials and equipment provided by the Contractor to satisfy the Contract.

2. TERM OF CONTRACT.

(a) Term. The term of the Contract shall commence on the Effective Date and shall end on the Expiration Date identified in the Contract, subject to the other provisions of the Contract.

(b) Effective Date. The Effective Date shall be one of the following:

- the date the Contract has been fully executed by the Contractor and all approvals required by Commonwealth contracting procedures have been obtained; or
- the date stated in the Contract, whichever is later.

3. COMMENCEMENT OF PERFORMANCE.

(a) General. The Contractor shall not commence performance and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until both of the following have occurred:

- the Effective Date has occurred; and
- the Contractor has received a Purchase Order or other written notice to proceed signed by the Contracting Officer.

(b) Prohibition Prior to Effective Date. No Commonwealth employee has the authority to verbally direct the commencement of any Service or delivery of any Supply under this Contract prior to the date performance may commence. The Contractor hereby waives any claim or cause of action for any Service performed or Supply delivered prior to the date performance may commence.

4. EXTENSION OF CONTRACT TERM.

The Commonwealth reserves the right, upon notice to the Contractor, to extend the term of the Contract for up to ~~three (3)~~six (6) **months** upon the same terms and conditions.

5. ELECTRONIC SIGNATURES.

(a) The Contract and/or Purchase Orders may be electronically signed by the Commonwealth.

- *Contract*. "Fully Executed" at the top of the first page of the Contract output indicates that the signatures of all the individuals required to bind the Commonwealth to the terms of the Contract have been obtained. If the Contract output form does not have "Fully Executed" at the top of the first page, the Contract has not been fully executed.

- *Purchase Orders*. The electronically-printed name of the Purchasing Agent on the Purchase Order indicates that all approvals required by Commonwealth contracting procedures have been obtained.

(b) The Commonwealth and the Contractor specifically agree as follows:

- *Written signature not required.* No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

- *Validity; admissibility*. The parties agree that no writing shall be required in order to make the Contract or Purchase Order legally binding, notwithstanding contrary requirements in any law or regulation. The parties hereby agree not to contest the validity or enforceability of the Contract executed electronically, or acknowledgement issued electronically, under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements be in writing and signed by the party bound thereby. Any genuine Contract or acknowledgement executed or issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of a genuine Contract or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or acknowledgement were not in writing or signed by the parties. A Contract or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(c) Verification. Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

6. PURCHASE ORDERS.

(a) Purchase Orders. The Commonwealth may issue Purchase Orders against the Contract or issue a Purchase Order as the Contract. These Purchase Orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to, and including, the Expiration Date of the Contract are acceptable and must be performed in accordance with the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

(b) Electronic transmission. Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a Purchase Order shall require acknowledgement of receipt of the transmission by the Contractor.

(c) Receipt. Receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of a Purchase Order.

(d) Received next business day. Purchase Orders received by the Contractor after 4 p.m. will be considered received the following business day.

(e) Commonwealth Purchasing Card. Purchase Orders under $10,000 in total amount may also be made in person or by telephone using a Commonwealth Purchasing Card. When an order is placed by telephone, the Commonwealth agency shall provide the agency name, employee name, credit card number and expiration date of the card. The Contractor agrees to accept payment through the use of a Commonwealth Purchasing card.

7. CONTRACT SCOPE.

The Contractor agrees to furnish the requested Services and Supplies to the Commonwealth as such Services and Supplies are defined in this Contract.

8. ACCESS TO COMMONWEALTH FACILITIES.

If the Contractor must perform work at a Commonwealth facility outside of the daily operational hours set forth by the Commonwealth, it must make arrangements with the Commonwealth to assure access to the facility and equipment. No additional payment will be made on the basis of lack of access.

9. NON-EXCLUSIVE CONTRACT.

The Commonwealth reserves the right to purchase Services and Supplies within the scope of this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

10. INFORMATION TECHNOLOGY POLICIES.

(a) General. The Contractor shall comply with the IT standards and policies issued by the Governor's Office of Administration, Office for Information Technology (located at https://www.oa.pa.gov/Policies/Pages/itp.aspx), including the accessibility standards set out in IT Policy ACC001, Accessibility Policy. The Contractor shall ensure that Services and Supplies procured under the Contract comply with the applicable standards. In the event such standards change during the Contractor's performance, and the Commonwealth requests that the Contractor comply with the changed standard, then any incremental costs incurred by the Contractor to comply with such changes shall be paid for pursuant to a change order to the Contract.

(b) Waiver. The Contractor may request a waiver from an Information Technology Policy (ITP) by providing detailed written justification as to why the ITP cannot be met. The Commonwealth may waive the ITP in whole, in part or conditionally, or require that the Contractor provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

11. ORDER OF PRECEDENCE.

If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(a) The Contract document containing the parties' signatures;

(b) The IT Contract Terms and Conditions;

(c) The Request for Proposal; and

(d) The Contractor's Proposal.

12. CONTRACT INTEGRATION.

(a) Final contract. This Contract constitutes the final, complete, and exclusive Contract between the parties, containing all the terms and conditions agreed to by the parties.

(b) Prior representations. All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

(c) Conditions precedent. There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

(d) Sole applicable terms. No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

(e) Other terms unenforceable. The Contractor may not require the Commonwealth or any user of the Services or Supplies acquired within the scope of this Contract to sign, click through, or in any other way agree to any terms associated with use of or interaction with those Services and/or Supplies, unless the Commonwealth has approved the terms in writing in advance under this Contract, and the terms are consistent with this Contract. Further, changes to terms may be accomplished only by processes set out in this Contract; no quotations, invoices, business forms or other documentation, or terms referred to therein, shall become part of this Contract merely by their submission to the Commonwealth or their ordinary use in meeting the requirements of this Contract. Any terms imposed upon the Commonwealth or a user in contravention of this subsection (e) must be removed at the direction of the Commonwealth and shall not be enforced or enforceable against the Commonwealth or the user.

13. PERIOD OF PERFORMANCE.

The Contractor, for the term of this Contract, shall complete all Services and provide all Supplies as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services or Supplies provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services or Supplies.

14. INDEPENDENT PRIME CONTRACTOR.

(a) Independent contractor. In performing its obligations under the Contract, the Contractor will act as an independent contractor and not as an employee or agent of the Commonwealth.

(b) Sole point of contact. The Contractor will be responsible for all Services and Supplies in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

15. SUBCONTRACTS.

The Contractor may subcontract any portion of the Services or Supplies described in this Contract to third parties selected by Contractor and approved in writing by the Commonwealth, whose approval shall not be unreasonably withheld. Notwithstanding the above, if Contractor has disclosed the identity of subcontractor(s) together with the scope of work to be subcontracted in its Proposal, award of the Contract is deemed approval of all named subcontractors and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. Upon request of the Commonwealth, the Contractor must provide the Commonwealth with an un-redacted copy of the subcontract agreement between the Contractor and the subcontractor. The Commonwealth reserves the right, for good cause, to require that the Contractor remove a subcontractor from the project. The

Commonwealth will not be responsible for any costs incurred by the Contractor in replacing the subcontractor if good cause exists.

16. OTHER CONTRACTORS.

The Commonwealth may undertake or award other contracts for additional or related work, and the Contractor shall fully cooperate with other contractors and Commonwealth employees and coordinate its Services and/or its provision of Supplies with such additional work as may be required. The Contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees. This section shall be included in the Contracts of all contractors with which this Contractor will be required to cooperate. The Commonwealth shall equitably enforce this section as to all contractors to prevent the imposition of unreasonable burdens on any contractor.

17. ENHANCED MINIMUM WAGE.

(a) Enhanced Minimum Wage. Contractor/Lessor agrees to pay no less than $12.00 per hour to its employees for all hours worked directly performing the services called for in this Contract/Lease, and for an employee's hours performing ancillary services necessary for the performance of the contracted services or lease when such employee spends at least twenty per cent (20%) of their time performing ancillary services in a given work week.

(b) Adjustment. Beginning July 1, 2019, and annually thereafter, the minimum wage rate shall be increased by $0.50 until July 1, 2024, when the minimum wage reaches $15.00. Thereafter, the minimum wage rate would be increased by an annual cost-of-living adjustment using the percentage change in the Consumer Price Index for All Urban Consumers (CPI-U) for Pennsylvania, New Jersey, Delaware, and Maryland. The applicable adjusted amount shall be published in the Pennsylvania Bulletin by March 1 of each year to be effective the following July 1.

(c) Exceptions. These Enhanced Minimum Wage Provisions shall not apply to employees:

- exempt from the minimum wage under the Minimum Wage Act of 1968;
- covered by a collective bargaining agreement;
- required to be paid a higher wage under another state or federal law governing the services, including the *Prevailing Wage Act* and Davis-Bacon Act; or
- required to be paid a higher wage under any state or local policy or ordinance.

(d) Notice. Contractor/Lessor shall post these Enhanced Minimum Wage Provisions for the entire period of the contract conspicuously in easily-accessible and well-lighted places customarily frequented by employees at or near where the contracted services are performed.

(e) Records. Contractor/Lessor must maintain and, upon request and within the time periods requested by the Commonwealth, furnish all employment and wage records necessary to document compliance with these Enhanced Minimum Wage Provisions.

(f) Sanctions. Failure to comply with these Enhanced Minimum Wage Provisions may result in the imposition of sanctions, which may include, but shall not be limited to, termination of the contract or lease, nonpayment, debarment or referral to the Office of General Counsel for appropriate civil or criminal referral.

(g) Subcontractors. Contractor/Lessor shall include the provisions of these Enhanced Minimum Wage Provisions in every subcontract so that these provisions will be binding upon each subcontractor.

18. COMPENSATION.

(a) General. The Contractor shall be required to perform at the price(s) quoted in the Contract. All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and Services performed to the satisfaction of the Commonwealth.

(b) Travel. The Contractor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Contract. If not otherwise specified in the Contract, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

19. BILLING REQUIREMENTS.

(a) Unless the Contractor has been authorized by the Commonwealth for Evaluated Receipt Settlement or Vendor Self-Invoicing, the Contractor shall include in all of its invoices the following minimum information:

- Vendor name and "Remit to" address, including SAP Vendor number;
- Bank routing information, if ACH;
- SAP Purchase Order number;
- Delivery Address, including name of Commonwealth agency;

- Description of the supplies/services delivered in accordance with SAP Purchase Order (include Purchase Order line number if possible);
- Quantity provided;
- Unit price;
- Price extension;
- Total price; and
- Delivery date of supplies or services.

(b) If an invoice does not contain the minimum information set forth in this section, and comply with the provisions located at https://www.budget.pa.gov/Programs/Pages/E-Invoicing.aspx, relating to the Commonwealth E-Invoicing Program, the Commonwealth may return the invoice as improper. If the Commonwealth returns an invoice as improper, the time for processing a payment will be suspended until the Commonwealth receives a correct invoice. The Contractor may not receive payment until the Commonwealth has received a correct invoice.

20. PAYMENT.

(a) Payment Date. The Commonwealth shall put forth reasonable efforts to make payment by the required payment date. The required payment date is:

- the date on which payment is due under the terms of the Contract;
- **thirty (30) days** after a proper invoice actually is received at the "Bill To" address if a date on which payment is due is not specified in the Contract (a "proper" invoice is not received until the Commonwealth accepts the service as satisfactorily performed); or
- the payment date specified on the invoice if later than the dates established by paragraphs (a)(i) and (a)(ii), above.

(b) Delay; Interest. Payment may be delayed if the payment amount on an invoice is not based upon the price(s) as stated in the Contract. If any payment is not made within **15 days** after the required payment date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act of December 13, 1982, P.L. 1155, No. 266, 72 P. S. § 1507, (relating to interest penalties on Commonwealth accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to interest penalties for late payments to qualified small business concerns).

(c) Payment should not be construed by the Contractor as acceptance of the Service performed by the Contractor. The Commonwealth reserves the right to conduct further testing and inspection after payment, but within a reasonable time after performance, and to reject the service if such post payment testing or inspection discloses a defect or a failure to meet specifications.

21. ELECTRONIC PAYMENTS.

(a) The Commonwealth will make contract payments through the Automated Clearing House (ACH). Within **10 days** of award of the Contract, the Contractor must submit or must have already submitted its ACH information within its user profile in the Commonwealth's procurement system (SRM).

(b) The Contractor must submit a unique invoice number with each invoice submitted. The unique invoice number will be listed on the Commonwealth's ACH remittance advice to enable the Contractor to properly apply the state agency's payment to the invoice submitted.

(c) It is the responsibility of the Contractor to ensure that the ACH information contained in SRM is accurate and complete. Failure to maintain accurate and complete information may result in delays in payments.

22. ASSIGNABILITY.

(a) Subject to the terms and conditions of this section the Contract is binding upon the parties and their respective successors and assigns.

(b) The Contractor may not assign, in whole or in part, the Contract or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of the Commonwealth, which consent may be withheld at the sole and absolute discretion of the Commonwealth.

(c) For the purposes of the Contract, the term "assign" shall include, but shall not be limited to, the sale, gift, assignment, encumbrance, pledge, or other transfer of any ownership interest in the Contractor provided, however, that the term shall not apply to the sale or other transfer of stock of a publicly traded company.

(d) Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned.

(e) Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the

Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

(f) A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

23. INSPECTION AND ACCEPTANCE.

(a) Developed Works and Services.

- *Acceptance*. Acceptance of any Developed Work or Service will occur in accordance with an acceptance plan (Acceptance Plan) submitted by the Contactor and approved by the Commonwealth. Upon approval of the Acceptance Plan by the Commonwealth, the Acceptance Plan becomes part of this Contract.

- *Software Acceptance Test Plan*. For contracts where the development of Software, the configuration of Software or the modification of Software is being inspected and accepted, the Acceptance Plan must include a Software Acceptance Test Plan, as mutually agreed to by the Parties. The Software Acceptance Test Plan will provide for a final acceptance test, and may provide for interim acceptance tests. Each acceptance test will be designed to demonstrate that the Software conforms to the functional specifications, if any, and the requirements of this Contract. The Contractor shall notify the Commonwealth when the Software is completed and ready for acceptance testing. The Commonwealth will not unreasonably delay commencement of acceptance testing.

- If software integration is required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be final unless at the time of final acceptance, the Software does not meet the acceptance criteria set forth in the Contract.

- If software integration is not required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be complete and final.

- *Certification of Completion*. The Contractor shall certify, in writing, to the Commonwealth when an item in the Acceptance Plan is completed and ready for acceptance. The Acceptance Plan shall define acceptance periods for both interim and final items as may be agreed to by the parties. Following receipt of the Contractor's certification of completion of an item, the Commonwealth shall, either:

(1) Provide the Contractor with Commonwealth's written acceptance of the work product; or

(2) Identify to the Contractor, in writing, the failure of the work product to comply with the specifications, listing all such errors and omissions with reasonable detail.

- *Deemed Acceptance*. If the Commonwealth fails to notify the Contractor in writing of any failures in the work product within the applicable acceptance period, the work product shall be deemed accepted.

- *Correction upon Rejection*. Upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the work product to comply with the specifications, the Contractor shall have **15 business days**, or such other time as the Commonwealth and the Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected item, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the items have been brought into compliance with the specifications. Upon receipt of such corrected and resubmitted items and certification, the Commonwealth shall have **15 business days** to test the corrected items to confirm that they are in compliance with the specifications. If the corrected items are in compliance with the specifications, then the Commonwealth shall provide the Contractor with its acceptance of the items in the completed milestone.

- *Options upon Continued Failure*. If, in the opinion of the Commonwealth, the corrected items still contain material failures, the Commonwealth may either:

  (1) Repeat the procedure set forth above; or

  (2) Proceed with its rights under **Section 28, Termination**, except that the cure period set forth in **Subsection 28(c)** may be exercised in the Commonwealth's sole discretion.

(b) Supplies.

- *Inspection prior to Acceptance*. No Supplies received by the Commonwealth shall be deemed accepted until the Commonwealth has had a reasonable opportunity to inspect the Supplies.

- *Defective Supplies*. Any Supplies discovered to be defective or that fail to conform to the specifications may be rejected upon initial inspection or at any later time if the defects contained in the Supplies or the noncompliance

with the specifications were not reasonably ascertainable upon the initial inspection.

(1) The Contractor shall remove rejected item(s) from the premises without expense to the Commonwealth within **15 days** after notification.

(2) Rejected Supplies left longer than **30 days** will be regarded as abandoned, and the Commonwealth shall have the right to dispose of them as its own property and shall retain that portion of the proceeds of any sale which represents the Commonwealth's costs and expenses in regard to the storage and sale of the Supplies.

(3) Upon notice of rejection, the Contractor shall immediately replace all such rejected Supplies with others conforming to the specifications and which are not defective. If the Contractor fails, neglects or refuses to do so, the Commonwealth may procure, in such manner as it determines, supplies similar or identical to the those that Contractor failed, neglected or refused to replace, and deduct from any monies due or that may thereafter become due to the Contractor, the difference between the price stated in the Contract and the cost thereof to the Commonwealth.

24. DEFAULT.

The Commonwealth may, subject to the provisions of **Section 25, Notice of Delays**, and **Section 66, Force Majeure**, and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate (as provided in **Section 28, Termination**) the whole or any part of this Contract for any of the following reasons:

- Failure to begin Services within the time specified in the Contract or as otherwise specified;
- Failure to perform the Services with sufficient labor, equipment, or material to insure the completion of the specified Services in accordance with the Contract terms;
- Unsatisfactory performance of the Services;
- Failure to meet requirements within the time periods(s) specified in the Contract;
- Multiple failures over time of a single service level agreement or a pattern of failure over time of multiple service level agreements;

- Failure to provide a Supply or Service that conforms with the specifications referenced in the Contract;
- Failure or refusal to remove material, or remove, replace or correct any Supply rejected as defective or noncompliant;
- Discontinuance of Services without approval;
- Failure to resume a Service, which has been discontinued, within a reasonable time after notice to do so;
- Insolvency;
- Assignment made for the benefit of creditors;
- Failure or refusal, within **10 days** after written notice by the Contracting Officer, to make payment or show cause why payment should not be made, of any amounts due subcontractors for materials furnished, labor supplied or performed, for equipment rentals or for utility services rendered;
- Failure to protect, repair or make good any damage or injury to property;
- Breach of any provision of this Contract;
- Any breach by Contractor of the security standards or procedures of this Contract;
- Failure to comply with representations made in the Contractor's Proposal; or
- Failure to comply with applicable industry standards, customs and practice.

25. NOTICE OF DELAYS.

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall promptly give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with **Section 27, Changes**.

26. CONDUCT OF SERVICES.

(a) Following the Effective Date of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

(b) In determining whether the Contractor has performed with due diligence under the Contract, it is agreed and understood that the Commonwealth may measure the amount and quality of the Contractor's effort against the representations made in the Contractor's Proposal. The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth reasonably determines that the Contractor has not performed with due diligence, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of **Section 30, Contract Controversies**.

27. CHANGES.

(a) At any time during the performance of the Contract, the Commonwealth or the Contractor may request a change to the Contract. Contractor will make reasonable efforts to investigate the impact of the change request on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commonwealth is the requestor of the change, the Contractor will inform the Commonwealth of any charges for investigating the change request prior to incurring such charges. If the Commonwealth and the Contractor agree on the results of the investigation and any necessary changes to the Contract, the parties must complete and execute a change order to modify the Contract and implement the change. The change order will be evidenced by a writing in accordance with the Commonwealth's change order procedures. No work may begin on the change order until the Contractor has received the executed change order. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall perform the Services according to a mutually agreed-to implementation schedule; and either party may elect to have the matter treated as a dispute between the parties under **Section 30, Contract Controversies**. During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts.

(b) Changes outside the scope of this Contract shall be accomplished through the Commonwealth's procurement procedures, and may result in an amended Contract or a new contract. No payment will be made for services outside of the scope of the Contract for which no amendment has been executed.

28. TERMINATION.

(a) <u>For Convenience</u>.

- The Commonwealth may terminate the Contract, or a Purchase Order issued against the Contract, in whole or in part, without cause by giving Contractor **30 days'** prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

  In the event of termination hereunder, Contractor shall receive payment for the following:

  (1) all Services performed consistent with the terms of the Contract prior to the effective date of termination;

  (2) all actual and reasonable costs incurred by Contractor as a result of the termination of the Contract; and

  In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any subcontractor), loss of use of money, or administrative or overhead costs.

  Failure to agree on any termination costs shall be a dispute handled in accordance with **Section 30, Contract Controversies**, of this Contract.

- The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such Services performed during the **30-day** notice period, if such Services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

- The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

(b) Non-Appropriation. Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When funds (state or federal) are not appropriated or

otherwise made available to support continuation of performance or full performance in a subsequent fiscal year period, the Commonwealth shall have the right to terminate the Contract in whole or in part. The Contractor shall be reimbursed in the same manner as that described in subsection (a) to the extent that appropriated funds are available.

(c) Default. The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within **30 days**, or if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

- Subject to **Section 38, Limitation of Liability**, in the event the Commonwealth terminates this Contract in whole or in part as provided in this subsection (c), the Commonwealth may procure services similar to those so terminated, and the Contractor, in addition to liability for any liquidated damages, shall be liable to the Commonwealth for the difference between the Contract price for the terminated portion of the Services and the actual and reasonable cost (but in no event greater than the fair market value) of producing substitute equivalent services for the terminated Services, provided that the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this section.

- Except with respect to defaults of subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism and unusually severe weather. The Contractor shall notify the Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

- Nothing in this subsection (c) shall abridge the Commonwealth's right to suspend, debar or take other administrative action against the Contractor.

- If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under subsection (a).

- If this Contract is terminated as provided by this subsection (c), the Commonwealth may, in addition to any other rights provided in this subsection (c), and subject law and to other applicable provisions of this

Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such Software, Data, Developed Works, Documentation and other materials as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated.

(d) The rights and remedies of the Commonwealth provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(e) The Commonwealth's failure to exercise any rights or remedies provided in this section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(f) Following exhaustion of the Contractor's administrative remedies as set forth in **Section 30, Contract Controversies**, the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

29. BACKGROUND CHECKS.

(a) The Contractor, at its expense, must arrange for a background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Commonwealth IT facilities, either through on-site access or through remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access and on an annual basis thereafter.

(b) Before the Commonwealth will permit access to the Contractor, the Contractor must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that an employee of the Contractor or an employee of a subcontractor of the Contractor has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the Contractor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee and shall not permit that employee remote access unless the Commonwealth consents to the access, in writing, prior to the access. The Commonwealth may withhold its consent in its sole discretion. Failure of the Contractor to comply with the terms of this section on more than one occasion or Contractor's failure to cure any single failure to the satisfaction of the Commonwealth may result in the Contractor being deemed in default of its Contract.

(c) The Commonwealth specifically reserves the right of the Commonwealth to conduct or require background checks over and above that described herein.

30. CONTRACT CONTROVERSIES.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Contract or a purchase order, the Contractor, within **six (6) months** after the cause of action accrues, must file a written claim with the Contracting Officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists. If the Contractor fails to file a claim or files an untimely claim, the Contractor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, https://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

(b) If the Contractor or the Contracting Officer requests mediation, and the other party agrees, the Contracting Officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the Contracting Officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the Contracting Officer and the Contractor. The Contracting Officer shall send his/her written determination to the Contractor. If the Contracting Officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The Contracting Officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Contractor shall proceed diligently with the performance of the Contract or Purchase Order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Contractor pursuant to the terms of the Contract or Purchase Order.

31. CONFIDENTIALITY, PRIVACY AND COMPLIANCE.

(a) General. The Contractor agrees to protect the confidentiality of the Commonwealth's confidential information. The Commonwealth agrees to protect the confidentiality of Contractor's confidential information. Unless the context otherwise clearly indicates the need for confidentiality, information is deemed

confidential only when the party claiming confidentiality designates the information as "confidential" in such a way as to give notice to the other party (for example, notice may be communicated by describing the information, and the specifications around its use or disclosure, in the Solicitation or in the Proposal). Neither party may assert that information owned by the other party is such party's confidential information. Notwithstanding the foregoing, all Data provided by, or collected, processed, or created on behalf of the Commonwealth is Confidential Information unless otherwise indicated in writing.

(b) Copying; Disclosure; Termination. The parties agree that confidential information shall not be copied, in whole or in part, or used or disclosed except when essential for authorized activities under this Contract and, in the case of disclosure, where the recipient of the confidential information has agreed to be bound by confidentiality requirements no less restrictive than those set forth herein. Each copy of confidential information shall be marked by the party making the copy with any notices appearing in the original. Upon expiration or termination of this Contract or any license granted hereunder, the receiving party will return to the disclosing party, or certify as to the destruction of, all confidential information in the receiving party's possession, other than one copy (where permitted by law or regulation), which may be maintained for archival purposes only, and which will remain subject to this Contract's security, privacy, data retention/destruction and confidentiality provisions. A material breach of these requirements may result in termination for default pursuant to **Subsection 28(c)**, in addition to other remedies available to the non-breaching party.

(c) Insofar as information is not otherwise protected by law or regulation, the obligations stated in this section do not apply to information:

- already known to the recipient at the time of disclosure other than through the contractual relationship;
- independently generated by the recipient and not derived from the information supplied by the disclosing party;
- known or available to the public, except where such knowledge or availability is the result of unauthorized disclosure by the recipient of the proprietary information;
- disclosed to the recipient without a similar restriction by a third party who has the right to make such disclosure; or
- required to be disclosed by the recipient by law, regulation, court order, or other legal process.

There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how or data processing techniques developed alone or jointly with

the Commonwealth in connection with services provided to the Commonwealth under this Contract.

(d) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare and submit an un-redacted version of the appropriate document;
- Prepare and submit a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret. The Contractor shall use a redaction program that ensures the information is permanently and irreversibly redacted; and
- Prepare and submit a signed written statement that identifies confidential or proprietary information or trade secrets and that states:

  (1) the attached material contains confidential or proprietary information or trade secrets;

  (2) the Contractor is submitting the material in both redacted and un-redacted format, if possible, in accordance with 65 P.S. § 67.707(b); and

  (3) the Contractor is requesting that the material be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(e) Disclosure of Recipient or Beneficiary Information Prohibited. The Contractor shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from Services under the Contract for any purpose not connected with the Contractor's responsibilities, except with consent pursuant to applicable law or regulations. All material associated with direct disclosures of this kind (including the disclosed information) shall be provided to the Commonwealth prior to the direct disclosure.

(f) Compliance with Laws. Contractor will comply with all applicable laws or regulations related to the use and disclosure of information, including information that constitutes Protected Health Information (PHI) as defined by the *Health Insurance Portability and Accountability* Act (HIPAA). Further, by signing this Contract, the Contractor agrees to the terms of the Business Associate Agreement, which is incorporated into this Contract as **Exhibit A**, or as otherwise negotiated by the Contractor and the purchasing agency. It is understood that **Exhibit A, *Commonwealth of Pennsylvania Business Associate Agreement***, is only applicable if and to the extent indicated in the Contract.

(g) Additional Provisions. Additional privacy and confidentiality requirements may be specified in the Contract.

(h) Restrictions on Use. All Data and all intellectual property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be used only for the work of this Contract. No Data, intellectual property, Documentation or Developed Works may be used, disclosed, or otherwise opened for access by or to the Contractor or any third party unless directly related to and necessary under the Contract.

32. PCI SECURITY COMPLIANCE.

(a) General. By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the payment brands (including, but not limited to, Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. The Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law or regulations.

(b) Compliance with Standards. The Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://www.pcisecuritystandards.org/security_standards/index.php. The Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. The Contractor shall provide a letter of certification to attest to meeting this requirement within **seven (7) days** of the Contractor's receipt of the annual PCI DSS compliance report.

33. DATA BREACH OR LOSS.

(a) The Contractor shall comply with all applicable data protection, data security, data privacy and data breach notification laws, including but not limited to the *Breach of Personal Information Notification Act,* Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329.

(b) For Data and Confidential Information in the possession, custody, and control of the Contractor or its employees, agents, and/or subcontractors:

■ The Contractor shall report unauthorized access, use, release, loss, destruction or disclosure of Data or Confidential Information ("Incident")

to the Commonwealth within **two (2) hours** of when the Contractor knows of or reasonably suspects such Incident, and the Contractor must immediately take all reasonable steps to mitigate any potential harm or further access, use, release, loss, destruction or disclosure of such Data or Confidential Information.

- The Contractor shall provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the Commonwealth. At the Commonwealth's request, Contractor shall, at its sole expense, provide credit monitoring services to all individuals that may be impacted by any Incident requiring notice.

- The Contractor shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents. In addition, any citizens impacted by breach of data will be offered at least 12 months of credit monitoring at the expense of the Contractor.

(c) As to Data and Confidential Information fully or partially in the possession, custody, or control of the Contractor and the Commonwealth, the Contractor shall diligently perform all of the duties required in this section in cooperation with the Commonwealth, until the time at which a determination of responsibility for the Incident, and for subsequent action regarding the Incident, is made final.

34. INSURANCE.

(a) General. Unless otherwise indicated in the Solicitation, the Contractor shall maintain at its expense and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance, issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

- Workers' Compensation Insurance for all of the Contractor's employees and those of any subcontractor engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

- Commercial general liability insurance providing coverage from claims for damages for personal injury, death and property of others, including loss of use resulting from any property damage which may arise from its operations under this Contract, whether such operation be by the Contractor, by any agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than **$500,000** per person and **$2,000,000** per occurrence, personal injury and property damage combined. Such policies shall be occurrence

based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or Supplies provided to the Commonwealth.

- Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of **$2,000,000**, per accident/occurrence/annual aggregate.

- Professional Liability/Errors and Omissions Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Network/Cyber Liability Insurance (including coverage for Professional and Technology-Based Services Liability if not covered under Company's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of **$3,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Completed Operations Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Comprehensive crime insurance in an amount of not less than **$5,000,000** per claim.

(b) Certificate of Insurance. Prior to commencing Services under the Contract, and annually thereafter, the Contractor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days'** prior written notice has been given to the Commonwealth. Such cancellation or change shall not relieve the Contractor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Contractor agrees to maintain such insurance for the latter of the life of the Contract, or the life of any Purchase Orders issued under the Contract.

35. CONTRACTOR RESPONSIBILITY PROGRAM.

(a) For the purpose of these provisions, the term Contractor is defined as any person, including, but not limited to, a bidder, offeror, loan recipient, grantee or lessor, who has furnished or performed or seeks to furnish or perform, goods, Supplies, Services, leased space, construction or other activity, under a contract, grant, lease, Purchase Order or reimbursement agreement with the Commonwealth of Pennsylvania (Commonwealth). The term Contractor includes a permittee, licensee, or any agency, political subdivision, instrumentality, public authority, or other public entity in the Commonwealth.

(b) The Contractor certifies, in writing, for itself and its subcontractors required to be disclosed or approved by the Commonwealth, that as of the date of its execution of this Bid/Contract, that neither the Contractor, nor any subcontractors, nor any suppliers are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its Bid/Contract, a written explanation of why such certification cannot be made.

(c) The Contractor also certifies, in writing, that as of the date of its execution of this Bid/Contract it has no tax liabilities or other Commonwealth obligations, or has filed a timely administrative or judicial appeal if such liabilities or obligations exist, or is subject to a duly approved deferred payment plan if such liabilities exist.

(d) The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the Contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or, to the best knowledge of the Contractor, any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such notification shall be made within **15 days** of the date of suspension or debarment.

(e) The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.

(f) The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative

costs for investigations that do not result in the Contractor's suspension or debarment.

(g) The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the Internet at https://www.dgs.pa.gov/Pages/default.aspx or contacting the:

Department of General Services
Office of Chief Counsel
603 North Office Building
Harrisburg, PA 17125
Telephone No. (717) 783-6472
FAX No. (717) 787-9138

36. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS.

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor or its subsidiaries to the Commonwealth against any payments due the Contractor under any contract with the Commonwealth.

37. TAXES-FEDERAL, STATE AND LOCAL.

The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-7400001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

38. LIMITATION OF LIABILITY.

(a) General. The Contractor's liability to the Commonwealth under this Contract shall be limited to the greater of **$250,000** or the value of this Contract (including any amendments). This limitation will apply, except as otherwise stated in this section, regardless of the form of action, whether in contract or in tort, including negligence. This limitation does not, however, apply to any damages:

■ for bodily injury;

- for death;
- for intentional injury;
- for damage to real property or tangible personal property for which the Contractor is legally liable;
- under **Section 42, Patent, Copyright, Trademark and Trade Secret Protection**;
- under **Section 33, Data Breach or Loss**; or
- under **Section 41, Virus, Malicious, Mischievous or Destructive Programming**.

(b) The Contractor will not be liable for consequential or incidental damages, except for damages as set forth in **paragraphs (a)(i)—(vii)** above, or as otherwise specified in the Contract.

39. COMMONWEALTH HELD HARMLESS.

(a) The Contractor shall indemnify the Commonwealth against any and all third party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its employees and agents under this Contract, provided the Commonwealth gives Contractor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act,* Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

(b) Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

40. SOVEREIGN IMMUNITY.

No provision of this Contract may be construed to waive or limit the sovereign immunity of the Commonwealth of Pennsylvania or its governmental sub-units.

41. VIRUS, MALICIOUS, MISCHIEVOUS OR DESTRUCTIVE PROGRAMMING.

(a) The Contractor shall be liable for any damages incurred by the Commonwealth if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The Contractor's liability shall cease if the Commonwealth has not fully complied with its own software security standards.

(b) The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of Software, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

(d) The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

(e) The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

(f) The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

(g) The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the

Commonwealth's anti-virus software or monitoring software on the Contractor's computers.

42. PATENT, COPYRIGHT, TRADEMARK AND TRADE SECRET PROTECTION.

(a) The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States or foreign patents, copyrights, trademarks or trade dress, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act*, Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion and under the terms it deems appropriate, may delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement that prevents the Commonwealth from continuing to use the Developed Works as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests that the Commonwealth provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. If OAG does not delegate the defense of the matter, the Contractor's obligation to indemnify ceases. The Contractor, at its expense, will provide whatever cooperation OAG requests in the defense of the suit.

(b) The Contractor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Contractor certifies that, in all respects applicable to this Contract, it has exercised and will continue to exercise due diligence to ensure that all works produced under this Contract do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties. The Contractor also agrees to certify that work produced for the Commonwealth under this contract shall be free and clear from all claims of any nature.

(c) If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs awarded therein against the Commonwealth. If information and assistance are furnished by the Commonwealth at the Contractor's written request,

it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

(d) If, in the Contractor's opinion, the products, materials, reports, studies, or computer programs furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a misappropriation of trade secret, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense:

- substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs; or
- obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs.

(e) If any of the products, materials, reports, studies, or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, the Contractor shall, at its own expense and at its option, either procure the right to publish or continue use of such infringing products, materials, reports, studies, or computer programs, replace them with non-infringing items, or modify them so that they are no longer infringing.

(f) If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

- any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the deliverable;
- any license fee less an amount for the period of usage of any software; and
- the prorated portion of any service fees representing the time remaining in any period of service for which payment was made.

(g) Notwithstanding the above, the Contractor shall have no obligation for:

- modification of any product, service, or deliverable provided by the Commonwealth;
- any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, service, or deliverable;
- use of the product, service, or deliverable in other than its specified operating environment;
- the combination, operation, or use of the product, service, or deliverable with other products, services, or deliverables not provided by the Contractor

as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Contractor did not provide;

- infringement of a non-Contractor product alone;
- the Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract; or
- the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge.

(h) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Contractor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

43. CONTRACT CONSTRUCTION.

The provisions of this Contract shall be construed in accordance with the provisions of all applicable laws and regulations of the Commonwealth. However, by executing this Contract, the Contractor agrees that it has and will continue to abide by the intellectual property laws and regulations of the United States of America.

44. USE OF CONTRACTOR AND THIRD PARTY PROPERTY.

(a) Definitions.

- "Contractor Property" refers to Contractor-owned tangible and intangible property.
- "Third Party" refers to a party that licenses its property to Contractor for use under this Contract.
- "Third Party Property" refers to property licensed by the Contractor for use in its work under this Contract.

(b) Contractor Property shall remain the sole and exclusive property of the Contractor. Third Party Property shall remain the sole and exclusive property of the Third Party. The Commonwealth acquires rights to the Contractor Property and Third Party Property as set forth in this Contract.

- Where the Contractor Property or Third Party Property is integrated into the Supplies or Services which are not Developed Works~~)~~, or the Contractor Property is otherwise necessary for the Commonwealth to attain the full benefit of the Supplies or Services in accordance with the terms of the Contract, the Contractor hereby grants to the Commonwealth a non-

exclusive, fully-paid up, worldwide license to use the Contractor Property as necessary to meet the requirements of the Contract, including the rights to reproduce, distribute, publicly perform, display and create derivative works of the Contractor Property. These rights are granted for a duration and to an extent necessary to meet the requirements under this Contract. If the Contractor requires a separate license agreement, such license terms shall include the aforementioned rights, be acceptable to the Commonwealth and include the applicable provisions set forth in these terms at **Exhibit B**, ***Software/Services License Requirements Agreement Template***.

- If Third Party Property is integrated into the Supplies or Services which are not Developed Works, or the Third Party Property is otherwise necessary for the Commonwealth to attain the full benefit of the Supplies or Services in accordance with the terms of the Contract, the Contractor shall gain the written approval of the Commonwealth prior to the use of the Third Party Property or the integration of the Third Party Property into the Supplies or Services. Third Party Property approved by the Commonwealth is hereby licensed to the Commonwealth as necessary to meet the Contract requirements.

- If the Third Party requires a separate license agreement, the license terms shall be acceptable to the Commonwealth and include the applicable provisions set forth in these terms at ***Exhibit B, Software/Services License Requirements Agreement Template***.

- If the use or integration of the Third Party Property is not approved in writing under this section, the Third Party Property shall be deemed to be licensed under paragraph (b)(i) above.

- If the Contract expires or is terminated for default pursuant to subsection 28(c) before the Contract requirements are complete, all rights are granted for a duration and for purposes necessary to facilitate Commonwealth's or a Commonwealth-approved vendor's completion of the Supplies, Services or Developed Works under this Contract. The Contractor, in the form used by Contractor in connection with the Supplies, Services, or Developed Works, shall deliver to Commonwealth the object code version of such Contractor Property, the Third Party Property and associated licenses immediately prior to such expiration or termination to allow the Commonwealth to complete such work.

- Where third party users are reasonably anticipated by the Contract, all users are granted the right to access and use Contractor Property for the purposes of and within the scope indicated in the Contract.

(c) The Commonwealth will limit its agents and contractors' use and disclosure of the Contractor Property as necessary to perform work on behalf of the Commonwealth.

(d) The parties agree that the Commonwealth, by acknowledging the Contractor Property, does not agree to any terms and conditions of the Contractor Property agreements that are inconsistent with or supplemental to this Contract.

(e) Reports. When a report is provided under this Contract, but was not developed specifically for the Commonwealth under this Contract, the ownership of the report will remain with the Contractor; provided, however, that the Commonwealth has the right to use, copy and distribute the report within the executive agencies of the Commonwealth.

45. USE OF COMMONWEALTH PROPERTY.

"Commonwealth Property" refers to Commonwealth-owned Software, Data and property (including intellectual property) and third party owned Software and property (including intellectual property) licensed to the Commonwealth.

(a) Confidentiality of Commonwealth Property. All Commonwealth Property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be considered confidential information under **Section 31, Confidentiality, Privacy, and Compliance**.

(b) License grant and restrictions. During the term of this Contract, Commonwealth grants to Contractor and its subcontractors for the limited purpose of providing the Services covered under this Contract, a limited, nonexclusive, nontransferable, royalty-free right (subject to the terms of any third party agreement to which the Commonwealth is a party) to access, use, reproduce, and modify Commonwealth Property in accordance with the terms of the Contract. The Commonwealth's license to Contractor is limited by the terms of this Contract.

- The Contractor hereby assigns to the Commonwealth its rights, if any, in any derivative works resulting from Contractor's modification of the Commonwealth Intellectual Property. Contractor agrees to execute any documents required to evidence this assignment and to waive any moral rights and rights of attribution provided for in Section 106A of Title 17 of the United States Code, the *Copyright Act of 1976,* as amended.

- Neither Contractor nor any of its subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Intellectual Property. Commonwealth hereby represents that it has the authority to provide the license grant and rights set forth in this section.

(c) Reservation of rights. All rights not expressly granted here to Contractor are reserved by the Commonwealth.

(d) Termination of Commonwealth license grant.

- *Rights Cease*. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract, all rights granted to Contractor under this section shall immediately cease.

- *Return Commonwealth Property*. Contractor shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Intellectual Property (including any related source code then in Contractor's possession or under its control) in the form in use as of the Effective Date of such expiration or termination (except that Commonwealth Data shall be turned over in a form acceptable to the Commonwealth).

- *List of utilized Commonwealth Property/Destruction*. Within **15 days** after termination, Contractor shall provide the Commonwealth with a current copy of the list of Commonwealth Intellectual Property in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth, in writing; provided, however, that Contractor may retain one archival copy of such Commonwealth Software, until final resolution of any actively asserted pending disputes between the Parties, such retention being for the sole purpose of resolving such disputes.

(e) Effect of license grant termination. Consistent with the provisions of this section, Contractor shall refrain from manufacturing, copying, marketing, distributing or using any Commonwealth Software or any other work which incorporates the Commonwealth Software.

(f) Commonwealth Property Protection.

- Contractor acknowledges Commonwealth's exclusive right, title and interest, including without limitation copyright and trademark rights, in and to Commonwealth Data, Commonwealth Software and the Developed Works developed under the provisions of this Contract, and Contractor shall not, directly or indirectly, do or cause to be done any act or thing contesting or in any way impairing or tending to impair any part of said right, title, and interest, and shall not use or disclose the Commonwealth Data, Commonwealth Software or the Developed Works without Commonwealth's written consent, which consent may be withheld by the Commonwealth for any reason.

- Contractor shall not, in any manner, represent that Contractor has any ownership interest in the Commonwealth Data, Commonwealth Software or the Developed Works.

46. OWNERSHIP OF DEVELOPED WORKS.

Unless otherwise specified in the Contract's Statement of Work, ownership of all Developed Works shall be in accordance with the provisions set forth in this section.

(a) Rules for usage for Developed Works.

- *Property of Contractor.* If Developed Works modify, improve, contain, or enhance application software programs or other materials generally licensed by the Contractor, then such Developed Works shall be the property of the Contractor, and Contractor hereby grants Commonwealth an irrevocable, nonexclusive, worldwide, fully paid-up license (to include source code and relevant documentation) in perpetuity to use, modify, execute, reproduce, display, perform, prepare derivative works from and distribute, within the Commonwealth, such Developed Works.

  (1) For purposes of distribution under the license grant created by this section, Commonwealth includes any government agency, department, instrumentality, division, unit or other office that is part of the Commonwealth of Pennsylvania, together with the State System of Higher Education (including any of its universities), any county, borough, commonwealth, city, municipality, town, township special purpose district, or other similar type of governmental instrumentality located within the geographical boundaries of the Commonwealth of Pennsylvania.

  (2) If federal funds are used in creation of the Developed Works, the Commonwealth also includes any other state government as well as the federal government.

- *Property of Commonwealth/licensor*. If the Developed Works modify, improve or enhance application software or other materials not licensed to the Commonwealth by the Contractor, then such modifications, improvements and enhancements shall be the property of the Commonwealth or its licensor.

(b) Copyright Ownership.

- *Works made for hire; general*. Except as indicated in paragraph (a)(i), above, Developed Works developed as part of the scope of work for the Project, including Developed Works developed by subcontractors, are the sole and exclusive property of the Commonwealth and shall be considered

"works made for hire" under the *Copyright Act of 1976*, as amended, 17 United States Code.

- *Assignment*. In the event that the Developed Works do not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns, all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such Developed Works to Commonwealth. Contractor further agrees that it will have its subcontractors assign, and upon their authorship or creation, expressly and automatically assigns all copyright interest, proprietary rights, trade secrets, and other right, title, and interest in and to the Developed Works to the Commonwealth.

- *Rights to Commonwealth*. Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the Developed Works in multiple copies, the right to distribute copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Developed Works and the right to display the Developed Works.

- *Subcontracts*. The Contractor further agrees that it will include the requirements of this section in any subcontractor or other agreement with third parties who in any way participate in the creation or development of Developed Works.

- *Completion or termination of Contract*. Upon completion or termination of this Contract, Developed Works, or completed portions thereof, shall immediately be delivered by Contractor to the Commonwealth.

- *Warranty of noninfringement*. Contractor represents and warrants that the Developed Works are original and do not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws and regulations of the United States.

(c) Patent ownership. Contractor and its subcontractors shall retain ownership to patentable items, patents, processes, inventions or discoveries (collectively, the Patentable Items) made by the Contractor during the performance of this Contract. Notwithstanding the foregoing, the Commonwealth shall be granted a nonexclusive, nontransferable, royalty free license to use or practice the Patentable Items. Commonwealth may disclose to third parties any such Patentable Items made by Contractor or any of its subcontractors under the scope of work for the Project that have been previously publicly disclosed. Commonwealth understands

and agrees that any third party disclosure will not confer any license to such Patentable Items.

(d) Federal government interests. Certain funding under this Contract may be provided by the federal government. Accordingly, the rights to Developed Works or Patentable Items of Contractors or subcontractors hereunder will be further subject to government rights as set forth in 37 C.F.R. Part 401, as amended, and other applicable law or regulations.

(e) Usage rights. Except as otherwise covered by this section either Party, in the ordinary course of conducting business, may use any ideas, concepts, know-how, methodologies, processes, components, technologies, algorithms, designs, modules or techniques relating to the Services.

(f) Contractor's copyright notice obligations. Contractor will affix the following Copyright Notice to the Developed Works developed under this section and all accompanying documentation: "*Copyright © [year] by the Commonwealth of Pennsylvania. All Rights Reserved*." This notice shall appear on all versions of the Developed Works delivered under this Contract and any associated documentation. It shall also be programmed into any and all Developed Works delivered hereunder so that it appears at the beginning of all visual displays of such Developed Works.

47. SOURCE CODE AND ESCROW ITEMS OBLIGATIONS.

(a) Source code. Simultaneously with delivery of the Developed Works to Commonwealth, Contractor shall deliver a true, accurate and complete copy of all source codes relating to the Developed Works.

(b) Escrow. To the extent that Developed Works and/or any perpetually-licensed software include application software or other materials generally licensed by the Contractor, Contractor agrees to place in escrow with an escrow agent copies of the most current version of the source code for the applicable software that is included as a part of the Services, including all updates, improvements, and enhancements thereof from time to time developed by Contractor.

(c) Escrow agreement. An escrow agreement must be executed by the parties, with terms acceptable to the Commonwealth, prior to deposit of any source code into escrow.

(d) Obtaining source code. Contractor agrees that upon the occurrence of any event or circumstance which demonstrates with reasonable certainty the inability or unwillingness of Contractor to fulfill its obligations to Commonwealth under this Contract, Commonwealth shall be able to obtain the source code of the then-current source codes related to Developed Works and/or any Contractor Property placed in escrow under subsection (b), above, from the escrow agent.

48. LOCATION, STATUS AND DISPOSITION OF DATA.

Unless the Solicitation specifies otherwise:

- All Data must be stored within the United States;
- The Contractor shall be responsible for maintaining the privacy, security and integrity of Data in the Contractor's or its subcontractors' possession;
- All Data shall be provided to the Commonwealth upon request, in a form acceptable to the Commonwealth and at no cost;
- Any Data shall be destroyed by the Contractor at the Commonwealth's request; and
- Any Data shall be held for litigation or public records purposes by the Contractor at the Commonwealth's request, and in accordance with the security, privacy and accessibility requirements of this Contract.

49. PUBLICATION RIGHTS AND/OR COPYRIGHTS.

(a) Except as otherwise provided in **Section 46, Ownership of Developed Works**, the Contractor shall not publish any of the results of the work without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

(b) Except as otherwise provided in the Contract, the Commonwealth shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

50. CHANGE OF OWNERSHIP OR INSOLVENCY.

In the event that the Contractor should change ownership for any reason whatsoever, the Commonwealth shall have the exclusive option of continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for the full remaining term of this Contract, or continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for such period of time as is necessary to replace the products, materials, reports, studies, or computer programs, or immediately terminating this Contract. Nothing in this section limits the Commonwealth's exercise of any rights that the Commonwealth may have under **Section 28, Termination**.

51. OFFICIALS NOT TO BENEFIT.

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

52. COMPLIANCE WITH LAWS.

(a) The Contractor shall comply with all federal, state and local laws, regulations and policies applicable to its Services or Supplies, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation.

(b) If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services or Supplies provided under this Contract, the Parties shall modify this Contract, via **Section 27, Changes**, to the extent reasonably necessary to:

- Ensure that such Services or Supplies will be in full compliance with such laws, regulations and policies; and
- Modify the rates applicable to such Services or Supplies, unless otherwise indicated in the Solicitation.

53. *THE AMERICANS WITH DISABILITIES ACT*.

During the term of this Contract, the Contractor agrees as follows:

(a) Pursuant to federal regulations promulgated under the authority of *The Americans With Disabilities Act*, 28 C.F.R.§ 35.101, *et seq*., the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this Contract or from activities provided for under this Contract. As a condition of accepting and executing this Contract, the Contractor agrees to comply with the *General Prohibitions Against Discrimination*, 28 C.F.R. § 35.130, and all other regulations promulgated under Title II of *The Americans With Disabilities Act* which are applicable to the benefits, services, programs, and activities provided by the Commonwealth of Pennsylvania through Contracts with outside Contractors.

(b) The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from losses, damages, expenses claims, demands, suits, and actions brought by any party against the Commonwealth of

Pennsylvania as a result of the Contractor's failure to comply with the provisions of subsection (a).

54. EXAMINATION OF RECORDS.

(a) The Contractor agrees to maintain, using its standard procedures, and in accordance with Generally Accepted Accounting Principles, books, records, documents, and other evidence pertaining to the charges under this Contract to the extent and in such detail as will properly reflect all charges for which reimbursement is claimed under the provisions of this Contract.

(b) The Contractor agrees to make available at the office of the Contractor at all reasonable times, and upon reasonable written notice, during the term of this Contract and the period set forth in subsection (c) below, any of the records for inspection, audit, or reproduction by any authorized Commonwealth representative. To the extent allowed by applicable laws or regulations, the Commonwealth agrees to maintain any documents so provided in accordance with the confidentiality provisions in **Section 31, Confidentiality, Privacy and Compliance**.

(c) The Contractor shall preserve and make available its records for a period of **three (3) years** from the date of final payment under this Contract.

- If this Contract is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of **three (3) years** from the date of any resulting final settlement.

- Non-privileged records which relate to litigation or the settlement of claims arising out of the performance of this Contract, or charges under this Contract as to which exception has been taken by the auditors, shall be retained by the Contractor until such litigation, claims, or exceptions have been finally resolved.

(d) Except for documentary evidence retained pursuant to paragraph (c)(ii) above, the Contractor may in fulfillment of its obligation to retain its records as required by this section substitute photographs, microphotographs, or other authentic reproductions of such records, after the expiration of **two (2) years** following the last day of the month of reimbursement to the Contractor of the invoice or voucher to which such records relate, unless a shorter period is authorized by the Commonwealth with the concurrence of its auditors.

(e) The provisions of this section shall be applicable to and included in each subcontract hereunder.

55. SINGLE AUDIT ACT OF 1984.

In compliance with the *Single Audit Act of 1984*, as amended, the Contractor agrees to the following:

(a) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in the most current version of *Government Auditing Standards* (Yellow Book).

(b) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984*, as amended, 31 U.S.C. § 7501, *et seq*., and all rules and regulations promulgated pursuant to the Act.

(c) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(d) The Contractor further agrees to comply with requirements that may be issued by the state agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984*, as amended.

56. AGENCY-SPECIFIC SENSITIVE AND CONFIDENTIAL COMMONWEALTH DATA (IF APPLICABLE).

(a) Contractor understands that its level of access may allow or require it to view or access highly sensitive and confidential Commonwealth and third party data. This data is subject to various state and federal laws, regulations and policies that vary from agency to agency, and from program to program within an agency. If applicable, prior to deployment of the Supplies or Services, the Contractor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth agency, including but not limited to, as necessary, HIPAA Business Associate Agreements. This sign-off document, a sample of which is attached as **Exhibit C, *Sample Sign-off Document***, will include a description of the nature of the data which may be implicated based on the nature of the Contractor's access, and will incorporate the Business Associate Agreement if it is applicable.

(b) The Contractor hereby certifies and warrants that, after being informed by the Commonwealth agency of the nature of the data which may be implicated and prior to the deployment of the Supplies or Services, the Contractor is and shall remain compliant with all applicable state and federal laws, regulations and policies regarding the data's protection, and with the requirements memorialized in every completed and signed sign-off document. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract.

(c) This section does not require a Commonwealth agency to exhaustively list the laws, regulations or policies to which implicated data is subject; the Commonwealth agency is obligated only to list the nature of the data implicated by the Contractor's access, to refer the Contractor to its privacy and security policies, and to specify requirements that are not otherwise inherent in compliance with applicable laws, regulations and policies.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Contract, its Exhibits, Appendices and Attachments, having to do with data privacy and security, including but not limited to the requirement that the Contractor comply with all applicable Commonwealth ITPs, which can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx.

(e) Contractor shall conduct additional background checks, in addition to those required in **Section 29, Background Checks**, as may be required by a Commonwealth agency in its sign-off documents. The Contractor shall educate and hold its agents, employees, contractors and subcontractors to standards at least as stringent as those contained in this Contract. The Contractor shall provide information regarding its agents, employees, contractors and subcontractors to the Commonwealth upon request.

57. FEDERAL REQUIREMENTS.

If applicable, the Contractor must receive and sign off on particular federal requirements that a Commonwealth agency may be required to include when utilizing federal funds to procure the Supplies and Services. This sign-off document, in addition to any applicable requirements of **Section 56, Agency-Specific Sensitive and Confidential Commonwealth Data**, will include a description of the required federal provisions, along with the applicable forms necessary for the Contractor and/or Software Licensor to execute, as necessary. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract. A sample sign-off document is attached to these Terms as **Exhibit C, *Sample Sign-off Document***.

58. ADDITIONAL FEDERAL PROVISIONS.

Additional contract provisions may be incorporated into this Contract pursuant to federal law, regulation or policy.

59. ENVIRONMENTAL PROTECTION.

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law,* Act of June 22, 1937 (P.L. 1987, No. 394), as amended, 35 P.S. §§ 691.1—691.801; the *Solid Waste Management Act,* Act of July 7, 1980 (P.L. 380, No. 97), as

amended, 35 P.S. §§ 6018.101—68.1003; and the *Dam Safety and Encroachment Act,* Act of November 26, 1978 (P.L. 1375, No. 325), as amended, 32 P.S. §§ 693.1—693.27.

60. NONDISCRIMINATION/SEXUAL HARASSMENT CLAUSE.

The Contractor agrees:

(a) In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the *Pennsylvania Human Relations Act* (PHRA) and applicable federal laws, against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

(b) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under the contract.

(c) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, in the provision of services under the contract.

(d) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against employees by reason of participation in or decision to refrain from participating in labor activities protected under the *Public Employee Relations Act*, *Pennsylvania Labor Relations Act* or *National Labor Relations Act*, as applicable and to the extent determined by entities charged with such Acts' enforcement, and shall comply with any provision of law establishing organizations as employees' exclusive representatives.

(e) The Contractor and each subcontractor shall establish and maintain a written nondiscrimination and sexual harassment policy and shall inform their employees in writing of the policy. The policy must contain a provision that sexual harassment will not be tolerated and employees who practice it will be disciplined. Posting this Nondiscrimination/Sexual Harassment Clause conspicuously in easily-accessible and well-lighted places customarily frequented by employees and at or near where the contracted services are performed shall satisfy this requirement for employees with an established work site.

(f) The Contractor and each subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of PHRA and applicable federal laws, against any subcontractor or supplier who is qualified to perform the work to which the contract relates.

(g) The Contractor and each subcontractor represents that it is presently in compliance with and will maintain compliance with all applicable federal, state, and local laws, regulations and policies relating to nondiscrimination and sexual harassment. The Contractor and each subcontractor further represents that it has filed a Standard Form 100 Employer Information Report ("EEO-1") with the U.S. Equal Employment Opportunity Commission ("EEOC") and shall file an annual EEO-1 report with the EEOC as required for employers' subject to *Title VII* of the *Civil Rights Act of 1964*, as amended, that have 100 or more employees and employers that have federal government contracts or first-tier subcontracts and have 50 or more employees. The Contractor and each subcontractor shall, upon request and within the time periods requested by the Commonwealth, furnish all necessary employment documents and records, including EEO-1 reports, and permit access to their books, records, and accounts by the contracting agency and the Bureau of Diversity, Inclusion and Small Business Opportunities for purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause.

(h) The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.

(i) The Contractor's and each subcontractor's obligations pursuant to these provisions are ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor and each subcontractor shall have an obligation to inform the Commonwealth if, at any time during the term of the contract, it becomes aware of any actions or occurrences that would result in violation of these provisions.

(j) The Commonwealth may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

61. CONTRACTOR INTEGRITY PROVISIONS.

It is essential that those who seek to contract with the Commonwealth of Pennsylvania ("Commonwealth") observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the Commonwealth contracting and procurement process.

(a) Definitions. For purposes of these Contractor Integrity Provisions, the following terms shall have the meanings found in this section:

- "*Affiliate*" means two or more entities where (a) a parent entity owns more than fifty percent of the voting stock of each of the entities; or (b) a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the entities; or (c) the entities have a common proprietor or general partner.

- "*Consent*" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by prequalification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of the execution of this contract.

- "*Contractor*" means the individual or entity, that has entered into this contract with the Commonwealth.

- "*Contractor Related Parties*" means any affiliates of the Contractor and the Contractor's executive officers, Pennsylvania officers and directors, or owners of 5 percent or more interest in the Contractor.

- "*Financial Interest*" means either:

  (1) Ownership of more than a five percent interest in any business; or

  (2) Holding a position as an officer, director, trustee, partner, employee, or holding any position of management.

- "*Gratuity*" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the *Governor's Code of Conduct, Executive Order 1980-18*, the 4 Pa. Code § 7.153(b), shall apply.

- "*Non-bid Basis*" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(b) In furtherance of this policy, Contractor agrees to the following:

- Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or

regulations, or other requirements applicable to Contractor or that govern contracting or procurement with the Commonwealth.

- Contractor shall establish and implement a written business integrity policy, which includes, at a minimum, the requirements of these provisions as they relate to the Contractor activity with the Commonwealth and Commonwealth employees and which is made known to all Contractor employees. Posting these Contractor Integrity Provisions conspicuously in easily-accessible and well-lighted places customarily frequented by employees and at or near where the contract services are performed shall satisfy this requirement.

- Contractor, its affiliates, agents, employees and anyone in privity with Contractor shall not accept, agree to give, offer, confer, or agree to confer or promise to confer, directly or indirectly, any gratuity or pecuniary benefit to any person, or to influence or attempt to influence any person in violation of any federal or state law, regulation, executive order of the Governor of Pennsylvania, statement of policy, management directive or any other published standard of the Commonwealth in connection with performance of work under this contract, except as provided in this contract.

- Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material under this contract, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest prior to Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.

- Contractor certifies to the best of its knowledge and belief that within the last **five (5) years** Contractor or Contractor Related Parties have not:

  (1) been indicted or convicted of a crime involving moral turpitude or business honesty or integrity in any jurisdiction;

  (2) been suspended, debarred or otherwise disqualified from entering into any contract with any governmental agency;

  (3) had any business license or professional license suspended or revoked;

  (4) had any sanction or finding of fact imposed as a result of a judicial or administrative proceeding related to fraud, extortion, bribery, bid rigging, embezzlement, misrepresentation or anti-trust; and

(5) been, and is not currently, the subject of a criminal investigation by any federal, state or local prosecuting or investigative agency and/or civil anti-trust investigation by any federal, state or local prosecuting or investigative agency.

If Contractor cannot so certify to the above, then it must submit along with its bid, proposal or contract a written explanation of why such certification cannot be made and the Commonwealth will determine whether a contract may be entered into with the Contractor. The Contractor's obligation pursuant to this certification is ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to immediately notify the Commonwealth in writing if at any time during the term of the contract if becomes aware of any event which would cause the Contractor's certification or explanation to change. Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause if it learns that any of the certifications made herein are currently false due to intervening factual circumstances or were false or should have been known to be false when entering into the contract.

Contractor shall comply with the requirements of the *Lobbying Disclosure Act* (65 Pa. C.S. § 13A01, et seq.) regardless of the method of award. If this contract was awarded on a Non-bid Basis, Contractor must also comply with the requirements of the Section 1641 of the *Pennsylvania Election Code* (25 P.S. § 3260a).

When Contractor has reason to believe that any breach of ethical standards as set forth in law, the Governor's Code of Conduct, or these Contractor Integrity Provisions has occurred or may occur, including but not limited to contact by a Commonwealth officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify the Commonwealth contracting officer or the Office of the State Inspector General in writing.

Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these Contractor Integrity Provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract, to include any extensions thereof. Contractor shall immediately notify the Commonwealth in writing of any actions for occurrences that would result in a violation of these Contractor Integrity Provisions. Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of the State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the

Commonwealth that results in the suspension or debarment of the Contractor. Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

- Contractor shall cooperate with the Office of the State Inspector General in its investigation of any alleged Commonwealth agency or employee breach of ethical standards and any alleged Contractor non-compliance with these Contractor Integrity Provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times and places. Contractor, upon the inquiry or request of an Inspector General, shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Office of the State Inspector General to Contractor's integrity and compliance with these provisions. Such information may include, but shall not be limited to, Contractor's business or financial records, documents or files of any type or form that refer to or concern this contract. Contractor shall incorporate this subsection in any agreement, contract or subcontract it enters into in the course of the performance of this contract/agreement solely for the purpose of obtaining subcontractor compliance with this provision. The incorporation of this provision in a subcontract shall not create privity of contract between the Commonwealth and any such subcontractor, and no third party beneficiaries shall be created thereby.

- For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these Provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise.

62. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS.

The Contractor and the Commonwealth recognize that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are subject to this Contract.

63. WARRANTIES.

Except as otherwise set forth in the Contract, the Contractor warrants that the Services, Supplies and Developed Works will conform in all material respects to the functional specifications for the Services, Supplies and Developed Works and/or the requirements of the Contract. The warranty period for the Services, Supplies and Developed Works shall be **90 days** from final acceptance. If third-party Services, Supplies or Developed Works are subject to a warranty that exceeds **90 days** from final acceptance, the longer warranty period shall apply. The Contractor shall correct any non-conformity within the warranty period specified herein.

(a) Disruption. The Contractor hereby represents and warrants to the Commonwealth that the Contractor will not cause, or take any action that, directly or indirectly, may cause a disruption of the Commonwealth's operations.

(b) Nonconformity. In the event of any nonconformity with the foregoing warranties, the Commonwealth will provide written notification of such nonconformity to the Contractor and the Contractor, at no cost to the Commonwealth, shall within **10 days'** notice of the nonconformity, commence work to remedy the nonconformity and shall work diligently, at no charge to the Commonwealth, until such time as the deliverable conforms, in all material respects, to the Service requirements and/or the functional specifications of the Developed Works set forth in this Contract. The Contractor shall have no obligation with respect to nonconformities arising out of:

- Modifications to Developed Works made by the Commonwealth;
- Use of the Developed Works not in accordance with the documentation or specifications applicable thereto;
- Failure by the Commonwealth to implement any corrections or enhancements made available by the Contractor;
- Combination of the Developed Works with any items not supplied or approved by the Contractor; or
- Failure of any software licensed under a separate license agreement to conform to its specifications or documentation.

(c) Industry standards. The Contractor hereby represents and warrants to the Commonwealth that the Services shall be performed in accordance with industry standards using the utmost care and skill.

(d) Right to perform. The Contractor hereby represents and warrants to the Commonwealth that the Contractor has the necessary legal rights, including licenses to third party products, tools or materials, to perform the Services and deliver the Developed Works under this Contract.

(e) Sole warranties. THE FOREGOING EXPRESS WARRANTIES ARE THE CONTRACTOR'S SOLE AND EXCLUSIVE WARRANTIES AND NO OTHER WARRANTIES, EXPRESS OR IMPLIED, SHALL APPLY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

64. PAYMENT PROCEDURE~~LIQUIDATED DAMAGES.~~

(a) Contractor will submit invoices to the Commonwealth for deliverables on the deliverable due date. All deliverables are subject to the inspection and acceptance as given in paragraph 23 of this Contract. The Commonwealth will pay for approved and completed work within 30 calendar days of receipt of an invoice containing all information required for processing.

(b) The Commonwealth will retain 20% of the payment for each accepted deliverable. The Commonwealth will pay Contractor the retainage after final acceptance of all deliverables and includes the Submit Final Implementation Report deliverable.

(c) By accepting this Contract, the Contractor agrees to the delivery and acceptance requirements of this Contract. The delivery dates for the deliverables are listed in the Deliverable Break Down, provided as an attachment to this contract. The Parties may mutually agree to adjust or update any deliverable due date as conditions warrant over the duration of the project. If a deliverable due date is not met or is rejected, payment for the deliverable will be withheld by the Commonwealth. Any missed deliverable due date or deliverable rejection is subject to the conditions as specified in paragraph 23, Inspection and Acceptance, which defines the processes for curing a rejected deliverable. The Contractor will have 30 days to submit the deliverable or cure the rejected deliverable.

(d) If, at the end of the 30-day period specified in subsection (c) above, the Contractor still has not met the requirements for the deliverable associated with the due date, then the Commonwealth, at no additional expense and at its option, may either:

(i) Immediately terminate the Contract in accordance with Subsection 28(c) and with no opportunity to cure; or

(ii) Order the Contractor to continue with no decrease in effort until the work is completed in accordance with the Contract and accepted by the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, any payment withholding and retainage will also continue until the work is completed.

~~(a) By accepting this Contract, the Contractor agrees to the delivery and acceptance requirements of this Contract. If a due date is not met, the delay will interfere with the Commonwealth's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the~~

~~Contractor is the material cause. The Commonwealth and the Contractor therefore agree that in the event of any such delay, the amount of damage shall be the amount set forth in this section, unless otherwise indicated in the Contract, and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty. Such liquidated damages are in lieu of all other damages arising from such delay.~~

~~(b) The amount of liquidated damages shall be as set out in the Solicitation. If not amount is set out in the Solicitation, the amount of liquidated damages for failure to meet a due date shall be three-tenths of a percent **(.3%)** of the price of the deliverable for each calendar day following the scheduled completion date. If the price of the deliverable associated with the missed due date is not identified, liquidated damages shall apply to the total value of the Contract. Liquidated damages shall be assessed each calendar day until the date on which the Contractor meets the requirements for the deliverable associated with the due date, up to a maximum of **30 days**. If indicated in the Contract, the Contractor may recoup all or some of the amount of liquidated damages assessed if the Contractor meets the final project completion date set out in the Contract.~~

~~(c) If, at the end of the **30-day** period specified in subsection (b) above, the Contractor still has not met the requirements for the deliverable associated with the due date, then the Commonwealth, at no additional expense and at its option, may either:~~

- ~~(i) Immediately terminate the Contract in accordance with **Subsection 28(c)** and with no opportunity to cure; or~~
- ~~(ii) Order the Contractor to continue with no decrease in effort until the work is completed in accordance with the Contract and accepted by the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, any liquidated damages will also continue until the work is completed.~~

~~At the end of a calendar month, or at such other time(s) as identified in the Contract, liquidated damages shall be paid by the Contractor and collected by the Commonwealth by:~~

- ~~Deducting the amount from the invoices submitted under this Contract or any other contract Contractor has with the Commonwealth;~~
- ~~Collecting the amount through the performance security, if any; or~~
- ~~Billing the Contractor as a separate item.~~

65. SERVICE LEVELS.

(a) The Contractor shall comply with the procedures and requirements of the Service Level Agreements, if any, which are made part of this Contract.

(b) Where there are expressly defined Service Levels, Contractor shall measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the parties. Regardless of the presence or absence of expressly defined Service Levels, any failure to adequately or timely perform a Service may result in consequences under this Contract, up to and including Contract termination.

(c) The Commonwealth's acceptance of any financial credit incurred by the Contractor in favor of the Commonwealth for a Service Level default ("Service Level Credit") shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation other claims for liquidated damages, injunctive relief and termination rights; provided however, Service Level Credits paid would be credited against any such claims for damages.

66. FORCE MAJEURE.

(a) Neither party will incur any liability to the other if its performance of any obligation under this Contract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, severe weather conditions, civil disorders, natural disasters, fire, epidemics and quarantines, general strikes throughout the trade, and freight embargoes.

(b) The Contractor shall notify the Commonwealth orally within **five (5) days** and in writing within **10 days** of the date on which the Contractor becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance under the contract is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The Contractor shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as the Commonwealth may reasonably request. After receipt of such notification, the Commonwealth may elect to cancel the Contract, or to extend the time for performance as reasonably necessary to compensate for the Contractor's delay.

(c) In the event of a declared emergency by competent governmental authorities, the Commonwealth by notice to the Contractor, may suspend all or a portion of the Contract.

67. PUBLICITY/ADVERTISEMENT.

The Contractor shall not issue news releases, internet postings, advertisements, endorsements, or any other public communication without prior written approval of the Commonwealth, and then only in coordination with the Commonwealth. This includes the use of any trademark or logo.

68. TERMINATION ASSISTANCE.

(a) Upon the Commonwealth's request, Contractor shall provide termination assistance services (Termination Assistance Services) directly to the Commonwealth, or to any vendor designated by the Commonwealth. The Commonwealth may request termination assistance from the Contractor upon full or partial termination of the Contract and/or upon the expiration of the Contract term, including any renewal periods. Contractor shall take all necessary and appropriate actions to accomplish a complete, timely and seamless transition of any Services from Contractor to the Commonwealth, or to any vendor designated by the Commonwealth, without material interruption of or material adverse impact on the Services. Contractor shall cooperate with the Commonwealth and any new contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and timely transition of any Services.

(b) Such Termination Assistance Services shall first be rendered using resources included within the fees for the Services, provided that the use of such resources shall not adversely impact the level of service provided to the Commonwealth; then by resources already included within the fees for the Services, to the extent that the Commonwealth permits the level of service to be relaxed; and finally, using additional resources at costs determined by the Parties via **Section 27, Changes**.

69. NOTICE.

Any written notice to any party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

70. *RIGHT-TO-KNOW LAW*.

(a) The Pennsylvania *Right-to-Know Law*, 65 P.S. §§ 67.101—3104, *as amended*, ("RTKL") applies to this Contract. For the purpose of this section, the term "the Commonwealth" shall refer to the contracting Commonwealth organization.

(b) If the Commonwealth needs the Contractor's assistance in any matter arising out of the RTKL that is related to this Contract, it shall notify the Contractor using the legal contact information provided in this Contract. The Contractor, at any time,

may designate a different contact for such purpose upon reasonable prior written notice to the Commonwealth.

(c) Upon written notification from the Commonwealth that it requires the Contractor's assistance in responding to a request under the RTKL for information related to this Contract that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL ("Requested Information"), the Contractor shall:

- Provide the Commonwealth, within **10 days** after receipt of written notification, access to, and copies of, any document or information in the Contractor's possession arising out of this Contract that the Commonwealth reasonably believes is Requested Information and may be a public record under the RTKL; and

- Provide such other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this Contract.

(d) If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within **seven (7) days** of receiving the written notification via certified mail, a written statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

(e) The Commonwealth will rely upon the written statement from the Contractor in denying a RTKL request for the Requested Information unless the Commonwealth determines that the Requested Information is clearly not protected from disclosure under the RTKL. Should the Commonwealth determine that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information within **five (5) business days** of receipt of written notification of the Commonwealth's determination.

(f) If the Contractor fails to provide the Requested Information within the time period required by these provisions, the Contractor shall indemnify and hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

(g) The Commonwealth will reimburse the Contractor for any costs associated with complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL if the fee schedule is inapplicable.

(h) The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts. ~~, however, the Contractor shall indemnify the Commonwealth for any legal expenses incurred by the Commonwealth as a result of such a challenge and shall hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth, regardless of the outcome of such legal challenge. As between the parties, the Contractor agrees to waive all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.~~

(i) The Contractor's duties relating to the RTKL are continuing duties that survive the expiration of this Contract and shall continue as long as the Contractor has Requested Information in its possession.

71. GOVERNING LAW.

This Contract shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. Except as set forth in **Section 30, Contract Controversies**, Commonwealth and Contractor agree that the courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof. Any legal action relating to this Contract must be brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

72. CONTROLLING TERMS AND CONDITIONS.

The terms and conditions of this Contract shall be the exclusive terms of agreement between the Contractor and the Commonwealth. Other terms and conditions or additional terms and conditions included or referenced in the Contractor's website, quotations, invoices, business forms, click-through agreements, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Contractor, and not binding on the Commonwealth.

73. SMALL DIVERSE BUSINESS/SMALL BUSINESS COMMITMENT.

The Contractor shall meet and maintain the commitments to small diverse businesses in the Small Diverse Business and Small Business ("SDB/SB") portion of its Proposal. Any proposed change to a SDB/SB commitment must be submitted to the DGS Bureau of Diversity, Inclusion and Small Business Opportunities ("BDISBO"), which will make a recommendation as to a course of action to the Commonwealth Contracting Officer. Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Commonwealth Contracting Officer and BDISBO within **10 business days** at the end of each calendar quarter that the Contract is in effect.

74. POST-CONSUMER RECYCLED CONTENT; RECYCLED CONTENT ENFORCEMENT.

Except as specifically waived by the Department of General Services in writing, any products which are provided to the Commonwealth as a part of the performance of the Contract must meet the minimum percentage levels for total recycled content as specified by the Environmental Protection Agency in its Comprehensive Procurement Guidelines, which can be found at https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program.

The Contractor may be required, after delivery of the Contract item(s), to provide the Commonwealth with documentary evidence that the item(s) was in fact produced with the required minimum percentage of post-consumer and recovered material content.

75. SURVIVAL.

Sections 11, 30, 31, 33, 37, 38, 39, 41, 42, 45, 46, 47, 48, 49, 52, 54, 55, 56, 63, 67, 69, 70, 71 and 75 and any right or obligation of the parties in this Contract which, by its express terms or nature and context is intended to survive termination or expiration of this Contract, will survive any such termination or expiration shall survive the expiration or termination of the Contract.

EXHIBIT A

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the [*name of program and/or Department*] (Covered Entity) and the **Contractor (Business Associate)**, intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be handled, used or disclosed only in accordance with this Business Associate Agreement (BAA), the Underlying Agreement and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**Business Associate Agreement**" or "**BAA**" shall mean this Agreement.

(c) "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(d) "**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended, Pub. L. No. 104-191.

(e) "**HITECH Act**" shall mean the Health Information Technology for Economic and Clinical Health (HITECH) Act, as amended, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(f) "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(g) "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(h) "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(i) "**Underlying Agreement**" shall mean Contract/Purchase Order # _____.

(j) "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. Changes in Law.

Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI.

Except as otherwise limited in this BAA, Business Associate shall be permitted to use or disclose PHI provided by or obtained by or obtained on behalf of Covered Entity to perform those functions, activities, or services for, or on behalf of, Covered Entity which are specified in Appendix A to this BAA, provided that such use or disclosure would not violate the HIPPA Rules if done by Covered Entity. Business Associate agrees to make uses, disclosures and requests for PHI consistent with Covered Entity's minimum policies and procedures.

4. Additional Purposes for Which Business Associate May Use or Disclose Information.

Business Associate shall not use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity for any other purposes except as required by law. Business Associate shall not use PHI to de-identify the information in accordance with 45 CFR § 164.514 (a)—(c) without the Covered Entity's express written authorization(s). Business

Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

5. Business Associate Obligations.

(a) **Limits on Use and Further Disclosure Established by Business Associate Agreement and Law**. Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of, Covered Entity shall not be further used or disclosed other than as permitted or required by BAA or as required by law.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this BAA that reasonably and appropriately protects the confidentiality, integrity, and availability of the PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity as required by Subpart C of 45 CFR Part 164. Appropriate safeguards shall include but are not limited to implementing:

- administrative safeguards required by 45 CFR § 164.308;
- physical safeguards as required by 45 CFR § 164.310;
- technical safeguards as required by 45 CFR § 164.312; and
- policies and procedures and document requirements as required by 45 CFR § 164.316.

(c) **Training and Guidance**. Business Associate shall provide annual training to relevant contractors, Subcontractors, employees, agents and representatives on how to prevent the improper use or disclosure of PHI. Business Associate shall also comply with annual guidance on the most effective and appropriate technical safeguards issued by the Secretary of Health and Human Services.

(d) **Reports of Improper Use or Disclosure or Breach**. Business Associate hereby agrees that it shall notify the Covered Entity's Project Officer and the Covered Entity's Legal Office within **two (2) days** of discovery of any use or disclosure of PHI not provided for or allowed by this BAA, including breaches of unsecured PHI as required by 45 CFR § 164.410. Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. Business Associate shall furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 CFR § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the **first day**

on which it is known to the Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.

(e) Business Associate agrees that if any of its employees, agents, contractors, subcontractors or representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information, Business Associate shall ensure that such employees, agents, contractors, subcontractors and representatives shall receive training on Business Associate's procedure for compliance with the HIPAA Rules. Business Associate Agrees that if any of its employees, agents, contractors, subcontractors or representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information in a manner not provided for in this BAA, Business Associate shall ensure that such employees, agents, contractors, subcontractors and representatives are sanctioned or prevented from accessing any PHI Business Associate receives from, or creates or receives on behalf of Covered Entity. Use or disclosure of PHI in a manner contrary to the terms of this BAA shall constitute a material breach of the Underlying Agreement.

(f) **Contractors, Subcontractors, Agents and Representatives**. In accordance with 45 CFR § 164.502(e)(1)(ii) and 45 CFR § 164.308(b)(2), if applicable, ensure that any contractors, subcontractors, agents and representatives that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. The existence of any contractors, subcontractors, agents and representatives shall not change the obligations of Business Associate to the Covered Entity under this BAA.

(g) **Reports of Security Incidents**. Business Associate hereby agrees that it shall notify, in writing, the Department's Project Officer within **two (2) days** of discovery of any Security Incident at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available.

(h) **Right of Access to PHI**. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within **10 business days** of receiving a written request from the Covered Entity or an authorized individual in accordance with the HIPAA Rules. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its contractors, subcontractors, agents or representatives, access to PHI, Business Associate shall notify Covered Entity of same within **five (5) business days**. Business Associate shall further conform with and meet all of the requirements of 45 CFR § 164.524.

(i) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a request from Covered Entity or from the individual for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available to the Covered Entity and incorporate the amendment to enable Covered Entity to comply with 45 CFR § 164.526. If any individual requests an amendment from Business Associate or its contractors, subcontractors, agents or representatives, Business Associate shall notify Covered Entity of same within **five (5) business days**.

(j) **Provide Accounting of Disclosures**. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 CFR § 164.528. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date which is **six (6) years** prior to the request. Business Associate shall make such record available to the individual or the Covered Entity within **10 business days** of a request for an accounting of disclosures and in accordance with 45 CFR § 164.528.

(k) **Access to Books and Records**. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, created or received by Business Associate on behalf of the Covered Entity, available to the Covered Entity and the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules.

(l) **Return or Destruction of PHI**. At termination of this BAA, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this BAA. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this BAA to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(m) **Maintenance of PHI**. Notwithstanding subsection 5(l) of this BAA, Business Associate and its contractors, subcontractors, agents and representatives shall retain all PHI throughout the term of the Underlying Agreement and shall continue to maintain the information required under subsection 5(j) of this BAA for a period of **six (6) years** after termination of the Underlying Agreement, unless Covered Entity and Business Associate agree otherwise.

(n) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this BAA or the HIPAA Rules. Business Associate further agrees to

mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this BAA or the Privacy Rule.

(o) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any contractor, Subcontractor, employee, agent and representative who violates this BAA or the HIPAA Rules.

(p) **Application of Civil and Criminal Penalties**. All Civil and Criminal Penalties under the HIPAA Rules shall apply to Business Associate's violation of any provision contained in the HIPAA Rules.

(q) **Breach Notification**. Business Associate shall comply with the Breach notification requirements of 45 CFR Part 164. In the event of a Breach requiring indemnification in accordance with subsection 5(v), below, Covered Entity may elect to directly comply with Breach notification requirements or require Business Associate to comply with all Breach notifications requirements of 45 CFR Part 164 on behalf of Covered Entity. If Covered Entity requires Business Associate to comply with Breach notification requirements, Business Associate shall provide Covered Entity with a detailed weekly, written report, starting one week following discovery of the Breach. The report shall include, at a minimum, Business Associate's progress regarding Breach notification and mitigation of the Breach. If Covered Entity elects to directly meet the requirements of 45 CFR Part 164, Business Associate shall be financially responsible to Covered Entity for all resulting costs and fees incurred by Covered Entity, including, but not limited to, labor, materials, or supplies. Covered Entity may at its sole option:

- Offset amounts otherwise due and payable to Business Associate under the Underlying Agreement; or
- Seek reimbursement of or direct payment to a third party of Covered Entity's costs and fees incurred under this subsection.

Business Associate shall make payment to Covered Entity (or a third party as applicable) within **30 days** from the date of Covered Entity's written notice to Business Associate.

(r) **Grounds for Breach**. Any non-compliance by Business Associate with this BAA or the HIPAA Rules will automatically be considered to be a breach of the Underlying Agreement.

(s) **Termination by Commonwealth**. Business Associate authorizes termination of this BAA or Underlying Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion that the Business Associate has violated a material term of this BAA.

(t) **Failure to Perform Obligations**. In the event Business Associate including its contractors, Subcontractors, agents and representatives fails, to perform its obligations under this BAA, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this BAA and applicable law.

(u) **Privacy Practices**. The Covered Entity will provide, and Business Associate shall immediately begin using and/or distributing to clients, any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date of this BAA, or as otherwise designated by the Program or Covered Entity. The Covered Entity retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change.

(v) **Indemnification**. Business Associate shall indemnify, defend and hold harmless Covered Entity from and all claims and actions, whether in law or equity, resulting from Business Associate's Breach or other violation of the HIPAA Rules (this includes but is not limited to Breach and violations by Business Associate's contractors, subcontractors, employees, agents and representatives). Additionally, Business Associate shall reimburse Covered Entity for any civil monetary penalties imposed on Covered Entity as a result of a Breach or violation cognizable under this subsection 5(v).

6. Obligations of Covered Entity.

(a) **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR § 164.520 (Appendix A to this BAA), as well as changes to such notice.

(b) **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) **Restrictions**. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR § 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

7. Survival.

The requirements, rights and obligations created by this BAA shall survive the termination of the Underlying Agreement.

Appendix A to Exhibit A,
Commonwealth of Pennsylvania Business Associate Agreement

Permitted Purposes for the Creation, Receipt, Maintenance, Transmission, Use and/or Disclosure of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of the Underlying Agreement.

2. Information to be disclosed to Business Associate: _____.

3. Use Shall Effectuate Purpose of Underlying Agreement: _____ may use and disclose PHI to the extent contemplated by the Underlying Agreement, and as permitted by law with Commonwealth approval.

EXHIBIT B

PA Supplier ID Number: _____

SOFTWARE/SERVICES LICENSE REQUIREMENTS AGREEMENT
BETWEEN
THE COMMONWEALTH OF PENNSYLVANIA,
ACTING BY AND THROUGH THE GOVERNOR'S OFFICE OF ADMINISTRATION
AND

_____

This Software/Services License Requirements Agreement ("Agreement") by and between _____ (Licensor) and the **Commonwealth of Pennsylvania**, acting by and through the **Governor's Office of Administration** (Commonwealth) is effective the date the Agreement has been fully executed by the Licensor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained.

1. Order of Precedence.

The terms and conditions of this Agreement supplement, and to the extent a conflict exists, supersede and take precedence over the terms and conditions of the attached [insert exhibits that are to be made part of this Agreement]. The parties agree that the terms of this Agreement supersede and take precedence over the terms included in any quote, purchase order, terms of any shrink-wrap agreement included with the Licensed Products, terms of any click through agreement included with the Licensed Products or any other terms purported to apply to the Licensed Products. The products specified in Attachment 1, along with support and services for said products, shall be referred to as "Licensed Products."

2. Enterprise Language.

(a) The parties agree that more than one agency of the Commonwealth ("Commonwealth Agency") may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Commonwealth Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Commonwealth Agency seeking to use the Licensed Products.

(b) The parties agree that, if the licensee is a "Commonwealth Agency" as defined by Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C. S. § 103, the terms and conditions of this Agreement apply to the procurement of Licensed Products made by the Commonwealth, and that the terms and conditions of this Agreement become part of the purchase order or other procurement document without further need for execution.

3. List of Licensed Products.

(a) Attached hereto and made a part of this Agreement by reference is Attachment 1, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Commonwealth, the list of Licensed Products on Attachment 1 may be updated by the Licensor providing the Commonwealth with a revised Attachment 1 that adds the new product to the list. The Commonwealth, in its sole discretion, may consent either via written communication directly to the Licensor or, if applicable, providing the Commonwealth's reseller with a copy of the Licensor's notification to update Attachment 1.

(b) No amendment will be required to add a new Licensed Product to the list. If, however, the Licensor desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

4. Choice of Law/Venue.

This Agreement shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. The courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof.

5. Indemnification/Immunity.

The Commonwealth does not have the authority to and shall not indemnify any entity. The Commonwealth agrees to pay for any loss, liability or expense, which arises out of or relates to the Commonwealth's acts or omissions with respect to its obligations hereunder, where a final determination of liability on the part of the Commonwealth is established by a court of law or where settlement has been agreed to by the Commonwealth. This provision shall not be construed to limit the Commonwealth's rights, claims or defenses that arise as a matter of law or pursuant to any other provision of this Agreement. No provision in this Agreement shall be construed to limit the sovereign immunity of the Commonwealth.

6. Patent, Copyright, Trademark and Trade Secret Protection.

(a) The Licensor shall, at its expense, defend, indemnify and hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States patents, copyrights, trademarks or trade dress, or for a misappropriation of a United States trade secret arising out of performance of this Agreement ("Claim"), including all Licensed Products provided by the Licensor. For the purposes of this Agreement, "indemnify and hold harmless" shall

mean the Licensor's specific, exclusive, and limited obligation to (a) pay any judgments, fines and penalties finally awarded by a court of competent jurisdiction, governmental/administrative body or any settlements reached pursuant to a Claim and (b) reimburse the Commonwealth for its reasonable administrative costs or expenses, including without limitation reasonable attorney's fees, it necessarily incurs in handling the Claim. The Commonwealth agrees to give the Licensor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act,* Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P. S. §§ 732-101—732-506, the Office of Attorney General ("OAG") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion, and under the terms the OAG deems appropriate, may delegate its right of defense of a Claim. If the OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of the Licensor made in the defense of and/or settlement of a Claim. The Licensor shall not, without the Commonwealth's consent, enter into any settlement agreement which (a) states or implies that the Commonwealth has engaged in any wrongful or improper activity other than the innocent use of the material which is the subject of the Claim, (b) requires the Commonwealth to perform or cease to perform any act or relinquish any right, other than to cease use of the material which is the subject of the Claim, or (c) requires the Commonwealth to make a payment which the Licensor is not obligated by this Agreement to pay on behalf of the Commonwealth. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Licensor that, in the event it requests that the Commonwealth provide support to the Licensor in defending any such Claim, the Licensor shall reimburse the Commonwealth for all necessary expenses (including attorneys' fees, if such are made necessary by the Licensor's request) incurred by the Commonwealth for such support. If the OAG does not delegate to the Licensor the authority to control the defense and settlement of a Claim, the Licensor's obligation under this section ceases. The Licensor, at its own expense, shall provide whatever cooperation the OAG requests in the defense of the suit.

(b) The Licensor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Licensor certifies that, in all respects applicable to this Agreement, it has exercised and will continue to exercise due diligence to ensure that all Licensed Products provided under this Agreement do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties.

(c) If the defense of a Claim and the authority to control any potential settlements thereof is delegated to the Licensor, the Licensor shall pay all damages and costs finally awarded therein against the Commonwealth or agreed to by Licensor in any settlement. If information and assistance are furnished by the Commonwealth at the Licensor's written request, it shall be at the Licensor's expense, but the responsibility for such expense shall be only that within the Licensor's written authorization.

(d) If, in the Licensor's opinion, the Licensed Products furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a misappropriation of trade secret, then without diminishing the Licensor's obligation to satisfy any final award, the Licensor may, at its option and expense:

- substitute functional equivalents for the alleged infringing Licensed Products; or
- obtain the rights for the Commonwealth to continue the use of such Licensed Products.

(e) If any of the Licensed Products provided by the Licensor are in such suit or proceeding held to constitute infringement and the use thereof is enjoined, the Licensor shall, at its own expense and at its option:

- procure the right to continue use of such infringing products;
- replace them with non-infringing items; or
- modify them so that they are no longer infringing.

(f) If use of the Licensed Products is enjoined and the Licensor is unable to do any of the preceding set forth in subsection (e) above, the Licensor agrees to, upon return of the Licensed Products, refund to the Commonwealth:

- the license fee paid for the infringing Licensed Products, less the amount for the period of usage of any software; and
- the pro-rated portion of any maintenance fees representing the time remaining in any period of services for which payment was made.

(g) The obligations of the Licensor under this section continue without time limit and survive the termination of this Agreement.

(h) Notwithstanding the above, the Licensor shall have no obligation under this section for:

- modification of any Licensed Products provided by the Commonwealth or a third party acting under the direction of the Commonwealth;
- any material provided by the Commonwealth to the Licensor and incorporated into, or used to prepare any Licensed Products;

- use of any Licensed Product after the Licensor recommends discontinuation because of possible or actual infringement and has provided one of the remedies under subsection (e) or subsection (f) above;

- use of any Licensed Products in other than its specified operating environment;

- the combination, operation, or use of the Licensed Products with other products, services, or deliverables not provided by the Licensor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Licensor did not provide;

- infringement of a non-Licensed Product alone;

- the Commonwealth's use of any Licensed Product beyond the scope contemplated by the Agreement; or

- the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Licensor at no charge.

(i) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Licensor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

7. Virus, Malicious, Mischievous or Destructive Programming.

(a) The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

(b) The Licensor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Licensor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Licensor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of any Licensed Products, the Licensor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

8. Limitation of Liability.

(a) The Licensor's liability to the Commonwealth under this Agreement shall be limited the total dollar amount of purchase orders issued for Licensed Products and services covered by this Agreement during the during the **12-month** period prior to the event giving rise to the damage claim. This limitation does not apply to damages:

- for bodily injury;
- for death;
- for intentional injury;
- to real property or tangible personal property for which the Licensor is legally liable;
- Under Section 6, Patent, Copyright, Trade Secret and Trademark Protection;
- for damages related to a breach of the security of a system maintained or managed by the Licensor, including the costs for notification, mitigation and credit monitoring services required due to such breach; or
- under Section 7, Virus, Malicious, Mischievous or Destructive Programming.

(b) In no event will the Licensor be liable for consequential, indirect, or incidental damages unless otherwise specified in the Agreement.

9. Payment.

The Commonwealth will make purchase and make payment through a reseller contract or another procurement document, which shall control with regard to payment amounts and provisions.

10. Termination.

(a) The Licensor may not terminate for non-payment of an order issued through a reseller contract or another procurement document that controls payment.

(b) The Commonwealth may terminate this Agreement without cause by giving the Licensor **30 calendar days'** prior written notice ("Notice of Termination") whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth ("Termination for Convenience").

11. Background Checks.

(a) Upon prior written request by the Commonwealth, the Licensor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to the Commonwealth's IT facilities, either through on site or remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access by an IT employee and annually thereafter.

(b) Before the Commonwealth will permit an employee access to the Commonwealth's facilities, the Licensor must provide written confirmation to the office designated by the applicable Commonwealth Agency that the background check has been conducted. If, at any time, it is discovered that an employee has a criminal record that includes a felony or misdemeanor involving terrorist threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Licensor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the Commonwealth Agency consents, in writing, prior to the access being provided. The Commonwealth Agency may withhold its consent at its sole discretion. Failure of the Licensor to comply with the terms of this subsection may result in the default of the Licensor under its Agreement with the Commonwealth.

(c) The Commonwealth specifically reserves the right to conduct background checks over and above that described herein.

(d) Access to certain Capitol Complex buildings and other state office buildings is controlled by means of card readers and secured visitors' entrances. Commonwealth contracted personnel who have regular and routine business in Commonwealth worksites may be issued a photo identification or access badge subject to the requirements of the applicable Commonwealth Agency and the Department of General Services set forth in Enclosure 3 of Commonwealth Management Directive 625.10 Amended, *Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings*. The requirements, policy and procedures include a processing fee payable by the Licensor for contracted personnel photo identification or access badges.

12. Confidentiality.

(a) Definition. "Confidential Information:"

- For the Commonwealth. All data and other information of or in the possession of the Commonwealth or any Commonwealth Agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party.

- For the Licensor. All information identified in writing by the Licensor as confidential or proprietary to the Licensor or its subcontractors.

(b) Confidential Information. All Confidential Information of or relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Agreement, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents, subcontractors and personnel and to the officers, agents, subcontractors and personnel of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Agreement; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Agreement by such officers, agents, subcontractors and personnel and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement imposing equally or more stringent requirements for data privacy and security. Except to the extent provided otherwise by any applicable law, the obligations of this subsection (b) shall not apply with respect to information which:

- is developed by the other party without violating the disclosing party's proprietary rights,

- is or becomes publicly known (other than through unauthorized disclosure),

- is disclosed by the owner of such information to a Third Party free of any obligation of confidentiality,

- is already known by such party without an obligation of confidentiality other than pursuant to this Agreement or any confidentiality contract entered into before the Effective Date of the Agreement between the Commonwealth and the Licensor, or

- is rightfully received by the disclosing party free of any obligation of confidentiality.

(c) Obligations. Each party shall:

- Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

- Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

- Use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights.

- Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

(d) Cost of compliance; required disclosure. Each party shall bear the cost it incurs as a result of compliance with this section. The obligations in this section shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such disclosure or order in a timeframe to allow the non-disclosing party to resist the disclosure or order).

(e) Submitting Confidential Information to the Commonwealth. The Licensor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare an un-redacted version of the appropriate document;

- Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret;

- Prepare a signed written statement that states:

  (1) the attached document contains confidential or proprietary information or trade secrets;

(2) the Licensor is submitting the document in both redacted and un-redacted format in accordance with Section 707(b) of the *Right-to-Know Law*, 65 P.S. § 67.707(b); and

(3) the Licensor is requesting that the document be considered exempt under Section 708(b)(11) of the *Right-to-Know Law*, 65 P.S. § 67.708(b)(11) from public records requests; and

- Submit the **two (2)** documents with the signed written statement to the Commonwealth.

(f) Confidential Information at termination. Upon expiration or termination of this Agreement, or a purchase order or other procurement document for Licensed Products governed by the terms of this Agreement, and at any other time at the written request of a party, the other party must promptly return to such party all of such party's Confidential Information and Data (and all copies of this information) that is in the other party's possession or control, in whatever form. With regard to the Commonwealth's Confidential Information and/or Data, the Licensor shall comply with the requirements of subsection (e).

(g) Not confidential. Additionally, neither the Agreement nor any pricing information related to the Agreement, nor purchase orders issued pursuant to the Agreement, will be deemed confidential.

13. Sensitive Information

(a) The Licensor shall not publish or otherwise disclose, except to the Commonwealth or the Licensor's subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

(b) The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Agreement for any purpose not connected with the parties' Agreement responsibilities.

(c) The Licensor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Agreement including by:

- Maintaining a valid and up to date registrations and certifications; and

- Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

14. Agency-specific Sensitive and Confidential Commonwealth Data (If applicable).

(a) The Licensor understands that its level of access may allow it to view or access highly sensitive and confidential Commonwealth and third party data. This data is subject to various state and federal laws and policies that vary from Commonwealth Agency to Commonwealth Agency, and from program to program within a Commonwealth Agency. If applicable, prior to the issuance of a purchase order or other procurement document for a Licensed Product or the deployment of a Licensed Product on any Commonwealth Agency's facilities, the Licensor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth Agency, including but not limited to, as necessary, Business Associate Agreements as required by the *Health Insurance Portability and Accountability Act* (HIPAA), as amended, a sample of which is attached hereto as Attachment 3. This sign-off document (a sample of which is attached hereto as Attachment 4), will include a description of the nature of the data which may be implicated based on the nature of the Licensor's access, and will incorporate the HIPAA Business Associate Agreement if it is applicable.

(b) The Licensor hereby certifies and warrants that, after being informed by the Commonwealth Agency of the nature of the data which may be implicated and prior to the installation of the Licensed Products), the Licensor is and shall remain compliant with all applicable state and federal law and policy regarding the data's protection, and with the requirements memorialized in every completed and signed Sign-Off document. Every sign-off document completed by a Commonwealth Agency and signed by at least one signatory of the Licensor authorized to bind the Licensor is valid and is hereby integrated and incorporated by reference into this Agreement.

(c) This section does not require a Commonwealth Agency to exhaustively list the law to which implicated data is subject; the Commonwealth Agency is obligated only to list the nature of the data implicated by the Licensor's access, to refer the Licensor to its privacy and security policies, and to specify requirements that are not otherwise inherent in compliance with law and policy.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Agreement and its Attachments and Exhibits having to do with data privacy and security, including but not limited to the requirement that the Licensor comply with Attachment 2, *Requirements for Non-Commonwealth Hosting Applications/Services*, and all applicable Commonwealth Information Technology Policies (ITPs), which can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx.

(e) The Licensor shall conduct additional background checks, in addition to those required in Section 11 of this Agreement, as may be required by a Commonwealth Agency in its sign-off documents. The Licensor shall educate and hold its agents, employees, contractors and subcontractors to standards at least as stringent as those

contained in this Agreement. The Licensor shall provide information regarding its agents, employees, contractors and subcontractors to the Commonwealth upon request.

15. Publicity/Advertisement.

The Licensor must obtain written Commonwealth approval prior to mentioning the Commonwealth or a Commonwealth agency in an advertisement, endorsement, or any other type of publicity. This includes the use of any trademark or logo.

16. Portability.

The parties agree that a Commonwealth Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Commonwealth or to a Commonwealth contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Commonwealth Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

17. Taxes-Federal, State and Local Taxes-Federal, State and Local.

(a) The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

(b) The only interest the Commonwealth is authorized to pay is in accordance with Act of December 13, 1982, P.L. 1155, No. 266, as amended, 72 P. S. § 1507, (relating to Interest Penalties on Commonwealth Accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to Interest Penalties for Late Payments).

18. Commonwealth Audit Responsibilities.

(a) The Commonwealth will maintain, and promptly provide to the Licensor upon its request, accurate records regarding use of the Licensed Product by or for the

Commonwealth. If the Commonwealth becomes aware of any unauthorized use of all or any part of the Licensed Product, the Commonwealth will notify the Licensor promptly, providing reasonable details. The limit of the Commonwealth's responsibility for use of the Licensed Products by more individuals than are permitted by the licensing terms applicable to the Licensed Products shall be to purchase additional licenses and Maintenance and Support (if applicable) for such Licensed Products through a reseller contract or another procurement document.

(b) The Commonwealth will perform a self-audit upon the request of the Licensor, which request may not occur more often than annually, and report any change in user count (hereinafter "True up number"). The Commonwealth shall notify the Licensor of the True up number no later than **45 calendar days** after the request that the Commonwealth perform a self-audit. If the user count has increased, the Commonwealth will make an additional purchase of the Licensed Products through a reseller contract or another procurement document, which is equivalent to the additional users. This section sets out the sole license audit right under this Agreement.

19. *Right-to-Know Law*.

The Pennsylvania *Right-to-Know Law*, Act of February 14, 2008, P.L. 6, No. 3, 65 P.S. §§ 67.101—3104 ("RTKL"), applies to this Agreement.

20. Third Party Software.

If the Licensed Product utilizes or includes third party software and other copyrighted material and is subject, therefore, to additional licensing terms, acknowledgements or disclaimers compliance with this Agreement constitutes compliance with those third-party terms. The parties agree that the Commonwealth, by acknowledging third party software, does not agree to any terms and conditions of the third party software agreements that are inconsistent with or supplemental to this Agreement.

21. Attorneys' Fees.

Each Party is responsible for their own ~~The Commonwealth will not pay~~ attorneys' fees. ~~incurred by or paid by the Licensor.~~

22. Controversies.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Agreement or a purchase order, the Licensor, within **six (6) months** after the claim accrues, must file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Licensor asserts a controversy exists. If the Licensor fails to file a claim or files an untimely claim, the Licensor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days**

thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, https://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

(b) If the Licensor or the contracting officer requests mediation and the other party agrees, the contracting officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the contracting officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the contracting officer and the Licensor. The contracting officer shall send a written determination to the Licensor. If the contracting officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The contracting officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Licensor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Licensor shall proceed diligently with the performance of the Agreement or purchase order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Licensor pursuant to the terms of the Agreement, purchase order or other procurement document.

23. Insurance.

(a) The Licensor shall maintain at its expense, and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

- Workers' Compensation Insurance for all of the employees engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

- Commercial general liability insurance providing coverage from claims for damages for personal injury, death (including bodily injury), sickness or disease, accidental death and damage to and property of others, including loss of use resulting from any property damage which may arise from the Licensor's operations under this Agreement, whether such operation be by the Licensor, its agent, contractor or subcontractor, or by anyone directly or

indirectly employed by either. The limits of such insurance shall be in an amount not less than $500,000 per person and $2,000,000 per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or supplies provided to the Commonwealth.

- Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of $2,000,000, per accident/occurrence/annual aggregate.

- Technology Products Liability/Professional Liability/Errors & Omissions Insurance in the aggregate amount of not less than $2,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Comprehensive crime insurance in an amount of not less than $5,000,000 per claim.

- Information Security and Privacy Liability Insurance including Privacy Notification Costs (including coverage for Technology Professional Liability if not covered under the Licensor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $3,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

(b) Certificate of Insurance. Prior to providing Licensed Products under this Agreement, and annually thereafter, the Licensor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days**' prior written notice has been received by the Commonwealth. Such cancellation or change shall not relieve the Licensor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Licensor agrees to maintain such insurance for the life of any applicable purchase order issued pursuant to the Agreement.

24. Federal Requirements.

If applicable, in addition to the requirements set forth in Section 14 of this Agreement, the Licensor must receive and sign off on particular federal requirements that a Commonwealth agency may be required to include when utilizing federal funds to procure the Licensed Products. This sign-off document, in addition to any applicable requirements of Section 14 of this Agreement, will include a description of the required federal provisions, along with the applicable forms necessary for the Licensor execute, as necessary. The sign-off document, along with attachments, must be attached to the purchase order.

25. Signatures.

The fully executed Agreement may not contain ink signatures by the Commonwealth. In that event, the Licensor understands and agrees that the receipt of an electronically-printed Agreement with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in the Agreement. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

26. Travel.

The Licensor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Agreement or Statement of Work. If not otherwise specified in the Agreement or Statement of Work, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

27. Entire Agreement.

This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter hereof, and supersedes and integrates all prior discussions, agreements and understandings pertaining thereto. No modification of this Agreement will be effective unless in writing and signed by both Parties. Other terms and conditions or additional terms and conditions included or referenced in the Licensor's quotations, invoices, business forms, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Licensor and not binding on the Commonwealth.

28. Notice.

Any written notice to any party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States

mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

29. Survival.

The termination or expiration of this Agreement will not affect any provisions of this Agreement which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, confidentiality, term and termination, effect of termination, intellectual property, license compliance, limitation of liability, indemnification and privacy.

30. Waiver.

Failure to enforce any provision will not constitute a waiver.

31. Severability.

If any provision is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.

32. Nonexclusive Remedy.

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.

33. Integration.

This Agreement, including all Exhibits, Attachments and referenced documents, and any Purchase Orders referencing this Agreement, constitutes the entire agreement between the parties. No agent, representative, employee or officer of the Commonwealth or of the Licensor has authority to make any statement, agreement, or representation, oral or written, in connection with this Agreement, which in any way can be deemed to modify, add to, or detract from, or otherwise change or alter its terms and conditions. No negotiations between the parties, nor any custom or usage, shall be permitted to modify or contradict any of the terms and conditions of this Agreement. No modifications, alterations, changes, or waiver to this Agreement or any of its terms shall be valid or binding unless accomplished by a written amendment executed by the parties.

IN WITNESS WHEREOF, the Parties to this Agreement have executed it, through their respective duly authorized representatives.

Witness:

_____
Signature Date

_____
Printed Name

_____
Title

Licensor:

_____
Signature Date

_____
Printed Name

_____
Title

If a corporation, the Chairman, President, Vice-President, Senior Vice-President, Executive Vice-President, Assistant Vice-President, Chief Executive Officer and Chief Operating Officer must sign; if a sole proprietor, then the owner must sign; if a general or limited partnership, a general partner must sign; if a limited liability company, then a member must sign, unless it is a managed by a manager, then the manager must sign; otherwise a resolution indicating authority to bind the corporation must be attached to this Agreement.

COMMONWEALTH OF PENNSYLVANIA

GOVERNOR'S OFFICE OF ADMINISTRATION

_____
See Section 25
Agency Head or Designee

APPROVED AS TO FORM AND LEGALITY:

_____
See Section 25
Office of Chief Counsel

_____
See Section 25
Office of General Counsel

_____
See Section 25
Office of Attorney General

APPROVED:

_____
See Section 25
Office of the Budget, Office of Comptroller Operations

ATTACHMENT 1

LIST OF LICENSED PRODUCTS

With the consent of the Commonwealth, the Licensor may add additional Licensed Products to this attachment by providing Commonwealth with a new copy of this Attachment 1.

Licensed Product:

The Licensed Product includes (list all titles covered by this agreement):

ATTACHMENT 2
Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this Attachment 2 is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements.

1. The Licensor or its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Quote and Statement of Work.

2. The Licensor shall provide secure access to applicable levels of users via the internet.

3. The Licensor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4. The Licensor or its subcontractors shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements.

5. The Licensor shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **two (2) business days**. In the event of any impermissible disclosure unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one (1) hour** of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. The Licensor or the Licensor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and within at least **three (3) business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Licensor or the Licensor's subcontractor shall locate servers in a climate-controlled environment. The Licensor or the Licensor's contractor shall house all servers and equipment in an operational environment that meets industry standards

including climate control, fire and security hazard detection, electrical needs, and physical security.

9. The Licensor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The Licensor shall completely test and apply patches for all third-party software products in the server environment before release.

11. The Licensor shall comply with Attachment 2-B, SOC Reporting Requirements.

B. Security Requirements.

1. The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense on an annual basis.

2. The Licensor shall comply with the Commonwealth's directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.

3. The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4. The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The Licensor shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. The Licensor shall limit access to Commonwealth-specific systems and services and provide access only to those staff that must have access to provide services proposed.

7. The Licensor shall provide the Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in Attachment 2-A, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

C. Data Storage.

1. The Licensor shall store all Commonwealth data in the United States.

2. The Licensor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk. The Licensor shall protect their operational systems with applicable anti-virus, host

intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Licensor shall be solely responsible for applicable data storage required.

4. The Licensor shall take all commercially viable and applicable measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

5. The Licensor agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or a Licensor-owned electronic device.

6. The Licensor shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

D. Adherence to Policy.

1. The Licensor's support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Licensor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment 2-A.

3. The Licensor shall comply with all pertinent federal and state privacy regulations.

E. Closeout.

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency to the Commonwealth Software Reseller within **sixty (60) days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

ATTACHMENT 2-A

Information Technology Policies (ITPs)
for
Outsourced/Licensor(s)-hosted Solutions

ITP Number-Name	Policy Link
ITP_ACC001-Accessibility Policy	https://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030-Active Directory Architecture	https://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007-Enterprise Service Catalog	https://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010-Business Process Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS011-Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_bus011.pdf
ITP_BUS012-Artificial Intelligence General Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000-Enterprise Data and Information Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001-Database Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006-Commonwealth County Code Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009-e-Discovery Technology Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010-Business Intelligence Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011-Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012-Dashboard Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001-The Life Cycle of Records: General Policy Statement	https://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004-Management of Web Records	https://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005-System Design Review of Electronic Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006-Electronic Document Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1-Electronic Commerce Formats and Standards	https://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2-Electronic Commerce Interface Guidelines	https://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006-Business Engine Rules	https://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004-Internet Protocol Address Standards	https://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005-Commonwealth External and Internal Domain Name Services (DNS)	https://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001-Commonwealth of Pennsylvania Electronic Information Privacy Policy	https://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000-Information Security Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC002-Internet Accessible Proxy Servers and Services	https://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003-Enterprise Security Auditing and Monitoring	https://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004-Enterprise Web Application Firewall	https://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006-Commonwealth of Pennsylvania Electronic Signature Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007-Minimum Standards for IDs, Passwords and Multi-Factor Authentication	https://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008-Enterprise E-mail Encryption	https://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf

ITP Number-Name	Policy Link
ITP_SEC009-Minimum Contractor Background Checks Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf
ITP_SEC010-Virtual Private Network Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf
ITP_SEC011-Enterprise Policy and Software Standards for Agency Firewalls	https://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC013-Identity Protection and Access Management (IPAM) Architectural Standard and Identity Management Services	https://www.oa.pa.gov/Policies/Documents/itp_sec013.pdf
ITP_SEC015-Data Cleansing	https://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC017-Copa Policy for Credit Card Use for e-Government	https://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019-Policy and Procedures for Protecting Commonwealth Electronic Data	https://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC020-Encryption Standards for Data at Rest	https://www.oa.pa.gov/Policies/Documents/itp_sec020.pdf
ITP_SEC021-Security Information and Event Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023-Information Technology Security Assessment and Testing Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024-IT Security Incident Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025-Proper Use and Disclosure of Personally Identifiable Information (PII)	https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029-Physical Security Policy for IT Resources	https://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031-Encryption Standards for Data in Transit	https://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032-Enterprise Data Loss Prevention (DLP) Compliance Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034-Enterprise Firewall Rule Set	https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC037-Identity Proofing of Online Users	https://www.oa.pa.gov/Policies/Documents/itp_sec037.pdf
ITP_SEC038-Commonwealth Data Center Privileged User IAM Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP_SFT000-Software Development Life Cycle (SDLC) Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001-Software Licensing	https://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002-Commonwealth of PA Website Standards	https://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003-Geospatial Enterprise Service Architecture	https://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004-Geospatial Information Systems (GIS)	https://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005-Managed File Transfer (MFT)	https://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007-Office Productivity Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008-Enterprise Resource Planning (ERP) Management	https://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009-Application Development	https://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003-Off-Site Storage for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004-Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006-Commonwealth IT Resources Patching Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008-Server Virtualization Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010-Enterprise Services Maintenance Scheduling	https://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

ATTACHMENT 2-B

SOC Reporting Requirements

(a) Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to, engage, on an annual basis, an independent auditing firm to conduct each the following:

(i) A SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions;

(ii) A SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access or contain Commonwealth Data; and

(iii) A SOC for Cybersecurity report with respect to controls used by the Contractor setting forth the description and effectiveness of the Contractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

Pennsylvania's fiscal year begins July 1 and ends on June 30. Audits shall be submitted annually no later than July 31 of the current year. All reports shall reflect the conduct of the Contractor during the **12 months** of the Commonwealth's previous fiscal year, unless otherwise agreed to in writing by the Commonwealth.

(b) SOC 2 Type II report reports shall address the following:

(i) Security of Information and Systems;

(ii) Availability of Information and Systems;

(iii) Processing Integrity;

(iv) Confidentiality;

(v) Privacy; and

(vi) If applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

(c) At the request of the Commonwealth, the Contractor shall complete additional SOC for Cybersecurity audits in the event:

(i) repeated non-conformities are identified in any SOC report required by subsection (a); or

(ii) if the Contractor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.);

The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

(d) The Commonwealth may specify other or additional standards, certifications or audits it requires under any Purchase Orders or within an ITP.

(e) The Contractor shall adhere to SSAE 18 audit standards. The Contractor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Contractor shall comply with such updates which shall be reflected in the next annual report.

(f) In the event an audit reveals any non-conformity to SSAE standards, the Contractor shall provide the Commonwealth, within **45 calendar days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity. The corrective action plan shall provide, in detail:

(i) clear responsibilities of the personnel designated to resolve the non-conformity;

(ii) the remedial action to be taken by the Contractor or its subcontractor(s);

(iii) the dates when each remedial action is to be implemented; and

(iv) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

(g) The Commonwealth may in its sole discretion agree, in writing, to accept alternative and equivalent reports or certifications in lieu of a SOC report.

ATTACHMENT 3

COMMONWEALTH OF PENNSYLVANIA
***SAMPLE* BUSINESS ASSOCIATE AGREEMENT**
(Business Associate Agreements as provided by Agencies may differ)

WHEREAS, the _____ (Covered Entity) and _____(Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be handled, used or disclosed only in accordance with this Agreement, and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(c) "**HIPAA**" shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.

(d) "**HITECH Act**" shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV

of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(e) "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(f) "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(g) "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(h) "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. Changes in Law.

Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI.

The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

_____
_____
_____
_____
_____
_____
_____
_____
_____

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

4. BUSINESS ASSOCIATE OBLIGATIONS.

(a) **Limits on Use and Further Disclosure**. Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity other than as permitted or required by this Addendum, as requested by Covered Entity, or as required by law and agency guidance.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

(c) **Reports of Improper Use or Disclosure**. Business Associate hereby agrees that it shall report to _____at _____, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

(d) **Reports on Security Incidents**. In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* ("HITECH Act"), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____, **within two (2) days** of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.

(e) **Subcontractors and Agents**. At any time PHI is provided or made available to Business Associate subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

(f) **Right of Access to PHI**. Business Associate shall allow, for any PHI maintained in a designated record set, Covered Entity to have access to and copy an individual's PHI within **five (5) business days** of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and Covered Entity. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within **five (5) business days**. Business Associate shall further conform with all of the requirements of 45 C.F.R. § 164.524 and other applicable laws, including the HITECH Act, as amended, related regulations and agency guidance. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(f).

(g) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a written request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act , as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within **five (5) business days**.

(h) **Provide Accounting of Disclosures**. Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended) in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the Covered Entity within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(h).

(i) **Requests for Restriction**. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health

plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) **Access to Books and Records**. Business Associate shall make its internal practices, books and records relating to the use or disclosure of PHI received from, or created or received, by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.

(k) **Return or Destruction of PHI**. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(l) **Maintenance of PHI**. Notwithstanding subsection 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.

(n) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.

(o) **Grounds for Breach**. Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-

compliance. Commonwealth may elect to terminate Business Associate's contract for such breach.

(p) **Termination by Commonwealth**. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

(q) **Failure to Perform Obligations**. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.

(r) **Privacy Practices**. Covered Entity will provide Business Associate with all applicable forms, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

5. OBLIGATIONS OF COVERED ENTITY.

(a) **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change.

(b) **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware if such changes affect Business Associate's permitted or required uses and disclosures.

(c) **Restrictions**. Covered Entity shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) **Requests**. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule, all as amended, if done by Covered Entity.

6. MISCELLANEOUS.

(a) **Regulatory References**. A reference in this Addendum to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.

(b) **Amendment**. The parties agree to take such action as is necessary to amend this Addendum from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.

(c) **Conflicts**. In the event that any terms of this Agreement are inconsistent with the terms of the Agreement, then the terms of this Agreement shall control.

ATTACHMENT 4

Sign-Off Document No. ____, under Agreement No. _____
Between
[Licensor_____] and the Commonwealth of PA, [Agency]

[Licensor_____] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Software/Services License Requirements Agreement No. _____ between the Commonwealth and _____ (Licensor), and is subject to the terms of that Agreement.

1. Scope of Deployment (need not be entire agency):

1. Nature of Data implicated or potentially implicated:

2. Agency Policies to which Licensor. is subject (incorporated by reference):

3. Background checks (describe if necessary):

4. Additional requirements (describe with specificity):

5. Is Licensor a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person Signature and Date: _____

[Licensor_____]
Authorized Signatory and Date: _____

EXHIBIT C

Sign-Off Document No. ____, under Agreement No. _____
Between
[Contractor_____] and the Commonwealth of PA, [Agency]

[Contractor_____] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Agreement No. _____ between the Commonwealth and _____ (Contractor), and is subject to the terms of that Agreement.

1. Scope of Deployment (need not be entire agency):

2. Nature of Data implicated or potentially implicated:

3. Agency Policies to which Contractor is subject (incorporated by reference):

4. Background checks (describe if necessary):

5. Additional requirements (describe with specificity):

6. Is Contractor a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person Signature and Date: _____

[Contractor_____]
Authorized Signatory and Date: _____

APPENDIX H
Service Level Agreements Vendor Hosted

Performance Measure	Performance Target	Definition	Calculation	Frequency of Review	
Deliverable(s) completed on time	100%	Deliverables completed and accepted by the Commonwealth by date agreed to in the project schedule. Commonwealth requires two (2) business days to complete the approval process.	Deliverable due date, completion and acceptance by 4:00 PM ET. (Acceptance Date – Due Date) = Result If Result is >0 Then: (Result x $500)= Service Credit	Continual	$500 p beginn the sc 100%
Severity Level* 1 and 2: Within 30 minutes during core and 60 minutes during non-core processing hours.	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 30 minutes by a live agent during the core business of 8:00 AM to 5:00 PM ET and within 30 minutes of the next business day if a request is logged during non-core hours.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo
Severity Level* 3 and 4: Within 60 minutes during core processing hours. Within 60 minutes of the next business day during non-core processing hours	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 60 minutes by a live agent during the core business of 8:00 AM to 5:00 PM ET and within 60 minutes of the next business day if a request is logged during non-core hours.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo
Severity Level* 1 and 2: Within 30 minutes during core pre-election hours Within 30 minutes of the next business day during	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 30 minutes by a live agent during the core business of 7:30 AM to 8:00 PM ET and within 30 minutes of the next business day if a request is logged during non-core hours on pre-election day hours.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo

non-core pre-election hours.					
Severity Level* 3 and 4: Within 60 minutes during core pre-election hours. Within 60 minutes of the next business day during non-core pre-election hours	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 60 minutes by a live agent during the core business of 8:00 AM to 8:00 PM ET and within 60 minutes of the next business day if a request is logged during non-core hours.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo
Severity Level* 1 and 2: Within 15 minutes during core Election Day hours	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 15 minutes by a live agent during the core business of 6:30 AM to 2:00 AM ET on election days, or as requested.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo
Severity Level* 3 and 4: Within 45 minutes during core Election Day hours.	100%	Any support request not answered by a live agent (ex. Phone, voicemail, chat, etc.) must be responded to within 45 minutes by a live agent during the core business of 6:30 AM to 2:00 AM ET (next day) on election days, or as requested.	Time from the initial contact until the response is received. (# of occurrences where the performance target is not met within a month)x(0.05)x(monthly Solution Maintenance and Support Cost) = monthly service credit	Monthly	5% Re cost fo Suppo
Severity Level* 1: Circumvention, Resolution within 4 hours	100%	Amount of time to resolve technical defects reported following a new release, patch or system upgrade in production based on the severity level of the defect. Defect will be circumvented, resolved or a rollback within 4 hours unless otherwise agreed to by DOS.	Time of defect reported until time of defect resolution – allotted amount of time for resolution based on severity level (# of occurrences where the performance target is not met within a month)x(1000) = monthly service credit	Monthly	$1000 additi until r
Severity Level* 2: Circumvention, Resolution within 48 hours	100%	Amount of time to resolve technical defects reported following a new release, patch or system upgrade in production based on the severity level of the defect.	Time of defect reported until time of defect resolution – allotted amount of time for resolution based on severity level	Monthly	$500 f additi beyon allotte

		Defect will be circumvented, resolved or a rollback within 48 hours unless otherwise agreed to by DOS.	(# of occurrences where the performance target is not met within a month)x(1000) = monthly service credit		
Severity Level* 3 and 4: Circumvention or Resolution by agreed upon release date	100%	Amount of time to resolve technical defects reported following a new release, patch or system upgrade in production based on the severity level of the defect. Date Commonwealth agrees, to with the selected Offeror to, circumvent or resolve a defect.	Day of the agreed upon release date to the date defect is resolved. (Actual Resolution Date - Agreed Upon Resolution Date)x(500) = monthly service credit	Monthly	$500 f additi beyon resolu resolu
>= 99.9% during core business hours defined as 8:00 AM to 5:00 PM Eastern Time (EST or EDT as applicable), excluding Commonwealth holidays, and weekends as requested.	100%	This service level measures the percentage of time the solution is available during the applicable measurement window. This measurement is by application, not by server instance. Availability is defined by whether the application is available to all users of the solution. During the Operations Maintenance and Support phases of the project, the accumulation of more than 0.1% of system down time, attributable to the Offeror, due to one or more incidents.	The Service Level calculation for solution Availability is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the solution, with the result expressed as a percentage. 1 – ((sum of minutes the application is actually available) / (sum of minutes the solution is scheduled to be available)) expressed as a percentage	Monthly	5% Re cost fo Suppo Incide failure perfor month
Within 1 hour	100%	The selected Offeror must notify the Commonwealth of any system unavailability within one (1) hour of discovering or receiving notice of system unavailability.	Time from discovering or receiving notice of system unavailability until notification is sent to the Commonwealth	Continual	one (1 Maint incide
Incident Resolution within 30 minutes during core business for critical time periods including to election day, pre-election- and other deadlines. 60 minutes within non-core business hours. During non-critical time periods, normal business	100%	Amount of time needed to circumvent or resolve a reported problem or incident unless otherwise approved by DOS. An incident is an unplanned or reduction in service.	The Service Level calculation for "Resolution Time for problems and incidents – Severity Level 1" is the total number of Incidents that are, or become, Severity Level 1 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 1 during the applicable Measurement Window, with the result expressed as a percentage.	Monthly	one (1 Maint incide Incide failure perfor month

operations resolution within 4 hours.			(Number of Severity Level 1 Incidents Resolved within Limit) / (Total Number of Severity Level 1 Incidents)		
Incident Resolution within 60 minutes during core business for critical time periods including to election day, pre-election- and other deadlines. 90 minutes within non-core business hours. During non-critical time periods, normal business operations resolution within 48 hours.	100%	Amount of time needed to circumvent or resolve a reported problem or incident unless otherwise approved by DOS. An incident is an unplanned or reduction in service.	The Service Level calculation for "Resolution Time for problems and incidents – Severity Level 2" is the total number of Incidents that are, or become, Severity Level 2 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 2 during the applicable Measurement Window, with the result expressed as a percentage. (Number of Severity Level 2 Incidents Resolved within Limit) / (Total Number of Severity Level 2 Incidents)	Monthly	one (1 Maint incide Incide failure perfor month
Incident Resolution by agreed upon date.	100%	Amount of time needed to circumvent or resolve a reported problem or incident unless otherwise approved by DOS. An incident is an unplanned or reduction in service.	The Service Level calculation for "Resolution Time for problems and incidents – Severity Level 3" is the total number of Incidents that are, or become, Severity Level 3 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 3 during the applicable Measurement Window, with the result expressed as a percentage. (Number of Severity Level 3 Incidents Resolved within Limit) / (Total Number of Severity Level 3 Incidents)	Monthly	one (1 Maint incide Incide failure perfor month
Notification prior to System Upgrades or Maintenance Windows	100%	Amount of time to notify the Commonwealth of system maintenance or upgrade windows prior to release. Any scheduled upgrade or maintenance windows scheduled during non-blackout periods, unless it's emergency maintenance, must be communicated 14 days prior to release.	Deliverable due date, completion and acceptance by 5:00 PM ET. (Due Date – Notification Date Date) = Result If Result is >0 Then: (Result x $500)= Service Credit	Continual	$500 p beginn the sc 100%
Notification of Intrusion or Breach	100%	Offeror agrees to notify the Commonwealth within 2) hours of a known cyber intrusion or breach incident of any Offeror platforms or services.	Deliverable due date, completion and acceptance by 5:00 PM ET. (Due Date – Notification Date Date) = Result	Continual	$500 p subse witho 100%

Notification within two (2) hours of a known event			If Result is >0 Then: (Result x $500)= Service Credit		
Scheduled downtimes for production vendor Business Services will not exceed 12 hours per month without prior approval from DOS	100%	Scheduled downtimes for production vendor Business services will be communicated in writing to client with a minimum of five (5) business days of notice. • The DOS has the right to request a scheduled maintenance be moved, to prevent business impact, within 1 business day of being notified. Scheduled downtimes for non-production vendor Business Services will be coordinated to minimize impact to the Client.	Scheduled downtime of the solution without 5 business days notification to the Department.	Continual	$500 f appro
Recovery of the production system during a disaster situation	Production Recovery Time Objective is 4 hours Production Recovery Point Objective is 8 hours	Times from the start of the disaster to when the production system is available to users in the secondary data center.	Time of disaster recovery declaration until time of available production system in the secondary data center. (# of hours greater than the four (4) hour objective)	Continual	$500 f additi beyon object
95% of all production users transactions will complete in <=2 seconds.	Transaction completing in >2 seconds shall be considered degraded	Excludes Reports, batch job processing, interfaces (transactions with call-outs to external systems), web publishing, logging in (including single sign on), and whitelisted transactions.		Monthly	
95% of backups completed on time		Backups includes, but are not limited to, device configurations, system configurations, applications configurations, user accounts, user permissions, application data, CRM records, images, and documents within the application. This includes; • Full backup once a week • Incremental backup every night that is full is not running • Hourly SQL Server transaction log backups	Time of backup – the backup deadline.	Monthly	$500 f additi beyon
Data Feed Interruptions Due to Selected Offeror	100%	Amount of time to begin remediation of a facility data feed. The target is within 1 business day after data feed interruption is discovered.	Date of remediation of data feed – (Date of disruption discovery + one (1) business day) = number of days for remediation	Continual	1.0% c charge
No more than 5% of the key personnel, and no more than 20% of the overall Offeror staff		% of key staff and % of overall staff replaced per year.	Number of key personnel replaced/number of key personnel assigned to the project.	Annual	5% Re cost fo Suppo

assigned to this project, may be substituted per year.					
Due with the release closeout report		The time required for the selected Offeror to deliver the final approved release associated documentation.	Time from release implementation until the delivery of release associated documentation.	Per Release	1% of per bu
Incidents caused by Changes	98%	Offeror shall deliver defect-free changes where 98% of implemented changes are delivered with no defects being determined.	Total number of changes that are not associated with any Defect within warranty period divided by Total number of changes where warranty period expires within such month multiplied by 100. = percentage of Defect-free Changes during such month	Monthly	1% of per bu
Solution Invoicing	100%	100% of invoices submitted on time that contain no errors in billing calculation and correct adjustment to align with any service credits that may be applicable. Invoice is submitted on time without errors to measure compliance.	For each identified invoice error, a $500 service credit shall be awarded to DOS.	Monthly	$500 f
Annual Vulnerability Testing	100%	[to complete an annual vulnerability assessment each calendar year]		Annual	5% Re cost fo Suppo

lth may request a Corrective Action Plan (CAP), at its sole discretion, based on the selected Offeror's non-compliance with the SLAs as agreed upon.

lth shall not invoke more than one (1) SLA if more than one (1) SLA is in non-compliance for a single incident.

hall mean an amount equal to the pro-rata annual recurring service charges (i.e., all annual recurring charges) for one (1) day of Service.

Category	Description
Critical	A "show stopper"; a critical system failure; no further processing is possible; users unable to perform work; no acceptable work-around, alternative, or bypass exists.
Major	Processing is severely impacted; users are unable to proceed with selected function or dependents; software does not operate as specified; a major function or feature is missing or not functioning which causes a degradation in service; inaccurate or incorrect data provided to customers; no acceptable work-around, alternative, or bypass is available.
Minor	A component, minor function, or procedure is impaired (down, disabled, incorrect) however processing can continue. A mutually agreed workaround, alternative, or bypass is available.

APPENDIX H

Service Level Agreements Vendor Hosted

Category	Description
Cosmetic	Minor cosmetic change is required, a superficial error with no effect on operations.

d Election day support:

tion support begins approximately 5 weeks prior to election day with extended hours Monday-Friday. Saturday hours begin approximately 4 weeks prior to election day.

day support commences on election day and completes on the following morning at approximately 2:00AM EST. The call center activities generally conclude at 8:00 PM EST whe

vania.

nded pre-election

APPENDIX I

CUSTOMER SERVICE TRANSFORMATION DESIGN PRINCIPLES AND REQUIREMENTS

1. Keystone Login provides:

    a. A single online destination for services:

    A single online destination will enable citizens and Business Partners to locate services and conduct business in the Commonwealth, even if they do not know which agency to contact. Citizens and Business Partners can still navigate directly to services on agency websites, if they wish.

    Offerors must be able to integrate with the single online destination, starting with PA.GOV. The selected Offeror shall be able to receive and validate the credentials of a citizen or Business Partner that were previously authenticated from an active session. This process is further defined below in design principle 2 - secure access to services through a single login.

    b. Secure access to services through a single login:

    The Commonwealth implemented a single login system known as Keystone Login. The purpose of Keystone Login is to provide a consistent and secure approach to account administration. The Keystone Login offers citizens and Business Partners a single online point of access to services offered by multiple Commonwealth agencies or other Business Partners. It is critical that by using Keystone Login any citizen or Business Partner can work with any Commonwealth agency or other Business Partner through the Commonwealth's external facing applications using a single login credential.

    The consistent and modern authentication standards available through Keystone Login will increase convenience for citizens and Business Partners by simplifying account management and eliminating the need to remember multiple usernames and passwords, while also strengthening the Commonwealth's security posture.

    In addition, Keystone Login provides the ability for a citizen or Business Partner to create a single profile managed by Keystone Login.

    The selected Offeror shall register with and utilize the Commonwealth's Keystone Login.

APPENDIX I

CUSTOMER SERVICE TRANSFORMATION DESIGN PRINCIPLES AND REQUIREMENTS

Applications that utilize Keystone Login can leverage authentication methods through one of the following approaches; (1) via a series of Application Programming Interfaces ("APIs"), or (2) as a redirect to the Keystone Login Portal. A detailed Developer Integration Guide will be provided to the selected Offeror, however, to aid in determining the level of effort, a summary version of the Developer Integration Guide and the Keystone Login Branding Guidelines are available at the following location: http://keystonelogindevelopers.pa.gov.

The summary version of the Developer Integration Guide and the Keystone Login Branding Guidelines should be reviewed by the Offerors prior to responding to this RFP to ensure the Offerors understand the mandatory APIs and services to be made available to citizens and Business Partners.

The Offerors shall include in their proposals an acknowledgement that they will utilize the Keystone Login. If the Offeror requires any additional information to verify the identification of citizens or Business Partners through the authentication process provided by Keystone Login, the Offeror must identify the additional required information in its proposal.

c. If the selected Offeror will be responsible for helpdesk calls from application users, Offeror shall comply with the following:

The selected Offeror is expected to provide Tier 1 Helpdesk support. Keystone Login provides an internal admin dashboard designed to provide Helpdesk information to aid a caller with several Tier 1 level tasks. This is a secure internal administration site; hence, the selected Offeror will need a COPA account, along with VPN in order to access this site and be provided access by the Commonwealth. The dashboard provides the following information:

Exception Logs: A log of all the errors that occur in the Keystone Login site, calls to Keystone Login APIs, and the Admin site. The list can be searched and filtered by different parameters (User Name, Email Address, Start Date, End Date, Agency, or Application). Returns: ID, Log Date, User Name, User Email, Application Code, Message, Method, File Path, Line Number and Stack Trace.

User Logs: A log of all user activity. The list can be searched and filtered by different parameters (User Name, Email Address, Start Date, End Date, Agency, or Application). Returns: ID, Log Date, User Name, User Email, Application Code, User Event Type and Message.

Search: Used for searching users in Commonwealth domains. Search also provides the ability to edit Keystone Login accounts, unlock accounts when locked, change or reset passwords. User Search: Username, Email address, first name, last name, phone or domain. Returns: Name, User Name, Domain with buttons to see Details, User Logs, Exception Logs, Reset Password, Change Password, Edit, or Social Logins.

2. A consistent and user-friendly online experience across all services:

A common look and feel increases trust by enabling citizens and Business Partners to easily recognize official services provided by the Commonwealth. This also includes ensuring that online services and information are accessible to all citizens and Business Partners, regardless of ability.

Offerors shall acknowledge compliance with the Commonwealth's web site and mobile application design standards. Refer to the Commonwealth Information Technology Policies (ITPs) SFT002 – Commonwealth of PA Website Standards, NET005 - Commonwealth External and Internal Domain Name Services (DNS), and SFT009 – Application Development.

Offerors must acknowledge and demonstrate compliance to relevant federal, state and local laws, regulations, rules and legislation, including, but not limited to:

- Title III of the Americans with Disabilities Act (ADA) which prohibits discrimination on the basis of disability;
- Section 508 Amendment to the Rehabilitation Act of 1973 which requires all Federal agencies' electronic and information technology to be accessible to those with disabilities; and
- Section 504 of the Rehabilitation Act which prohibits discrimination on the basis of disability for entities receiving federal funds.

In addition, Offerors must acknowledge compliance with the Web Content Accessibility Guidelines (WCAG) 2.0, which are industry standards. The

selected Offeror must provide quarterly reports that demonstrate compliance with WCAG. Refer to the Commonwealth Information Technology Policy (ITP) ACC001 – Information Technology Accessibility Policy for additional information.

3. A consolidated and streamlined digital footprint:

   The Commonwealth is looking to streamline its online presence and make information easier to find by eliminating or consolidating small, outdated or low traffic Commonwealth websites.

   The selected Offerors must use the PA.GOV domain for proposed websites. By using PA.GOV, citizens and Business Partners will know that they are utilizing official services from the Commonwealth.

4. Continuous improvement through customer feedback:

   The Commonwealth will be collecting feedback from our citizen and Business Partners regarding the Customer Service Transformation. The Commonwealth may use the feedback to identify new opportunities to improve and innovate services.

   The selected Offerors shall have the ability to collect satisfaction and feedback related data from citizens and Business Partners.

5. A single phone number to direct citizens to the services they are seeking:

   The Commonwealth intends to make it easier for citizens and Business Partners to find the services they are seeking by calling a single Commonwealth phone number. Citizens and Business Partners may still contact agencies directly through existing call centers and phone numbers, if they wish.

   The selected Offeror will be expected to collaborate with this initiative where appropriate.

APPENDIX J
Support Hours and Activity

BEST, BEN, and BCFCE Support Hours:

Hours of Operation		
Normal Core Business Hours:	Monday – Friday	8:00 AM – 5:00 PM Eastern Time (EST)
*Pre-Election Core Business Hours:	Monday – Friday Saturday	7:30 AM – 8:00 PM EST 9:00 AM – 5:00PM EST
**Election Day Core Business Hours:	Tuesday into Wednesday	6:30 AM – 2:00 AM EST
***Petition Filing Core Business Hours:	Monday – Friday	7:30 AM – 5:00PM EST, except for Petition Filing Closing which may end at 7:00 PM EST

Commonwealth holidays:
The Commonwealth holiday calendar (https://www.budget.pa.gov/Services/ForAgencies/Payroll/Pages/Holiday-and-Pay-Calendars.aspx) should be used as a baseline calendar. There will be certain holidays where County Election Offices are open during Commonwealth holidays. For these few instances, the vendor will be required to provide Tier 1 support, as requested.

Pre-election and Election day support:

- Pre-election support begins approximately 5 weeks prior to election day with extended hours Monday-Friday. Saturday hours begin approximately 4 weeks prior to election day.
- Election day support commences on election day and completes on the following morning at approximately 2:00AM EST. The call center activities generally conclude at 8:00 PM EST when polls close in Pennsylvania.
- All extended pre-election and election day extended hours are completed on the day after the election.

Petition Filing support:
Petition Filing support will begin with the "First day to circulate and file nomination petitions" and end with the "Last day to circulate and file nomination petitions" per the official PA Election calendar. All work days will follow the timeframes noted above, except the closing date may extend up until ~ 7:00 PM to allow all potential candidates in line at 5:00PM to be properly processed.

Call Center Activity:

- Currently, several mechanisms exist for call center notifications for our users (e.g., DOS, county election officials, public technical assistance)
    - A toll-free number exists for all users including the public. That number is 1-866-472-7873.

- A resource account exists for all users including the public. That resource account is RA-SURE_helpdesk@pa.gov.
- Help Desk support also utilizes Skype for Business to chat with DOS users. The Skype for Business accounts are provided by the Commonwealth.

- Since May 2018, more than 10,000 service requests have been logged by our Tier 1 support into Service NOW. Approximately 80% have been resolved on the initial call. Roughly 20% require escalation to our Tier 2 or Tier 3 support teams.

Average Daily Activity	**Normal Business Cycles**
Call Volumes	1,300 monthly avg.
Email Volumes	50-150 daily avg.

Call volumes are greatest during the hours of 8:30 AM- 11:30 AM and 2:00 PM – 3:00 PM ET, Monday through Friday, including during the election cycles.

Average Election Volumes	**2015 Cycle Avg. (April – June)**	**2015 Cycle Avg. (Oct – Dec)**	**2016 Cycle Avg. (Mar – May)**	**2016 Cycle Avg. (Oct – Dec)**	**2018 Cycle Avg. (April – June)**	**2018 Cycle Avg. (Oct – Dec)**
Call Volumes	1,200 monthly avg.	1,500 monthly avg.	2,200 monthly avg.	2,500 monthly avg.	1,050 monthly avg.	2,350 monthly avg.
Email Volumes	100 daily avg.	150 daily avg.	300 daily avg.	350 daily avg.	200 daily avg.	250 daily avg.

2018 Counts of Service Requests (tickets)	May	June	July	August	September	October	November	December
Service Requests	48	849	738	606	1,157	570	661	502
Escalated Requests	29	107	128	97	132	240	119	93

*It's important to note that request volumes are also driven by election cycle. It's also important to note that DOS transitioned to a new instance of ServiceNOW in May 2018. *

2019 Counts of Service Requests (tickets)	January	February	March	April	May	June	July	August
Service Requests	707	494	576	653	765	631	641	412
Escalated Requests	125	92	146	145	139	134	145	72

*It's important to note that request volumes are also driven by election cycle. It's also important to note that DOS transitioned to a new instance of ServiceNOW in May 2018 *

Appendix K
DGS UniqueSource Subcontract Language (FINAL) (Pilot)
SUPPLIES MANUFACTURED AND SERVICES PROVIDED BY PERSONS WITH DISABILITIES
(Applicable to contracts over $100,000 for goods and over $250,000 for services)

a. **General Information.** UniqueSource Products & Services, d/b/a UniqueSource ("UniqueSource"), is the Pennsylvania marketing organization for agencies employing persons with disabilities designated to furnish up to 75% of the direct labor of manufacturing certain supplies or providing certain services to the Commonwealth pursuant to Section 520 of the Commonwealth Procurement Code, *62 Pa.C.S. §520*. Section 520 of the Procurement Code requires the Commonwealth to procure certain supplies or certain services from UniqueSource as the prime contractor without competitive bidding. In the event that UniqueSource is not the prime contractor, the Commonwealth intends to work with UniqueSource and the awarded Contractor to retain UniqueSource as a mandatory subcontractor of certain direct supplies or services to be provided to the Commonwealth under this Contract. Pennsylvania Law requires the Commonwealth to support this program through its contracting practices.

b. **UniqueSource Carve-Out List Supplies and Services.**

1) **Mandatory Items.**

a) This Section shall apply when the following conditions are met:

i. The Contractor is not a producer of the direct supplies and/or is not a provider for the direct services contracted for herein; OR

ii. The Contractor must subcontract for the direct supplies and/or services; AND

iii. The direct supplies and/or services contracted herein fall under the UniqueSource Carve-Out List.
A list of all supplies and services that are currently provided by UniqueSource can be found at the following link:
http://www.dgsweb.state.pa.us/comod/UniqueSource/CarveOutList.pdf

b) As a responsibility under the Contract with the Commonwealth, the awarded Contractor is expected to manage Commonwealth orders for the direct supplies and/or services stipulated herein. The awarded Contractor will subcontract with UniqueSource as one of its manufacturers/suppliers on such direct supplies or services as a component of the supplies and/or services contracted herein. The direct supplies and services required to be provided by UniqueSource under this Contract are set forth in the **Technical Submittal DOS Election RFP**, section **AA.1. Call Center Support.**

2) **Additional Items.** The Commonwealth encourages the awarded Contractor to utilize UniqueSource as a subcontractor or supplier for any non-mandatory/indirect supplies or services needed by the awarded Contractor to perform this Contract.

c. **Proposal Development.**

1) UniqueSource will establish the sales price or service rate based on the then current sales price or service rate in effect at the time the contract is entered into, subject to the Department of General Services' (DGS) fair market price evaluation. The DGS-established fair market prices shall remain firm for a one-year period. For each year thereafter, UniqueSource, the awarded Contractor, and/or DGS may request annual price adjustments based on PPI increases or other fair market price changes. The Commonwealth agrees that the Contractor may add a reasonable mark-up to the DGS-established fair market prices for the UniqueSource-provided items which cannot exceed the lesser of 10% or the actual cost to administer the UniqueSource subcontract. The Contractor must disclose the proposed mark-up percentage as part of its Bid or Cost Submittal.

2) The UniqueSource subcontract must not exceed 49% of labor performed or amount paid by the Commonwealth under this Contract.

3) If UniqueSource determines that it does not have the capacity to subcontract and declines to enter into a subcontract for any particular mandatory supply or service, or for a limited volume of such supply or service, the Contractor must receive a notice in writing from UniqueSource stating it declines the opportunity to subcontract on the Contract or stating the parameters of its capacity. The Contractor must then notify DGS for permission to proceed to subcontract in the market for the declined supplies or services or the remainder of limited supplies or services needed for the Contract.

d. **Subcontract Requirements.**

1) The awarded Contractor must work directly with UniqueSource to establish a subcontractor agreement as described below.

2) The awarded Contractor must submit a final, definitive subcontract agreement signed by the Contractor and UniqueSource within 30 days of the final execution date of the Commonwealth Contract. The DGS Model Form of UniqueSource Subcontractor Agreement attached to this Solicitation as Appendix K.1 may be utilized to satisfy this requirement.

3) The subcontract must contain:

a) The specific work, supplies or services UniqueSource will perform; location for work performed; how the work, supplies or services relate to the project; and the

specific timeframe during the initial term and any extensions, options and renewals of the prime contract when the work, supplies or services will be provided or performed.

b) The estimated contract percentage and dollar value that UniqueSource will receive based on the cost for the initial term of the prime contract.

c) Payment terms indicating that UniqueSource will be paid for services or supplies provided to, for, or on behalf of the Contractor within 30 days net from the invoice date. Prompt payment to UniqueSource within 30 days net is not contingent on the Contractor's receipt of payment from the Commonwealth for such work.

d) Commercially reasonable terms for the applicable business/industry that are no less favorable than the terms of the awarded Contractor's contract with the Commonwealth and that do not place disproportionate risk on UniqueSource relative to the nature and level of UniqueSource's participation in the project.

4) If the awarded Contractor and UniqueSource cannot agree upon a definitive subcontract within 30 days of the final execution date of the Commonwealth Contract, the Contractor must notify DGS.

e. <u>Prime Contract Requirements.</u>

1) The awarded Contractor shall notify the Contracting Officer of the Issuing Office and DGS when circumstances arise that may negatively impact the Contractor's ability to comply with its subcontract with UniqueSource and to provide a corrective action plan. Disputes will be decided by the Issuing Office and DGS.

2) If the awarded Contractor fails to satisfy its subcontract with UniqueSource, it may be subject to a range of sanctions DGS deems appropriate. Such sanctions include, but are not limited to, one or more of the following: a determination that the awarded Contractor is not responsible under the Contractor Responsibility Program; withholding of payments; suspension or termination of the Contract together with consequential damages; and/or suspension or debarment from future contracting opportunities with the Commonwealth.

f. <u>Waiver</u>

1) If the awarded Contractor is intractable to a subcontract relationship with UniqueSource, the Contractor may request from DGS a waiver to disaggregate the contract into two separate agreements, one for the prime Contractor, and a separate contract between the Commonwealth and UniqueSource for the required UniqueSource-provided supplies and services. UniqueSource will still provide the

direct supplies or services to the Commonwealth, but would not be in a subcontract relationship with the Contractor. If DGS determines it is in the best interests of the Commonwealth to procure the supplies or services from UniqueSource directly, DGS will notify the Contractor of its decision to do so.

APPENDIX K.1

MODEL FORM OF UNIQUESOURCE SUBCONTRACTOR AGREEMENT

This Subcontractor Agreement ("Subcontract") is made effective as of _____ __, 20__, by and between _____, ("Contractor") and UniqueSource Products & Services ("Subcontractor" or "UniqueSource") (collectively referred to as the "Parties").

RECITALS

Contractor has entered into a contract dated _____ (the "Prime Contract") with the Department of _____ of the Commonwealth of Pennsylvania ("Commonwealth"). Under the Prime Contract, Contractor has agreed to provide certain goods and/or services ("Services") to the Commonwealth.

UniqueSource Products & Services, d/b/a UniqueSource, is the Pennsylvania marketing organization for agencies employing persons with disabilities designated to furnish up to 75% of the direct labor of manufacturing certain supplies or providing certain services to the Commonwealth pursuant to Section 520 of the Commonwealth Procurement Code, 62 Pa.C.S. §520.

UniqueSource would be entitled to provide certain of the Prime Contract Services directly to the Commonwealth pursuant to the Operational Agreement for the Procurement of Goods Manufactured and Services Performed by Persons with Disabilities executed with the Commonwealth, had such goods and services been procured separately from the scope of the Prime Contract Services.

The Parties have agreed to enter into this Subcontract to fulfill the UniqueSource Carve-Out List Subcontract Requirement expressed in the Procurement and as required by the Prime Contract.

DEFINITIONS

The following words and terms when used in this Subcontract shall have the following meanings:

Contracting Officer – The person authorized to administer and make written determinations for the Commonwealth with respect to the Prime Contract.

Department – The Department of General Services of the Commonwealth of Pennsylvania.

Issuing Office – The department, board, commission or other agency of the Commonwealth of Pennsylvania that issued the Procurement.

Procurement – The Invitation for Bids, Request for Proposals, Invitation to Qualify, or other solicitation and all associated final procurement documentation issued by the Commonwealth to obtain bids/proposals from firms for award of the Prime Contract.

UniqueSource Carve-Out Items – Specific Goods and Services that the Department and UniqueSource have identified and the Department has set aside for procurement from UniqueSource and its Agencies For Persons with Disabilities, provided that UniqueSource and its Agencies for Disabilities can provide them at a fair market price and meet the requirements of Subsection IV.A of the Operational Agreement between UniqueSource and the Commonwealth.

AGREEMENT

Now, therefore, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound, the Parties hereby agree as follows:

1. Subcontractor Representations. Subcontractor represents and warrants to Contractor as follows:

   (a) Subcontractor possesses the necessary knowledge, experience, expertise, capital, resources and personnel required to perform the Services it will provide under this Subcontract;

   (b) Subcontractor (i) is duly organized, validly existing and in good standing under the laws of its state of incorporation or organization, (ii) has the power and authority to own its properties and to carry on business as now being conducted, and (iii) has the power to execute and deliver this Subcontract;

   (c) The execution and performance by Subcontractor of the terms and provisions of this Subcontract have been duly authorized by all requisite action, and neither the execution nor the performance of this Subcontract by Subcontractor will violate any provision of law, any order of any court or other agency of government, the organizational documents of Subcontractor or any indenture, agreement or other instrument to which Subcontractor is a party, or by which Subcontractor is bound, or be in conflict with, result in a breach of, or constitute (with due notice or lapse of time or both) a default under, or except as may be provided by this Subcontract, result in the creation or imposition of any lien,

charge or encumbrance of any nature whatsoever upon any of the property or assets of Subcontractor pursuant to, any such indenture agreement or instrument;

(d) Subcontractor has obtained all licenses, permits and approvals required to perform the Services it will provide under this Subcontract; and

(e) Subcontractor is not under suspension or debarment by the Commonwealth or any other governmental entity, instrumentality or authority.

2. Contractor Representations. Contractor represents and warrants to Subcontractor as follows:

(a) Contractor (i) is duly organized, validly existing and in good standing under the laws of its state of incorporation or organization, (ii) has the power and authority to own its properties and to carry on business as now being conducted, and (iii) has the power to execute and deliver this Subcontract;

(b) The execution and performance by Contractor of the terms and provisions of this Subcontract by Contractor have been duly authorized by all requisite action, and neither the execution nor the performance of this Subcontract will violate any provision of law, any order of any court or other agency of government, the organizational documents of Contractor or any indenture, agreement or other instrument to which Contractor is a party, or by which Contractor is bound, or be in conflict with, result in a breach of, or constitute (with due notice or lapse of time or both) a default under, or except as may be provided by this Subcontract, result in the creation or imposition of any lien, charge or encumbrance of any nature whatsoever upon any of the property or assets of Contractor pursuant to, any such indenture agreement or instrument;

(c) Contractor has obtained all licenses, permits and approvals required to perform the Services to be provided by Contractor under the Prime Contract; and

(d) Contractor is not under suspension or debarment by the Commonwealth or any other governmental entity, instrumentality or authority.

3. Relationship of the Parties. The provisions of this Subcontract are not intended to create, nor shall be deemed or construed to create, any joint venture, partnership or other relationship between Contractor and Subcontractor, other than that of independent entities contracting with each other solely for the purpose of carrying out the provisions of this Subcontract. Neither of the Parties to this Subcontract, nor any of their respective employees, agents, or other representatives, shall be construed to be the agent, employee or representative of the other party. Neither party shall have the authority to bind the other party, nor shall a party be responsible for the acts or omissions of the other party, unless otherwise stated in this Subcontract. Similarly, the Parties expressly acknowledge

that neither the Contractor nor the Subcontractor is an agent, employee or representative of the Commonwealth and each party covenants not to represent itself accordingly.

4. Prime Contract Flow-Down.

(a) General. This agreement is a subcontract under the Prime Contract and all provisions of the Prime Contract and any amendments thereto applicable to the Services being performed by the Subcontractor shall extend to and be binding upon the Parties as part of this Subcontract.

(b) Specific. The Parties agree to comply with the following provisions of the Prime Contract, which are incorporated herein by reference:

(1) The Americans with Disabilities Act Provisions.
(2) Nondiscrimination/Sexual Harassment Clause.
(3) Contractor Integrity Provisions.
(4) Contractor Responsibility Provisions.

(c) Termination. Should the Prime Contract be terminated pursuant to the terms and conditions provided in the Procurement, such termination shall have the same effect on this Subcontract. Payment for Services provided as of the date of termination must be made in accordance with Section 12 of this Subcontract.

(d) Audit Provisions. The Commonwealth shall have the right, at reasonable times and at a site designated by the Commonwealth, to audit the books, documents, and records of the Parties to the extent that the books, documents, and records relate to the Parties' compliance with the provisions set forth in subsections (a) and (b) above or to the UniqueSource Carve-Out List Requirement effectuated through this Subcontract. The Parties shall preserve such books, documents, and records for a period of three years from the date of final payment hereunder. The Parties shall give full and free access to all such records to the Commonwealth and/or its authorized representatives.

5. Order of Precedence. The Procurement and the Prime Contract are incorporated herein by reference into this Subcontract. In the event of any conflict or inconsistency among the individual components of this Subcontract, such conflict or inconsistency shall be resolved by observing the following order of precedence:

(a) This Subcontract;

(b) The Prime Contract; and

(c) The Procurement.

6. Further Action. The Parties shall take such actions and complete, execute and deliver any and all documents or instruments necessary to carry out the terms and provisions of this

Subcontract, to effectuate the purpose of this Subcontract, and to fulfill the obligations of each party hereunder.

7. Description of Services. Subcontractor will deliver the following products and/or perform the following Services for the Contractor which Contractor is obligated to provide to the Commonwealth under the Prime Contract:

[DESCRIBE IN DETAIL THE SPECIFIC SUPPLIES, SERVICES OR CONSTRUCTION THE SUBCONTRACTOR WILL PROVIDE OR PERFORM]

_____
_____
_____
_____
_____
_____.

8. Performance of Services. Subcontractor may not subcontract more than 49% of the work subcontracted to it hereunder without written permission from the Department. Subcontractor will supply the Goods and/or perform the Services strictly in accordance with any applicable plans and specifications as contained in the Prime Contract and the reasonable deadlines set by Contractor in view of the requirements of the Prime Contract, and in a good workmanlike manner consistent with industry standards, meeting all applicable local, state and federal laws, regulations and policies.

9. Location of Goods and/or Services. Subcontractor will provide the Goods and/or Services at the following address(es):

_____
_____.

10. Timeframe for Providing Goods and/or Performance of Services. The Goods and/or Services will be provided by Subcontractor during the initial term of the Prime Contract, and during any extensions, options or renewal periods of the Prime Contract exercised by the Commonwealth, as more specifically set forth below:

[IDENTIFY THE SPECIFIC TIME PERIODS DURING THE INITIAL CONTRACT TERM AND EXTENSIONS, OPTIONS AND RENEWALS WHEN THE SUBCONTRACTOR WILL PERFORM COMPONENT SERVICES]

_____
_____
_____

_____

_____.

11. Pricing of Services. Subcontractor shall provide the Goods and/or Services at the pricing specified in Exhibit ___ to this Subcontract. [ATTACH A BILL OF MATERIALS, RATE CARD OR OTHER APPROPRIATE COST SHEET COVERING THE SERVICES TO BE PROVIDED.]

12. Payment for Services. Unless the parties expressly agree upon a different payment schedule or structure as set forth below, Contractor shall pay Subcontractor for services or supplies provided to, for, or on behalf of the Contractor within 30 days net from the invoice date of such services or supplies. Prompt payment to Subcontractor is not contingent on the Contractor's receipt of payment from the Commonwealth for such work.

_____

_____

_____.

13. Change Orders. If the Commonwealth issues any change order or other formal contract instrument either expanding or limiting the work to be performed under the Prime Contract, the Parties shall accept such Change Orders. Contractor agrees to provide Subcontractor with written notice of any such change orders that affect the Services to be provided by the Subcontractor hereunder as soon as practical after Contractor receives such notice.

14. Non-Disclosure Clause. The Contractor may require the Subcontractor to sign a confidentiality/disclosure of information agreement.

15. Force Majeure. Neither party will incur any liability to the other if its performance of any obligation under this Subcontract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, severe weather conditions, civil disorders, natural disasters, fire, epidemic and quarantines, general strikes throughout the trade, and freight embargoes. The existence of such causes beyond a party's control shall extend the period for performance to such extent as may be necessary to enable complete performance in the exercise of reasonable diligence after the causes have been removed.

16. Dispute Resolution.

(a) The Parties will attempt to resolve any dispute arising out of or relating to this Subcontract through friendly negotiations.

(1) The Parties expressly acknowledge and confer upon the Department the authority to adjudicate disputes that the Parties cannot resolve amicably concerning the Parties' compliance with the UniqueSource Carve-Out List Subcontract Requirement as provided in the Prime Contract and this Subcontract.

(2) The Department may recommend to the Contracting Officer a range of sanctions it deems appropriate if the Department determines a party has failed to satisfy or perform its UniqueSource Carve-Out List Requirement. Such sanctions include, but are not limited to, one or more of the following: a determination that the party is not responsible under the Contractor Responsibility Program; withholding of Prime Contract and/or Subcontract payments; suspension or termination of the Prime Contract and/or Subcontract together with consequential damages; and/or suspension or debarment of one or both parties from future contracting opportunities with the Commonwealth.

(b) Nothing herein shall be construed to prevent either party from seeking such relief as provided by law in a court or tribunal of competent jurisdiction.

17. Notices. Any written notice to any party under this Subcontract shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.) with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, and sent to the following:

If to Contractor:

_____
_____
_____

If to Subcontractor:

_____

_____
_____

18. Waiver. No waiver by either party of any breach of this Subcontract shall be deemed to waive any other breach. No acceptance of payment or performance after any breach shall be deemed a waiver of any breach. No failure or delay to exercise any right by a party upon another's default shall prevent that party from later exercising that right, nor shall such failure or delay operate as a waiver of any default.

19. Severability. If any provision of this Subcontract shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision of this Subcontract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

20. Assignment. Neither party may assign or transfer this Subcontract without the prior written consent of the Commonwealth. If Contractor's Prime Contract with the Commonwealth is assigned to another contractor, the new contractor must maintain the UniqueSource Carve-Out List Requirement set forth in the Prime Contract as implemented through this Subcontract.

21. Applicable Law. This Subcontract shall be governed by the laws of the Commonwealth of Pennsylvania.

22. Entire Agreement. This Subcontract constitutes the entire agreement of the Parties regarding the subject of this Subcontract as of the date of execution. No other agreement or understandings, verbal or written, expressed or implied, are a part of this Subcontract unless specified herein.

23. Amendment. This Subcontract may be modified or amended only if made in writing and signed by both Parties. Any proposed change to the Contractor's UniqueSource Carve-Out List Subcontract Requirement must be submitted in writing to the Department which will make a recommendation to the Contracting Officer regarding a course of action.

24. Binding Effect. This Subcontract shall be binding upon, and inure to the benefit of, the Parties and their respective heirs, representatives, successors and assigns.

25. Counterparts. This Subcontract may be executed by the Parties in counterparts, each of which together shall be deemed an original but all of which together shall constitute one and the same instrument. A party's delivery of a duly executed signature page of this Subcontract in electronic format shall have the same force and effect as delivery of an original signature page.

ADDITIONAL TERMS AND CONDITIONS

THE PARTIES MAY INCLUDE ADDITIONAL TERMS AND CONDITIONS APPROPRIATE FOR THE GOODS MANUFACTURED AND/OR SERVICES TO BE PROVIDED SO LONG AS THEY ARE COMMERCIALLY REASONABLE TERMS FOR THE APPLICABLE BUSINESS OR INDUSTRY, ARE NO LESS FAVORABLE THAN THE TERMS OF THE PRIME CONTRACT, AND DO NOT PLACE DISPROPORTIONATE RISK ON UNIQUESOURCE RELATIVE TO THE NATURE AND LEVEL OF UNIQUESOURCE'S PARTICIPATION IN THE PROJECT. SUCH TERMS MAY INCLUDE:

Background Checks

Confidentiality/Disclosure of Information

Data Security

Insurance

Invoicing Requirements

Environmental Protection

Intellectual Property Rights

Record Retention/Audits

Service Level Agreements (SLAs) (consistent with Prime Contract SLAs)

Public Works Construction Requirements (including Bonding, E-Verify, Prevailing Wage, and Prompt Payment provisions)

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Appendix K
DGS UniqueSource Subcontract Language (FINAL) (Pilot)

IN WITNESS WHEREOF, the Parties hereto have caused this Subcontract to be executed by their duly authorized officers as set forth below.

Contractor	Subcontractor
Insert Company Name	*UniqueSource Products & Services*
By: _____	By: _____
Signature	Signature
_____	_____
Printed Name	Printed Name
_____	_____
Title	Title
_____	_____
Date	Date

Appendix L, Non-Commonwealth Hosting Requirements

Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this Appendix is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements

1. The Licensor or its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Quote and Statement of Work.

2. The Licensor shall provide secure access to applicable levels of users via the internet.

3. The Licensor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4. The Licensor or its subcontractors shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements.

5. The Licensor shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **two (2) business days**. In the event of any impermissible disclosure unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one (1) hour** of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. The Licensor or the Licensor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and within at least **three (3) business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Licensor or the Licensor's subcontractor shall locate servers in a climate-controlled environment. The Licensor or the Licensor's contractor shall house all

servers and equipment in an operational environment that meets industry standards including climate control, fire and security hazard detection, electrical needs, and physical security.

9. The Licensor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The Licensor shall completely test and apply patches for all third-party software products in the server environment before release.

11. The Licensor shall comply with **Attachment B, SOC Reporting Requirements**.

B. Security Requirements

1. The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense on an annual basis.

2. The Licensor shall comply with the Commonwealth's directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.

3. The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4. The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The Licensor shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. The Licensor shall limit access to Commonwealth-specific systems and services and provide access only to those staff, located in the United States, that must have access to provide services proposed.

7. The Licensor shall provide the Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in Attachment A, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

C. Data Storage

1. The Licensor shall store all Commonwealth data in the United States.

2. The Licensor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk.

The Licensor shall protect their operational systems with applicable anti-virus, host intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Licensor shall be solely responsible for applicable data storage required.

4. The Licensor shall take all commercially viable and applicable measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

5. The Licensor agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or Licensor-owned electronic device.

6. The Licensor shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

D. Adherence to Policy

1. Licensor support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. Licensor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment A.

3. Licensor shall comply with all pertinent federal and state privacy regulations.

E. Closeout

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency to the Commonwealth Software Reseller within **sixty (60) days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

ATTACHMENT A

Information Technology Policies (ITPs)
for
Outsourced/Licensor(s)-hosted Solutions

ITP Number - Name	Policy Link
ITP_ACC001- Accessibility Policy	http://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030- Active Directory Architecture	http://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007- Enterprise Service Catalog	http://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010-Business Process Management Policy	http://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS011-Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_bus011.pdf
ITP_BUS012-Artifical Intelligence General Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000- Enterprise Data and Information Management Policy	http://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001- Database Management Systems	http://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006- Commonwealth County Code Standard	http://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009- e-Discovery Technology Standard	http://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010- Business Intelligence Policy	http://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011- Reporting Policy	http://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012- Dashboard Policy	http://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001- The Life Cycle of Records: General Policy Statement	http://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004- Management of Web Records	http://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005- System Design Review of Electronic Systems	http://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006- Electronic Document Management Systems	http://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1- Electronic Commerce Formats and Standards	http://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2- Electronic Commerce Interface Guidelines	http://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006- Business Engine Rules	http://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004- Internet Protocol Address Standards	http://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005- Commonwealth External and Internal Domain Name Services (DNS)	http://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001- Commonwealth of Pennsylvania Electronic Information Privacy Policy	http://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000 - Information Security Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC002- Internet Accessible Proxy Servers and Services	http://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003- Enterprise Security Auditing and Monitoring	http://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004- Enterprise Web Application Firewall	http://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006- Commonwealth of Pennsylvania Electronic Signature Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007- Minimum Standards for IDs, Passwords and Multi-Factor Authentication	http://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008- Enterprise E-mail Encryption	http://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf
ITP_SEC009- Minimum Contractor Background Checks Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf

ITP Number - Name	Policy Link
ITP_SEC010- Virtual Private Network Standards	http://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf
ITP_SEC011- Enterprise Policy and Software Standards for Agency Firewalls	http://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC013- Identity Protection and Access Management (IPAM) Architectural Standard and Identity Management Services	http://www.oa.pa.gov/Policies/Documents/itp_sec013.pdf
ITP_SEC015- Data Cleansing	http://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC017- Copa Policy for Credit Card Use for e-Government	http://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019- Policy and Procedures for Protecting Commonwealth Electronic Data	http://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC020- Encryption Standards for Data at Rest	http://www.oa.pa.gov/Policies/Documents/itp_sec020.pdf
ITP_SEC021- Security Information and Event Management Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023- Information Technology Security Assessment and Testing Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024- IT Security Incident Reporting Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025- Proper Use and Disclosure of Personally Identifiable Information (PII)	http://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029- Physical Security Policy for IT Resources	http://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031- Encryption Standards for Data in Transit	http://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032- Enterprise Data Loss Prevention (DLP) Compliance Standards	http://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034- Enterprise Firewall Rule Set	http://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC037- Identity Proofing of Online Users	http://www.oa.pa.gov/Policies/Documents/itp_sec037.pdf
ITP_SEC038- Commonwealth Data Center Privileged User IAM Policy	http://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP SFT000- Software Development Life Cycle (SDLC) Policy	http://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001 Software Licensing	http://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002 Commonwealth of PA Website Standards	http://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003- Geospatial Enterprise Service Architecture	http://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004 Geospatial Information Systems (GIS)	http://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005- Managed File Transfer (MFT)	http://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007- Office Productivity Policy	http://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008- Enterprise Resource Planning (ERP) Management	http://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009- Application Development	http://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003- Off-Site Storage for Commonwealth Agencies	http://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004- Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	http://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006- Commonwealth IT Resources Patching Policy	http://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008- Server Virtualization Policy	http://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010- Enterprise Services Maintenance Scheduling	http://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

ATTACHMENT B

SOC Reporting Requirements

(a) Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to, engage, on an annual basis, an independent auditing firm to conduct each the following:

(i) a SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions;
(ii) a SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access or contain Commonwealth Data; and
(iii) a SOC for Cybersecurity report with respect to controls used by the Contractor setting forth the description and effectiveness of Contractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

Pennsylvania's fiscal year begins July 1 and ends on June 30. Audits shall be submitted annually no later than July 31 of the current year. All reports shall reflect the conduct of the Contractor during the 12 months of the Commonwealth's previous fiscal year, unless otherwise agreed to in writing by the Commonwealth.

(b) SOC 2 Type II report reports shall address the following:

(i) Security of Information and Systems;
(ii) Availability of Information and Systems;
(iii) Processing Integrity;
(iv) Confidentiality;
(v) Privacy; and
(vi) if applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

(c) At the request of the Commonwealth, the Contractor shall complete additional SOC for Cybersecurity audits in the event:

(i) repeated non-conformities are identified in any SOC report required by subsection (a); or
(ii) if the Contractor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.);

The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within 60 days of its completion.

(d) The Commonwealth may specify other or additional standards, certifications or audits it requires under any Purchase Orders or within an ITP.

(e) The Contractor shall adhere to SSAE 18 audit standards. The Contractor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Contractor shall comply with such updates which shall be reflected in the next annual report.

(f) In the event an audit reveals any non-conformity to SSAE standards, the Contractor shall provide the Commonwealth, within 45 calendar days of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity. The corrective action plan shall provide, in detail:

(i) clear responsibilities of the personnel designated to resolve the non-conformity;
(ii) the remedial action to be taken by the Contractor or its subcontractor(s);
(ii) the dates when each remedial action is to be implemented; and
(iii) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

(g) The Commonwealth may in its sole discretion agree, in writing, to accept alternative and equivalent reports or certifications in lieu of a SOC report.

Office of Information Technology
Information Technology
Systems Management

Release Management
Process Plan

Version 1.0

Prepared for

Commonwealth of Pennsylvania
Department of Labor and Industry

June 13, 2017

Table of Contents

1.0 About this document 1

2.0 Process Owner Document Update Responsibility 1

3.0 Release Management Process 2

- 3.1 Primary goal 2
- 3.2 Process Definition 2
- 3.3 Objectives 2
- 3.4 Terminology and Acronyms 2
- 3.5 Process Scope 3
- 3.6 Exclusions 3
- 3.7 High-level process model 4
- 3.8 Detailed Design 5
- 3.9 Inputs and Outputs 5
- 3.10 Critical Success Factors and Key Performance Indicators 6
- 3.11 Reporting Responsibilities 6

4.0 Roles and Responsibilities 8

- 4.1 Process 8
- 4.2 Process Owner 8
- 4.3 Process Manager 8

5.0 Continual Service Improvement 9

6.0 Training and Communication 10

7.0 Communication will be in accordance with the Communication Plan for ITSM processes.
Appendix A– Terminology 10

8.0 Appendix B – Acronyms 11

- 8.1 OIT Acronyms 11

9.0 Appendix C – RACI Matrix 12

10.0 Appendix D – Monthly Report Format 13

11.0 Appendix E – Quarterly Report Format 14

1.0 About this document

This document describes the Release Management Process. The Process provides a consistent method for everyone to follow when there is a release of code for a custom built application or a Commercial Off the Shelf (COTS) product.

2.0 Process Owner Document Update Responsibility

This process document will be reviewed by the process owner and ITSM Governance Board members on an annual basis at a minimum. The document will be released at least once every three years. The document will be held under change control and stored within the ITSM tool's Document Management system.

3.0 Release Management Process

3.1 Primary goal

Release Management delivers changes to an organization at optimal cost and a minimized risk. It will improve consistenciy in implementation across the projects and COTS products within the agency and will ensure they meet audit requirements for traceability throughout service transition.

3.2 Process Definition

The Release Management Process is to plan, schedule and control the build, test and deployment of releases, and to deliver new functionality required by the business while protecting the integrity of the existing services.

3.3 Objectives

Release Management will:

- Ensure all releases can be tracked, installed, tested, verified, and backed out if appropriate
- Ensure service design packages are completed and upated with release plans throughout the process and stored in the ITSM tool
- Deploy releases following the release plans and agreed upon schedule
- Record and manage deviations, risks and issues related to the change and take necessary action

3.4 Terminology and Acronyms

A terminology document has been created and is stored on the ITIL SharePoint site. The link to this site is contained in Appendix A.

Acronyms used throughout this document are provided in Appendix B.

System Development Life Cycle (SDLC)	The systems development life cycle (**SDLC**), also referred to as the application development life cycle, is a term used to describe a process for planning, creating, testing, and deploying an information system.
Release Pipeline	In theory, a release pipeline is a process that dictates how you deliver software to your end users. In practice, a release pipeline is an implementation of that pattern. The pipeline begins with code in version control and ends with code deployed to the production environment.
Business Relationship Management	The ITSM process responsible for maintaining a positive relationship with customers. Business relationship management identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalogue of services. This process has strong links with service level management.

3.5 Process Scope

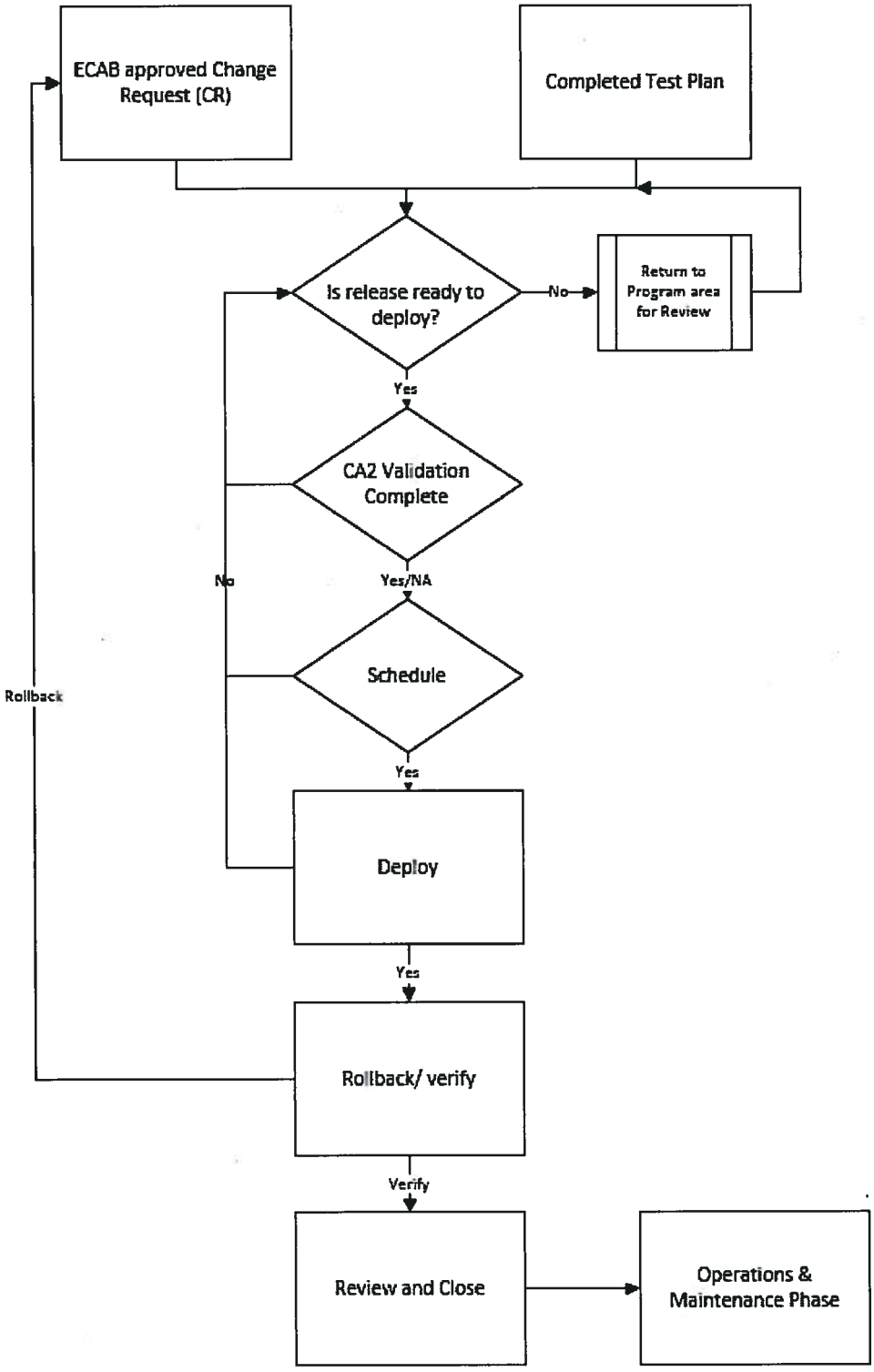
The Release Management process includes the processes, systems and functions to package, build, test and deploy a release into live use and hand the service over to operations. It includes all configuration items required to implement a release such as:

- Hardware
- Storage
- Network
- Software
- Services including all related contracts and agreements

3.6 Exclusions

While testing is a part of Release Management it is covered in the Service, Validation, and Testing Management Process. Release Management is also not responsible for authorizing any changes which will be handled in Change Management.

3.7 High-level process model



Output	To
Version Update	Application Inventory
Continuity Change/Documentation	Continuity Coordinator
Completion feedback	Asset and Configuration Management, Change Management, Business Relationship Management
Monitoring of deployment	Event Management
Deployment metrics	Application team, SDLC, and Business Relationship Management (BRM)

3.10 Critical Success Factors and Key Performance Indicators

Since we cannot manage what is not measured, performance measures will be included in every process improvement strategy using Critical Success Factors and Key Performance Indicators.

A Critical Success Factor (CSF) is something that must happen if an IT service, process, plan, project or other activity is to succeed. Key Performance Indicators (KPIs) are used to measure the achievement of each critical success factor. For example, a critical success factor of 'protect IT services when making changes' could be measured by key performance indicators such as 'percentage reduction of unsuccessful changes', 'percentage reduction in changes causing incidents' etc.

A Key Performance Indicator is a metric that is used to help manage an IT service, process, plan, project or other activity. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity. They should be selected to ensure that efficiency, effectiveness and cost effectiveness are all managed.

Critical Success Factor	Key Performance Indicator
More Successful Releases	% decrease in Security Vulnerabilities Increased number of releases using common framework and reusable processes
Agency is compliant with audit requirements	% decrease in number of external audit findings Increase in internal security audits

3.11 Reporting Responsibilities

The process owner is responsible for reporting on all Critical Success Factors and Key Performance Indicators to the ITSM Manager on a monthly basis. The report is to be submitted to the ITSM Manager each month. Where questions arise, attendance may be required at the ITSM Governance Board. Use the report template found in Appendix D.

3.8 Detailed Design

Role	Step	Description
Release Management Team/ Application Team	➢	Assess the readiness to deploy the release to the production environment verifying that the checklist of prerequisite activities have been completed. Refer to Release procedure for detailed steps.
Release Management Team	➢	Determine if the CA2 process is completed and approved by OA, giving final go ahead for new public facing applications.
Release Management Team/ Application Team	➢	Determine approved schedule for deployment. If the release did not already have an approved schedule coming out of change management, the release management team and the application owners will schedule the deployment based on resource availability.
Release Management Team	➢	Deploy the code if it is determined to be ready. Refer to Release procedure for detailed steps.
Release Management Team/ Application Team	➢	Verify deployment for completion and effectiveness. If needed it will be rolled back per the plan submitted in the Service Design Package. Refer to Release procedure for detailed steps.
Release Management Team/ Application Team	➢	Perform periodic reviews with the application team on the success of their release looking for improvements. Refer to Release procedure for detailed steps.

3.9 Inputs and Outputs

Input	From
Authorized Change Request	Change Management
Completed Test Plan	Service, Validation, and Test process

On a quarterly basis, the process owner will provide a report on the overall process. The report is to be submitted to the ITSM Manager by the 15th of March, June, September and December. The quarterly report will require information on what is working well or poorly, any issues encountered, and any suggestions for improvement. Use the report template found in Appendix E.

4.0 Roles and Responsibilities

Responsibilities may be delegated, but escalation does not remove responsibility from the individual accountable for a specific action. A RACI Matrix is provided as Appendix C.

4.1 Process

A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. It may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions if they are needed.

4.2 Process Owner

The person who is held accountable for ensuring that a process is fit for purpose. The process owner's responsibilities include sponsorship, design, change management and continual improvement of the process and its metrics. This role can be assigned to the same person who carries out the process manager role, but the two roles may be separate in larger organizations.

4.3 Process Manager

A role responsible for the operational management of a process. The process manager's responsibilities include planning and coordination of all activities required to carry out, monitor and report on the process. There may be several process managers for one process -- for example, regional change managers or IT service continuity managers for each data center. The process manager role is often assigned to the person who carries out the process owner role, but the two roles may be separate in larger organizations.

5.0 Continual Service Improvement

Suggestions for improvement are to be reported to the CSI Manager for entry onto the CSI Register. These improvement suggestions may require the process owner to attend the next ITSM Governance Board meeting to provide any additional detail or answer questions of the Board members.

The CSI Register will be reviewed monthly by the CSI Manager and Project Management Office Chief to determine level of effort for the improvement to determine if it rises to the level of a project.

Questions to help identify improvements:

- What do we want to do better?
- What do we want to stop doing?
- What do we want to start doing?

6.0 Training and Communication

Training for OIT or other staff will be provided by the process owner or process manager. Training may be accomplished in numerous ways including knowledge sharing sessions, formal and/or formal training such as hands-on training where appropriate. At a minimum, several knowledge sharing sessions will be conducted for any new or modified process.

7.0 Communication will be in accordance with the Communication Plan for ITSM processes. Appendix A– Terminology

Terminology related to ITIL processes and/or best practices is contained in the ITIL Terminology document which can be accessed through the following link:

ITIL Terminology Document

8.0 Appendix B – Acronyms

8.1 OIT Acronyms

Acronym	Definition
ASD	Application Support and Delivery
BES	Business Enterprise Services
BRM	Business Relationship Management
CIO	Chief Information Officer
CSO	Compute Services Operations Division
DAS	Database Administration Services Division
DCIO	Deputy Chief Information Officer
DDS	Disability Determination Support Division
EAS	Enterprise Architecture and Standards Section
EPM	Enterprise Project Management Section
ESC	Enterprise Security & Compliance Section
ESS	Enterprise Shared Services Division
ICS	Infrastructure and Computing Services
IEO	Infrastructure Engineering & Operations Division
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
OIT	Office of Information Technology
PAS	Procurement & Administrative Support Division
SCM	Service Control Management Division
SLA	Service Level Agreement
SMA	Service Management & Administration Division
SME	Subject Matter Experts
SWI	State Workers' Insurance Division
UCBA	Unemployment Compensation Benefits & Allowances Division
UCTW	Unemployment Compensation Tax & Wage Division
VCL	Vocational Rehabilitation, Central Services and Safety and Labor/Management Relations Division
WCDD	Workers' Comp & Disability Determination Division
WDI	Workforce Development and Information Division
WOTS	Workstation Operations & Technical Services Division

9.0 Appendix C – RACI Matrix

Obligation	Role Description
Responsible	Responsible to perform the assigned task
Accountable (only 1 person)	Accountable to make certain work is assigned and performed
Consulted	Consulted about how to perform the task appropriately
Informed	Informed about key events regarding the task

	Activity	Application Team	Release Management Team	Change Management Team	BRM
	Access Readiness of Release	I	A/R	I	I
	Schedule Release	R	A	I	I
	Deploy Code	I	A/R	I	I
	Roll back Code	I	A/R	I	I
	Review and Close	R	A/R	I	I

10.0 Appendix D – Monthly Report Format

Sample Monthly
Incident Management Process
Report

June 2016

Date Prepared:	Prepared By:

List all Critical Success Factors, Key Performance Indicators and metrics to be achieved for the period covering the previous month. Include suggestions for improvement which will be added to the CSI Register.

Examples:

1.

CSF	KPI
More Successful Releases	• % decrease in Security Vulnerabilities • Increased number of releases using common framework and reusable processes
Baseline:	• Current Code DX scans with number of Vulnerabilities for each project (March 2017) • No projects currently utilizing common framework

Metrics to be achieved:

- A 5% decrease in Security Vulnerabilities found in Code DX scans
- Two projects utilizing common framework

Suggestion for improvement:

- TBD

2.

CSF	KPI
Agency is compliant with audit requirements	1. % decrease in external audit findings 2. Increase in internal audits
Baseline:	Findings exist with UCMS, CWDS, and SWIF No current internal audits

Overview:

Metrics to be achieved:

- 5% decrease in external audit findings
- Create mechanism and schedule for internal audits

Suggestion for improvement:

11.0 Appendix E – Quarterly Report Format

Create a quarterly report for this process for submission to the ITSM Manager as outlined in Section 3.11. Report Format:

Sample Quarterly
Incident Management Process
Report

June 2016

Date Prepared:	Prepared By:

Provide the following information at a minimum:

1. Are there any concerns with how staff are following this process? If so, what suggestions do you have for improvement?
2. Do the core team process members have the right knowledge, skills, motivation and attitude?
3. Did the Critical Success Factors and Key Performance Indicators provide meaningful information? If not, what changes need to be made?

4. What went well during this quarter?
5. What did not go well during this quarter?
6. Are there any concerns with tasks spanning more than one process and/or who is responsible for tasks?
7. Are there recommendations for improvement of this process? If so, provide detail.
8. Provide any other comments you deem appropriate.

APPENDIX N

Historic Release Information

BEST, BEN, and BCFCE:

The Bureau of Election Security and Technology, Bureau of Elections and Notaries, and Bureau of Campaign Finance and Civic Engagement have several applications that support their business. All these applications are on the same release cycle, but not all applications are updated with every release. It should be noted that currently these applications are custom applications that require excessive customizations that are reflected in the historical release efforts below:

- Statewide Uniform Registry of Electors (SURE VR)
- SURE Portal
- Petition Filing
- Lobbying Disclosure and Reporting
- Election and Campaign Finance
- Election Night Returns Online Application
- Election Night Returns Tool
- Election Night Returns Ballot Data Entry
- PA Online Absentee Application
- PA Online Voter Registration Drive
- PA Online Voter Registration (web API)
- County Extranet
- PA Voter Services (PAVS)
- PA Portal Locator
- Provisional Ballot Phone System
- Voter Information Project Feed
- Campaign Finance Online

Table 1 (BEST, BEN, BCFCE Historical Release Information) outlines the average number of hours associated with various release activities for the past six (6) releases. Please note that there are no releases around the Primary and General Elections blackout periods (typically ~30d prior to May [April for Presidential years] and November). Development during those time periods is scaled back, as the same resource team is focused on supporting election-related activities. Development is also on-going, but those sprints are not deployed until after the election blackout window expires (typically June [May for Presidential years] and December).

Table 1: BEST, BEN, BCFCE Historical Release Information – Average Hours

	Average hours
SCRUM Master Activities	164
Business Analysis	199
Quality Assurance/Testing	218
Development	862
Application Support Activities	947
Total Average Hours	2391

APPENDIX N

Historic Release Information

Table 2: BEST, BEN, BCFCE Historical Release Information – User Stories

Last 12 Months	**Approx. User Story Count**
September 2018	8
October 2018	11
November 2018	6
December 2018	19
January 2019	15
February 2019	12
March 2019	11
April 2019	11
May 2019	7
June 2019	9
July 2019	10
August 2019	18
Total User Stories	137

It should also be noted that the stated hours do not include the actual deployment of the Sprint, which is highly dependent on the Sprint User Stories included in the Sprint. Deployment activities usually involve server and database administrative resources, development and test resources for verification testing and program area resources for final verification. Deployments are currently scheduled for after normal business hours as to minimize impact to the County Election Offices.

APPENDIX O
Current Deployment Methodologies

Current Deployment Methodology

- The deployment methodology may vary depending on the location of the deployment. It should be noted that:
- DOS Deployment Methodology encompasses application deployments in both the STAGING and PROD environments
- PA Computing Services (PACS) Deployment Methodology encompasses infrastructure, security and configuration deployments for the PACS datacenter.
- Enterprise Data Center (EDC) Deployment Methodology application deployments in the DEV/QA environment.
- Enterprise Data Center Managed Services Deployment Methodology encompasses infrastructure, security and configuration deployments for the EDC datacenter.

DOS Deployment Methodology

- A scheduled deployment date must be agreed upon by BMIS, development and test teams and the Program Area, looking at availability, impact to business functions and corresponding deadlines.
- An ITSM Ticket must be submitted to BMIS Ops requesting a date for deployment.
- BMIS Ops will put the deployment on the CAB calendar for approval
- Test and UAT teams will validate the changes and test the acceptance criteria (using defined test cases) for the affected User Stories.
- Deployment documentation must be submitted to BMIS Ops prior to the agreed deployment date.
    - Document must be approved by BMIS, Development, Testing and Program Area teams for its sequence and content.
- BMIS Ops in conjunction with Development will deploy specific User Stories to the staging environment based on the availability and readiness of the User Story for UAT.
- Upon the Sprint end, all successful User Stories will be packaged into a deployment package within TFS.
- BMIS Ops will deploy to the production environment based on the agreed deployment date and approved Deployment document. Deployment verification testing is performed by both the development test and stakeholder test teams, based on a predefined verification test matrix.

PA Computing Services (PACS) Deployment Methodology

- New deployments and changes to existing deployments are initiated with completion and submission of a PACS Change Request (CR) form.
    - These are submitted by BMIS, upon prior initial approval with supporting documentation, such as quotes
    - Any changes requiring a financial cost/impact must be approved by the Program Area and the Bureau of Fiscal Operations?? (BFO)
- The submitted CR is approved by the PACS vendor and the Delivery Center ISO group and returned back to the BMIS or Commonwealth contact for final approval, including implementation schedule.
- At start time of the CR implementation window, the implementer will contact PACS Operations to initiate the CR. BMIS may be also included in this communication.
- After completion of the CR, the implementer will contact PACS Operations and BMIS to close out the CR.
- Notification is given to the Commonwealth contact that the CR has been completed, deferred, or cancelled depending on the deployment outcome.
    - It is also requested that the requestor validate the CR and give feedback the PACS Operations.

APPENDIX O
Current Deployment Methodologies

Enterprise Data Center (EDC) Deployment Methodology

- New deployments and changes to existing deployments are initiated and tracked within TFS.
- The Application Development team works internally to establish deployment dates in the DEV/QA environment.
- All deployments are performed by the Application Development team (code and database) within the DEV environment based on the Sprint cycle (and within TFS).
- The Application Development and Test teams perform various testing scenarios for the User Stories within the current Sprint.

Enterprise Data Center (EDC) Managed Services Deployment Methodology

- An ITSM Ticket must be submitted to the OA/OIT (Office of Administration/Office of Information Technology) team requesting a change request and its corresponding deployment schedule.
- Deployment documentation must be submitted to OA/OIT prior to the agreed deployment date.
    - These are submitted by BMIS, upon prior initial approval with supporting documentation, such as quotes
    - Any changes requiring a financial cost/impact must be approved by the Program Area and the Bureau of Fiscal Operations?? (BFO)
- The submitted request is reviewed and approved by the Office of Administration and the Delivery Center ISO group and returned back to the BMIS or Commonwealth contact for final approval, including implementation schedule.
- At start time of the CR implementation window, the implementer will contact EDC Operations to initiate the CR. BMIS may be also included in this communication.
- After completion of the CR, the implementer will contact EDC Operations and BMIS to close out the CR.
- Notification is given to the Commonwealth contact that the CR has been completed, deferred, or cancelled depending on the deployment outcome.
    - It is also requested that the requestor validate the CR and give feedback the EDC Operations.

EXHIBIT A

Contract Terms and Conditions

1. DEFINITIONS.

(a) Agency. The department, board, commission or other agency of the Commonwealth of Pennsylvania listed as the Purchasing Agency. If a COSTARS entity or external procurement activity has issued an order against this Contract, that entity shall also be identified as "Agency."

(b) Commonwealth. The Commonwealth of Pennsylvania.

(c) Contract. The integrated documents as defined in **Section 11, Order of Precedence**.

(d) Contracting Officer. The person authorized to administer this Contract for the Commonwealth and to make written determinations with respect to the Contract.

(e) Data. Any recorded information, regardless of the form, the media on which it is recorded or the method of recording.

(f) Days. Calendar days, unless specifically indicated otherwise.

(g) Developed Works. All of the fully or partially complete property, whether tangible or intangible prepared by the Contractor for ownership by the Commonwealth in fulfillment of the requirements of this Contract, including but not limited to: documents; sketches; drawings; designs; works; papers; files; reports; computer programs; documentation; data; records; software; samples; literary works and other works of authorship. Developed Works include all material necessary to exercise all attributes of ownership or of the license granted in **Section 46, Ownership of Developed Works**.

(h) Documentation. All materials required to support and convey information about the Services or Supplies required by this Contract, including, but not limited to: written reports and analyses; diagrams maps, logical and physical designs; system designs; computer programs; flow charts; and disks and/or other machine-readable storage media.

(i) Expiration Date. The last valid date of the Contract, as indicated in the Contract documents to which these IT Contract Terms and Conditions are attached.

(j) Purchase Order. Written authorization for Contractor to proceed to furnish Supplies or Services.

(k) Proposal. Contractor's response to a Solicitation issued by the Issuing Agency, as accepted by the Commonwealth.

(l) Services. All Contractor activity necessary to satisfy the Contract.

(m) Software. A collection of one or more programs, databases or microprograms fixed in any tangible medium of expression that comprises a sequence of instructions (source code) to carry out a process in, or convertible into, a form executable by an electronic computer (object code).

(n) Solicitation. A document issued by the Commonwealth to procure Services or Supplies, e.g., Request for Proposal; Request for Quotation; Supplier Pricing Request; or Invitation for Bid, including all attachments and addenda thereto.

(o) Supplies. All tangible and intangible property including, but not limited to, materials and equipment provided by the Contractor to satisfy the Contract.

2. TERM OF CONTRACT.

(a) Term. The term of the Contract shall commence on the Effective Date and shall end on the Expiration Date identified in the Contract, subject to the other provisions of the Contract.

(b) Effective Date. The Effective Date shall be one of the following:

- the date the Contract has been fully executed by the Contractor and all approvals required by Commonwealth contracting procedures have been obtained; or

- the date stated in the Contract, whichever is later.

3. COMMENCEMENT OF PERFORMANCE.

(a) General. The Contractor shall not commence performance and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until both of the following have occurred:

- the Effective Date has occurred; and

- the Contractor has received a Purchase Order or other written notice to proceed signed by the Contracting Officer.

(b) Prohibition Prior to Effective Date. No Commonwealth employee has the authority to verbally direct the commencement of any Service or delivery of any Supply under this Contract prior to the date performance may commence. The Contractor

hereby waives any claim or cause of action for any Service performed or Supply delivered prior to the date performance may commence.

4. EXTENSION OF CONTRACT TERM.

The Commonwealth reserves the right, upon notice to the Contractor, to extend the term of the Contract for up to **three (3) months** upon the same terms and conditions.

5. ELECTRONIC SIGNATURES.

(a) The Contract and/or Purchase Orders may be electronically signed by the Commonwealth.

- *Contract*. "Fully Executed" at the top of the first page of the Contract output indicates that the signatures of all the individuals required to bind the Commonwealth to the terms of the Contract have been obtained. If the Contract output form does not have "Fully Executed" at the top of the first page, the Contract has not been fully executed.

- *Purchase Orders*. The electronically-printed name of the Purchasing Agent on the Purchase Order indicates that all approvals required by Commonwealth contracting procedures have been obtained.

(b) The Commonwealth and the Contractor specifically agree as follows:

- *Written signature not required.* No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

- *Validity; admissibility*. The parties agree that no writing shall be required in order to make the Contract or Purchase Order legally binding, notwithstanding contrary requirements in any law or regulation. The parties hereby agree not to contest the validity or enforceability of the Contract executed electronically, or acknowledgement issued electronically, under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements be in writing and signed by the party bound thereby. Any genuine Contract or acknowledgement executed or issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of a genuine Contract or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or acknowledgement were not in writing or signed by the parties. A Contract

or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(c) Verification. Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

6. PURCHASE ORDERS.

(a) Purchase Orders. The Commonwealth may issue Purchase Orders against the Contract or issue a Purchase Order as the Contract. These Purchase Orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to, and including, the Expiration Date of the Contract are acceptable and must be performed in accordance with the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

(b) Electronic transmission. Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a Purchase Order shall require acknowledgement of receipt of the transmission by the Contractor.

(c) Receipt. Receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of a Purchase Order.

(d) Received next business day. Purchase Orders received by the Contractor after 4 p.m. will be considered received the following business day.

(e) Commonwealth Purchasing Card. Purchase Orders under $10,000 in total amount may also be made in person or by telephone using a Commonwealth Purchasing Card. When an order is placed by telephone, the Commonwealth agency shall provide the agency name, employee name, credit card number and expiration date of the card. The Contractor agrees to accept payment through the use of a Commonwealth Purchasing card.

7. CONTRACT SCOPE.

The Contractor agrees to furnish the requested Services and Supplies to the Commonwealth as such Services and Supplies are defined in this Contract.

8. ACCESS TO COMMONWEALTH FACILITIES.

If the Contractor must perform work at a Commonwealth facility outside of the daily operational hours set forth by the Commonwealth, it must make arrangements with the Commonwealth to assure access to the facility and equipment. No additional payment will be made on the basis of lack of access.

9. NON-EXCLUSIVE CONTRACT.

The Commonwealth reserves the right to purchase Services and Supplies within the scope of this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

10. INFORMATION TECHNOLOGY POLICIES.

(a) General. The Contractor shall comply with the IT standards and policies issued by the Governor's Office of Administration, Office for Information Technology (located at https://www.oa.pa.gov/Policies/Pages/itp.aspx), including the accessibility standards set out in IT Policy ACC001, Accessibility Policy. The Contractor shall ensure that Services and Supplies procured under the Contract comply with the applicable standards. In the event such standards change during the Contractor's performance, and the Commonwealth requests that the Contractor comply with the changed standard, then any incremental costs incurred by the Contractor to comply with such changes shall be paid for pursuant to a change order to the Contract.

(b) Waiver. The Contractor may request a waiver from an Information Technology Policy (ITP) by providing detailed written justification as to why the ITP cannot be met. The Commonwealth may waive the ITP in whole, in part or conditionally, or require that the Contractor provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

11. ORDER OF PRECEDENCE.

If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(a) The Contract document containing the parties' signatures;

(b) The IT Contract Terms and Conditions;

(c) The Request for Proposal; and

(d) The Contractor's Proposal.

12. CONTRACT INTEGRATION.

(a) Final contract. This Contract constitutes the final, complete, and exclusive Contract between the parties, containing all the terms and conditions agreed to by the parties.

(b) Prior representations. All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

(c) Conditions precedent. There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

(d) Sole applicable terms. No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

(e) Other terms unenforceable. The Contractor may not require the Commonwealth or any user of the Services or Supplies acquired within the scope of this Contract to sign, click through, or in any other way agree to any terms associated with use of or interaction with those Services and/or Supplies, unless the Commonwealth has approved the terms in writing in advance under this Contract, and the terms are consistent with this Contract. Further, changes to terms may be accomplished only by processes set out in this Contract; no quotations, invoices, business forms or other documentation, or terms referred to therein, shall become part of this Contract merely by their submission to the Commonwealth or their ordinary use in meeting the requirements of this Contract. Any terms imposed upon the Commonwealth or a user in contravention of this subsection (e) must be removed at the direction of the Commonwealth and shall not be enforced or enforceable against the Commonwealth or the user.

13. PERIOD OF PERFORMANCE.

The Contractor, for the term of this Contract, shall complete all Services and provide all Supplies as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services or Supplies provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services or Supplies.

14. INDEPENDENT PRIME CONTRACTOR.

(a) Independent contractor. In performing its obligations under the Contract, the Contractor will act as an independent contractor and not as an employee or agent of the Commonwealth.

(b) Sole point of contact. The Contractor will be responsible for all Services and Supplies in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

15. SUBCONTRACTS.

The Contractor may subcontract any portion of the Services or Supplies described in this Contract to third parties selected by Contractor and approved in writing by the Commonwealth, whose approval shall not be unreasonably withheld. Notwithstanding the above, if Contractor has disclosed the identity of subcontractor(s) together with the scope of work to be subcontracted in its Proposal, award of the Contract is deemed approval of all named subcontractors and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. Upon request of the Commonwealth, the Contractor must provide the Commonwealth with an un-redacted copy of the subcontract agreement between the Contractor and the subcontractor. The Commonwealth reserves the right, for good cause, to require that the Contractor remove a subcontractor from the project. The Commonwealth will not be responsible for any costs incurred by the Contractor in replacing the subcontractor if good cause exists.

16. OTHER CONTRACTORS.

The Commonwealth may undertake or award other contracts for additional or related work, and the Contractor shall fully cooperate with other contractors and Commonwealth employees and coordinate its Services and/or its provision of Supplies with such additional work as may be required. The Contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees. This section shall be included in the Contracts of all contractors with which this Contractor will be required to cooperate. The Commonwealth shall equitably enforce this section as to all contractors to prevent the imposition of unreasonable burdens on any contractor.

17. ENHANCED MINIMUM WAGE.

(a) Enhanced Minimum Wage. Contractor/Lessor agrees to pay no less than $12.00 per hour to its employees for all hours worked directly performing the services called for in this Contract/Lease, and for an employee's hours performing ancillary services necessary for the performance of the contracted services or lease when such employee spends at least twenty per cent (20%) of their time performing ancillary services in a given work week.

(b) Adjustment. Beginning July 1, 2019, and annually thereafter, the minimum wage rate shall be increased by $0.50 until July 1, 2024, when the minimum wage reaches $15.00. Thereafter, the minimum wage rate would be increased by an annual cost-of-living adjustment using the percentage change in the Consumer Price Index for All Urban Consumers (CPI-U) for Pennsylvania, New Jersey, Delaware, and Maryland. The applicable adjusted amount shall be published in the Pennsylvania Bulletin by March 1 of each year to be effective the following July 1.

(c) Exceptions. These Enhanced Minimum Wage Provisions shall not apply to employees:

- ☐ exempt from the minimum wage under the Minimum Wage Act of 1968;
- ☐ covered by a collective bargaining agreement;
- ☐ required to be paid a higher wage under another state or federal law governing the services, including the *Prevailing Wage Act* and Davis-Bacon Act; or
- ☐ required to be paid a higher wage under any state or local policy or ordinance.

(d) Notice. Contractor/Lessor shall post these Enhanced Minimum Wage Provisions for the entire period of the contract conspicuously in easily-accessible and well-lighted places customarily frequented by employees at or near where the contracted services are performed.

(e) Records. Contractor/Lessor must maintain and, upon request and within the time periods requested by the Commonwealth, furnish all employment and wage records necessary to document compliance with these Enhanced Minimum Wage Provisions.

(f) Sanctions. Failure to comply with these Enhanced Minimum Wage Provisions may result in the imposition of sanctions, which may include, but shall not be limited to, termination of the contract or lease, nonpayment, debarment or referral to the Office of General Counsel for appropriate civil or criminal referral.

(g) Subcontractors. Contractor/Lessor shall include the provisions of these Enhanced Minimum Wage Provisions in every subcontract so that these provisions will be binding upon each subcontractor.

18. COMPENSATION.

(a) General. The Contractor shall be required to perform at the price(s) quoted in the Contract. All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and Services performed to the satisfaction of the Commonwealth.

(b) Travel. The Contractor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Contract. If not otherwise specified in the Contract, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

19. BILLING REQUIREMENTS.

(a) Unless the Contractor has been authorized by the Commonwealth for Evaluated Receipt Settlement or Vendor Self-Invoicing, the Contractor shall include in all of its invoices the following minimum information:

- Vendor name and "Remit to" address, including SAP Vendor number;
- Bank routing information, if ACH;
- SAP Purchase Order number;
- Delivery Address, including name of Commonwealth agency;
- Description of the supplies/services delivered in accordance with SAP Purchase Order (include Purchase Order line number if possible);
- Quantity provided;
- Unit price;
- Price extension;
- Total price; and
- Delivery date of supplies or services.

(b) If an invoice does not contain the minimum information set forth in this section, and comply with the provisions located at https://www.budget.pa.gov/Programs/Pages/E-Invoicing.aspx, relating to the Commonwealth E-Invoicing Program, the Commonwealth may return the invoice as improper. If the Commonwealth returns an invoice as improper, the time for processing a payment will be suspended until the Commonwealth receives a correct invoice. The Contractor may not receive payment until the Commonwealth has received a correct invoice.

20. PAYMENT.

(a) Payment Date. The Commonwealth shall put forth reasonable efforts to make payment by the required payment date. The required payment date is:

- the date on which payment is due under the terms of the Contract;
- **thirty (30) days** after a proper invoice actually is received at the "Bill To" address if a date on which payment is due is not specified in the Contract (a

"proper" invoice is not received until the Commonwealth accepts the service as satisfactorily performed); or

- the payment date specified on the invoice if later than the dates established by paragraphs (a)(i) and (a)(ii), above.

(b) Delay; Interest. Payment may be delayed if the payment amount on an invoice is not based upon the price(s) as stated in the Contract. If any payment is not made within **15 days** after the required payment date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act of December 13, 1982, P.L. 1155, No. 266, 72 P. S. § 1507, (relating to interest penalties on Commonwealth accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to interest penalties for late payments to qualified small business concerns).

(c) Payment should not be construed by the Contractor as acceptance of the Service performed by the Contractor. The Commonwealth reserves the right to conduct further testing and inspection after payment, but within a reasonable time after performance, and to reject the service if such post payment testing or inspection discloses a defect or a failure to meet specifications.

21. ELECTRONIC PAYMENTS.

(a) The Commonwealth will make contract payments through the Automated Clearing House (ACH). Within **10 days** of award of the Contract, the Contractor must submit or must have already submitted its ACH information within its user profile in the Commonwealth's procurement system (SRM).

(b) The Contractor must submit a unique invoice number with each invoice submitted. The unique invoice number will be listed on the Commonwealth's ACH remittance advice to enable the Contractor to properly apply the state agency's payment to the invoice submitted.

(c) It is the responsibility of the Contractor to ensure that the ACH information contained in SRM is accurate and complete. Failure to maintain accurate and complete information may result in delays in payments.

22. ASSIGNABILITY.

(a) Subject to the terms and conditions of this section the Contract is binding upon the parties and their respective successors and assigns.

(b) The Contractor may not assign, in whole or in part, the Contract or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of the

Commonwealth, which consent may be withheld at the sole and absolute discretion of the Commonwealth.

(c) For the purposes of the Contract, the term "assign" shall include, but shall not be limited to, the sale, gift, assignment, encumbrance, pledge, or other transfer of any ownership interest in the Contractor provided, however, that the term shall not apply to the sale or other transfer of stock of a publicly traded company.

(d) Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned.

(e) Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

(f) A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

23. INSPECTION AND ACCEPTANCE.

(a) Developed Works and Services.

■ *Acceptance*. Acceptance of any Developed Work or Service will occur in accordance with an acceptance plan (Acceptance Plan) submitted by the Contactor and approved by the Commonwealth. Upon approval of the Acceptance Plan by the Commonwealth, the Acceptance Plan becomes part of this Contract.

■ *Software Acceptance Test Plan*. For contracts where the development of Software, the configuration of Software or the modification of Software is being inspected and accepted, the Acceptance Plan must include a Software Acceptance Test Plan, as mutually agreed to by the Parties. The Software Acceptance Test Plan will provide for a final acceptance test, and may provide for interim acceptance tests. Each acceptance test will be designed to demonstrate that the Software conforms to the functional specifications, if any, and the requirements of this Contract. The Contractor shall notify the Commonwealth when the Software is completed and ready for acceptance testing. The Commonwealth will not unreasonably delay commencement of acceptance testing.

- If software integration is required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be final unless at the time of final acceptance, the Software does not meet the acceptance criteria set forth in the Contract.

- If software integration is not required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be complete and final.

- *Certification of Completion*. The Contractor shall certify, in writing, to the Commonwealth when an item in the Acceptance Plan is completed and ready for acceptance. The Acceptance Plan shall define acceptance periods for both interim and final items as may be agreed to by the parties. Following receipt of the Contractor's certification of completion of an item, the Commonwealth shall, either:

  (1) Provide the Contractor with Commonwealth's written acceptance of the work product; or

  (2) Identify to the Contractor, in writing, the failure of the work product to comply with the specifications, listing all such errors and omissions with reasonable detail.

- *Deemed Acceptance*. If the Commonwealth fails to notify the Contractor in writing of any failures in the work product within the applicable acceptance period, the work product shall be deemed accepted.

- *Correction upon Rejection*. Upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the work product to comply with the specifications, the Contractor shall have **15 business days**, or such other time as the Commonwealth and the Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected item, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the items have been brought into compliance with the specifications. Upon receipt of such corrected and resubmitted items and certification, the Commonwealth shall have **15 business days** to test the corrected items to confirm that they are in compliance with the specifications. If the corrected items are in compliance with the specifications, then the Commonwealth shall provide the Contractor with its acceptance of the items in the completed milestone.

■ *Options upon Continued Failure*. If, in the opinion of the Commonwealth, the corrected items still contain material failures, the Commonwealth may either:

(1) Repeat the procedure set forth above; or

(2) Proceed with its rights under **Section 28, Termination**, except that the cure period set forth in **Subsection 28(c)** may be exercised in the Commonwealth's sole discretion.

(b) Supplies.

■ *Inspection prior to Acceptance*. No Supplies received by the Commonwealth shall be deemed accepted until the Commonwealth has had a reasonable opportunity to inspect the Supplies.

■ *Defective Supplies*. Any Supplies discovered to be defective or that fail to conform to the specifications may be rejected upon initial inspection or at any later time if the defects contained in the Supplies or the noncompliance with the specifications were not reasonably ascertainable upon the initial inspection.

(1) The Contractor shall remove rejected item(s) from the premises without expense to the Commonwealth within **15 days** after notification.

(2) Rejected Supplies left longer than **30 days** will be regarded as abandoned, and the Commonwealth shall have the right to dispose of them as its own property and shall retain that portion of the proceeds of any sale which represents the Commonwealth's costs and expenses in regard to the storage and sale of the Supplies.

(3) Upon notice of rejection, the Contractor shall immediately replace all such rejected Supplies with others conforming to the specifications and which are not defective. If the Contractor fails, neglects or refuses to do so, the Commonwealth may procure, in such manner as it determines, supplies similar or identical to the those that Contractor failed, neglected or refused to replace, and deduct from any monies due or that may thereafter become due to the Contractor, the difference between the price stated in the Contract and the cost thereof to the Commonwealth.

24. DEFAULT.

The Commonwealth may, subject to the provisions of **Section 25, Notice of Delays**, and **Section 66, Force Majeure**, and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate (as provided in **Section 28, Termination**) the whole or any part of this Contract for any of the following reasons:

- Failure to begin Services within the time specified in the Contract or as otherwise specified;
- Failure to perform the Services with sufficient labor, equipment, or material to insure the completion of the specified Services in accordance with the Contract terms;
- Unsatisfactory performance of the Services;
- Failure to meet requirements within the time periods(s) specified in the Contract;
- Multiple failures over time of a single service level agreement or a pattern of failure over time of multiple service level agreements;
- Failure to provide a Supply or Service that conforms with the specifications referenced in the Contract;
- Failure or refusal to remove material, or remove, replace or correct any Supply rejected as defective or noncompliant;
- Discontinuance of Services without approval;
- Failure to resume a Service, which has been discontinued, within a reasonable time after notice to do so;
- Insolvency;
- Assignment made for the benefit of creditors;
- Failure or refusal, within **10 days** after written notice by the Contracting Officer, to make payment or show cause why payment should not be made, of any amounts due subcontractors for materials furnished, labor supplied or performed, for equipment rentals or for utility services rendered;
- Failure to protect, repair or make good any damage or injury to property;
- Breach of any provision of this Contract;

- Any breach by Contractor of the security standards or procedures of this Contract;
- Failure to comply with representations made in the Contractor's Proposal; or
- Failure to comply with applicable industry standards, customs and practice.

25. NOTICE OF DELAYS.

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall promptly give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with **Section 27, Changes**.

26. CONDUCT OF SERVICES.

(a) Following the Effective Date of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

(b) In determining whether the Contractor has performed with due diligence under the Contract, it is agreed and understood that the Commonwealth may measure the amount and quality of the Contractor's effort against the representations made in the Contractor's Proposal. The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth reasonably determines that the Contractor has not performed with due diligence, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of **Section 30, Contract Controversies**.

27. CHANGES.

(a) At any time during the performance of the Contract, the Commonwealth or the Contractor may request a change to the Contract. Contractor will make reasonable efforts to investigate the impact of the change request on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commonwealth is the requestor of the change, the Contractor will inform the

Commonwealth of any charges for investigating the change request prior to incurring such charges. If the Commonwealth and the Contractor agree on the results of the investigation and any necessary changes to the Contract, the parties must complete and execute a change order to modify the Contract and implement the change. The change order will be evidenced by a writing in accordance with the Commonwealth's change order procedures. No work may begin on the change order until the Contractor has received the executed change order. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall perform the Services according to a mutually agreed-to implementation schedule; and either party may elect to have the matter treated as a dispute between the parties under **Section 30, Contract Controversies**. During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts.

(b) Changes outside the scope of this Contract shall be accomplished through the Commonwealth's procurement procedures, and may result in an amended Contract or a new contract. No payment will be made for services outside of the scope of the Contract for which no amendment has been executed.

28. TERMINATION.

(a) For Convenience.

■ The Commonwealth may terminate the Contract, or a Purchase Order issued against the Contract, in whole or in part, without cause by giving Contractor **30 days'** prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of termination hereunder, Contractor shall receive payment for the following:

(1) all Services performed consistent with the terms of the Contract prior to the effective date of termination;

(2) all actual and reasonable costs incurred by Contractor as a result of the termination of the Contract; and

In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any subcontractor), loss of use of money, or administrative or overhead costs.

Failure to agree on any termination costs shall be a dispute handled in accordance with **Section 30, Contract Controversies**, of this Contract.

- The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such Services performed during the **30-day** notice period, if such Services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

- The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

(b) Non-Appropriation. Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When funds (state or federal) are not appropriated or otherwise made available to support continuation of performance or full performance in a subsequent fiscal year period, the Commonwealth shall have the right to terminate the Contract in whole or in part. The Contractor shall be reimbursed in the same manner as that described in subsection (a) to the extent that appropriated funds are available.

(c) Default. The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within **30 days**, or if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

- Subject to **Section 38, Limitation of Liability**, in the event the Commonwealth terminates this Contract in whole or in part as provided in this subsection (c), the Commonwealth may procure services similar to

those so terminated, and the Contractor, in addition to liability for any liquidated damages, shall be liable to the Commonwealth for the difference between the Contract price for the terminated portion of the Services and the actual and reasonable cost (but in no event greater than the fair market value) of producing substitute equivalent services for the terminated Services, provided that the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this section.

- Except with respect to defaults of subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism and unusually severe weather. The Contractor shall notify the Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

- Nothing in this subsection (c) shall abridge the Commonwealth's right to suspend, debar or take other administrative action against the Contractor.

- If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under subsection (a).

- If this Contract is terminated as provided by this subsection (c), the Commonwealth may, in addition to any other rights provided in this subsection (c), and subject law and to other applicable provisions of this Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such Software, Data, Developed Works, Documentation and other materials as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated.

(d) The rights and remedies of the Commonwealth provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(e) The Commonwealth's failure to exercise any rights or remedies provided in this section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(f) Following exhaustion of the Contractor's administrative remedies as set forth in **Section 30, Contract Controversies**, the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

29. BACKGROUND CHECKS.

(a) The Contractor, at its expense, must arrange for a background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Commonwealth IT facilities, either through on-site access or through remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access and on an annual basis thereafter.

(b) Before the Commonwealth will permit access to the Contractor, the Contractor must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that an employee of the Contractor or an employee of a subcontractor of the Contractor has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the Contractor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee and shall not permit that employee remote access unless the Commonwealth consents to the access, in writing, prior to the access. The Commonwealth may withhold its consent in its sole discretion. Failure of the Contractor to comply with the terms of this section on more than one occasion or Contractor's failure to cure any single failure to the satisfaction of the Commonwealth may result in the Contractor being deemed in default of its Contract.

(c) The Commonwealth specifically reserves the right of the Commonwealth to conduct or require background checks over and above that described herein.

30. CONTRACT CONTROVERSIES.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Contract or a purchase order, the Contractor, within **six (6) months** after the cause of action accrues, must file a written claim with the Contracting Officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists. If the Contractor fails to file a claim or files an untimely claim, the Contractor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, https://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

(b) If the Contractor or the Contracting Officer requests mediation, and the other party agrees, the Contracting Officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the Contracting Officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the Contracting Officer and the Contractor. The Contracting Officer shall send his/her written determination to the Contractor. If the Contracting Officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The Contracting Officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Contractor shall proceed diligently with the performance of the Contract or Purchase Order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Contractor pursuant to the terms of the Contract or Purchase Order.

31. CONFIDENTIALITY, PRIVACY AND COMPLIANCE.

(a) General. The Contractor agrees to protect the confidentiality of the Commonwealth's confidential information. The Commonwealth agrees to protect the confidentiality of Contractor's confidential information. Unless the context otherwise clearly indicates the need for confidentiality, information is deemed confidential only when the party claiming confidentiality designates the information as "confidential" in such a way as to give notice to the other party (for example, notice may be communicated by describing the information, and the specifications around its use or disclosure, in the Solicitation or in the Proposal). Neither party may assert that information owned by the other party is such party's confidential information. Notwithstanding the foregoing, all Data provided by, or collected, processed, or created on behalf of the Commonwealth is Confidential Information unless otherwise indicated in writing.

(b) Copying; Disclosure; Termination. The parties agree that confidential information shall not be copied, in whole or in part, or used or disclosed except when essential for authorized activities under this Contract and, in the case of disclosure, where the recipient of the confidential information has agreed to be bound by confidentiality requirements no less restrictive than those set forth herein. Each copy of confidential information shall be marked by the party making the copy with any notices appearing in the original. Upon expiration or termination of this

Contract or any license granted hereunder, the receiving party will return to the disclosing party, or certify as to the destruction of, all confidential information in the receiving party's possession, other than one copy (where permitted by law or regulation), which may be maintained for archival purposes only, and which will remain subject to this Contract's security, privacy, data retention/destruction and confidentiality provisions. A material breach of these requirements may result in termination for default pursuant to **Subsection 28(c)**, in addition to other remedies available to the non-breaching party.

(c) Insofar as information is not otherwise protected by law or regulation, the obligations stated in this section do not apply to information:

- already known to the recipient at the time of disclosure other than through the contractual relationship;
- independently generated by the recipient and not derived from the information supplied by the disclosing party;
- known or available to the public, except where such knowledge or availability is the result of unauthorized disclosure by the recipient of the proprietary information;
- disclosed to the recipient without a similar restriction by a third party who has the right to make such disclosure; or
- required to be disclosed by the recipient by law, regulation, court order, or other legal process.

There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how or data processing techniques developed alone or jointly with the Commonwealth in connection with services provided to the Commonwealth under this Contract.

(d) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare and submit an un-redacted version of the appropriate document;
- Prepare and submit a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret. The Contractor shall use a redaction program that ensures the information is permanently and irreversibly redacted; and

- Prepare and submit a signed written statement that identifies confidential or proprietary information or trade secrets and that states:

  (1) the attached material contains confidential or proprietary information or trade secrets;

  (2) the Contractor is submitting the material in both redacted and un-redacted format, if possible, in accordance with 65 P.S. § 67.707(b); and

  (3) the Contractor is requesting that the material be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(e) Disclosure of Recipient or Beneficiary Information Prohibited. The Contractor shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from Services under the Contract for any purpose not connected with the Contractor's responsibilities, except with consent pursuant to applicable law or regulations. All material associated with direct disclosures of this kind (including the disclosed information) shall be provided to the Commonwealth prior to the direct disclosure.

(f) Compliance with Laws. Contractor will comply with all applicable laws or regulations related to the use and disclosure of information, including information that constitutes Protected Health Information (PHI) as defined by the *Health Insurance Portability and Accountability* Act (HIPAA). Further, by signing this Contract, the Contractor agrees to the terms of the Business Associate Agreement, which is incorporated into this Contract as **Attachment A**, or as otherwise negotiated by the Contractor and the purchasing agency. It is understood that **Attachment A, *Commonwealth of Pennsylvania Business Associate Agreement***, is only applicable if and to the extent indicated in the Contract.

(g) Additional Provisions. Additional privacy and confidentiality requirements may be specified in the Contract.

(h) Restrictions on Use. All Data and all intellectual property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be used only for the work of this Contract. No Data, intellectual property, Documentation or Developed Works may be used, disclosed, or otherwise opened for access by or to the Contractor or any third party unless directly related to and necessary under the Contract.

32. PCI SECURITY COMPLIANCE.

(a) General. By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the payment brands (including, but not limited to, Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. The Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law or regulations.

(b) Compliance with Standards. The Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://www.pcisecuritystandards.org/security_standards/index.php. The Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. The Contractor shall provide a letter of certification to attest to meeting this requirement within **seven (7) days** of the Contractor's receipt of the annual PCI DSS compliance report.

33. DATA BREACH OR LOSS.

(a) The Contractor shall comply with all applicable data protection, data security, data privacy and data breach notification laws, including but not limited to the *Breach of Personal Information Notification Act,* Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329.

(b) For Data and Confidential Information in the possession, custody, and control of the Contractor or its employees, agents, and/or subcontractors:

- The Contractor shall report unauthorized access, use, release, loss, destruction or disclosure of Data or Confidential Information ("Incident") to the Commonwealth within **two (2) hours** of when the Contractor knows of or reasonably suspects such Incident, and the Contractor must immediately take all reasonable steps to mitigate any potential harm or further access, use, release, loss, destruction or disclosure of such Data or Confidential Information.

- The Contractor shall provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the Commonwealth. At the Commonwealth's request, Contractor shall, at its sole expense, provide credit monitoring services to all individuals that may be impacted by any Incident requiring notice.

- The Contractor shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents. In addition, any citizens impacted by breach of data will be offered at least 12 months of credit monitoring at the expense of the Contractor.

(c) As to Data and Confidential Information fully or partially in the possession, custody, or control of the Contractor and the Commonwealth, the Contractor shall diligently perform all of the duties required in this section in cooperation with the Commonwealth, until the time at which a determination of responsibility for the Incident, and for subsequent action regarding the Incident, is made final.

34. INSURANCE.

(a) General. Unless otherwise indicated in the Solicitation, the Contractor shall maintain at its expense and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance, issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

- Workers' Compensation Insurance for all of the Contractor's employees and those of any subcontractor engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

- Commercial general liability insurance providing coverage from claims for damages for personal injury, death and property of others, including loss of use resulting from any property damage which may arise from its operations under this Contract, whether such operation be by the Contractor, by any agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than **$500,000** per person and **$2,000,000** per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or Supplies provided to the Commonwealth.

- Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology

activities) in the amount of **$2,000,000**, per accident/occurrence/annual aggregate.

- Professional Liability/Errors and Omissions Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Network/Cyber Liability Insurance (including coverage for Professional and Technology-Based Services Liability if not covered under Company's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of **$3,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Completed Operations Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Comprehensive crime insurance in an amount of not less than **$5,000,000** per claim.

(b) Certificate of Insurance. Prior to commencing Services under the Contract, and annually thereafter, the Contractor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days'** prior written notice has been given to the Commonwealth. Such cancellation or change shall not relieve the Contractor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Contractor agrees to maintain such insurance for the latter of the life of the Contract, or the life of any Purchase Orders issued under the Contract.

35. CONTRACTOR RESPONSIBILITY PROGRAM.

(a) For the purpose of these provisions, the term Contractor is defined as any person, including, but not limited to, a bidder, offeror, loan recipient, grantee or lessor, who has furnished or performed or seeks to furnish or perform, goods, Supplies, Services, leased space, construction or other activity, under a contract, grant, lease, Purchase Order or reimbursement agreement with the Commonwealth of Pennsylvania (Commonwealth). The term Contractor includes a permittee,

licensee, or any agency, political subdivision, instrumentality, public authority, or other public entity in the Commonwealth.

(b) The Contractor certifies, in writing, for itself and its subcontractors required to be disclosed or approved by the Commonwealth, that as of the date of its execution of this Bid/Contract, that neither the Contractor, nor any subcontractors, nor any suppliers are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its Bid/Contract, a written explanation of why such certification cannot be made.

(c) The Contractor also certifies, in writing, that as of the date of its execution of this Bid/Contract it has no tax liabilities or other Commonwealth obligations, or has filed a timely administrative or judicial appeal if such liabilities or obligations exist, or is subject to a duly approved deferred payment plan if such liabilities exist.

(d) The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the Contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or, to the best knowledge of the Contractor, any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such notification shall be made within **15 days** of the date of suspension or debarment.

(e) The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.

(f) The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

(g) The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the Internet at https://www.dgs.pa.gov/Pages/default.aspx or contacting the:

Department of General Services

Office of Chief Counsel
603 North Office Building
Harrisburg, PA 17125
Telephone No. (717) 783-6472
FAX No. (717) 787-9138

36. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS.

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor or its subsidiaries to the Commonwealth against any payments due the Contractor under any contract with the Commonwealth.

37. TAXES-FEDERAL, STATE AND LOCAL.

The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-7400001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

38. LIMITATION OF LIABILITY.

(a) General. The Contractor's liability to the Commonwealth under this Contract shall be limited to the greater of **$250,000** or the value of this Contract (including any amendments). This limitation will apply, except as otherwise stated in this section, regardless of the form of action, whether in contract or in tort, including negligence. This limitation does not, however, apply to any damages:

- for bodily injury;
- for death;
- for intentional injury;
- for damage to real property or tangible personal property for which the Contractor is legally liable;

- under **Section 42, Patent, Copyright, Trademark and Trade Secret Protection**;
- under **Section 33, Data Breach or Loss**; or
- under **Section 41, Virus, Malicious, Mischievous or Destructive Programming**.

(b) The Contractor will not be liable for consequential or incidental damages, except for damages as set forth in **paragraphs (a)(i)—(vii)** above, or as otherwise specified in the Contract.

39. COMMONWEALTH HELD HARMLESS.

(a) The Contractor shall indemnify the Commonwealth against any and all third party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its employees and agents under this Contract, provided the Commonwealth gives Contractor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act,* Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

(b) Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

40. SOVEREIGN IMMUNITY.

No provision of this Contract may be construed to waive or limit the sovereign immunity of the Commonwealth of Pennsylvania or its governmental sub-units.

41. VIRUS, MALICIOUS, MISCHIEVOUS OR DESTRUCTIVE PROGRAMMING.

(a) The Contractor shall be liable for any damages incurred by the Commonwealth if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive

programming. The Contractor's liability shall cease if the Commonwealth has not fully complied with its own software security standards.

(b) The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of Software, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

(d) The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

(e) The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

(f) The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

(g) The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the Commonwealth's anti-virus software or monitoring software on the Contractor's computers.

42. PATENT, COPYRIGHT, TRADEMARK AND TRADE SECRET PROTECTION.

(a) The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments,

officers or employees for the alleged infringement of any United States or foreign patents, copyrights, trademarks or trade dress, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act*, Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion and under the terms it deems appropriate, may delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement that prevents the Commonwealth from continuing to use the Developed Works as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests that the Commonwealth provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. If OAG does not delegate the defense of the matter, the Contractor's obligation to indemnify ceases. The Contractor, at its expense, will provide whatever cooperation OAG requests in the defense of the suit.

(b) The Contractor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Contractor certifies that, in all respects applicable to this Contract, it has exercised and will continue to exercise due diligence to ensure that all works produced under this Contract do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties. The Contractor also agrees to certify that work produced for the Commonwealth under this contract shall be free and clear from all claims of any nature.

(c) If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs awarded therein against the Commonwealth. If information and assistance are furnished by the Commonwealth at the Contractor's written request, it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

(d) If, in the Contractor's opinion, the products, materials, reports, studies, or computer programs furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a

misappropriation of trade secret, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense:

- substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs; or
- obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs.

(e) If any of the products, materials, reports, studies, or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, the Contractor shall, at its own expense and at its option, either procure the right to publish or continue use of such infringing products, materials, reports, studies, or computer programs, replace them with non-infringing items, or modify them so that they are no longer infringing.

(f) If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

- any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the deliverable;
- any license fee less an amount for the period of usage of any software; and
- the prorated portion of any service fees representing the time remaining in any period of service for which payment was made.

(g) Notwithstanding the above, the Contractor shall have no obligation for:

- modification of any product, service, or deliverable provided by the Commonwealth;
- any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, service, or deliverable;
- use of the product, service, or deliverable in other than its specified operating environment;
- the combination, operation, or use of the product, service, or deliverable with other products, services, or deliverables not provided by the Contractor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Contractor did not provide;
- infringement of a non-Contractor product alone;

- the Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract; or

- the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge.

(h) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Contractor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

43. CONTRACT CONSTRUCTION.

The provisions of this Contract shall be construed in accordance with the provisions of all applicable laws and regulations of the Commonwealth. However, by executing this Contract, the Contractor agrees that it has and will continue to abide by the intellectual property laws and regulations of the United States of America.

44. USE OF CONTRACTOR AND THIRD PARTY PROPERTY.

(a) Definitions.

- "Contractor Property" refers to Contractor-owned tangible and intangible property.

- "Third Party" refers to a party that licenses its property to Contractor for use under this Contract.

- "Third Party Property" refers to property licensed by the Contractor for use in its work under this Contract.

(b) Contractor Property shall remain the sole and exclusive property of the Contractor. Third Party Property shall remain the sole and exclusive property of the Third Party. The Commonwealth acquires rights to the Contractor Property and Third Party Property as set forth in this Contract.

- Where the Contractor Property or Third Party Property is integrated into the Supplies or Services which are not Developed Works, or the Contractor Property is otherwise necessary for the Commonwealth to attain the full benefit of the Supplies or Services in accordance with the terms of the Contract, the Contractor hereby grants to the Commonwealth a non-exclusive, fully-paid up, worldwide license to use the Contractor Property as necessary to meet the requirements of the Contract, including the rights to reproduce, distribute, publicly perform, display and create derivative works of the Contractor Property. These rights are granted for a duration

and to an extent necessary to meet the requirements under this Contract. If the Contractor requires a separate license agreement, such license terms shall include the aforementioned rights, be acceptable to the Commonwealth and include the applicable provisions set forth in these terms at **Attachment B**, ***Software/Services License Requirements Agreement Template***.

- If Third Party Property is integrated into the Supplies or Services which are not Developed Works, or the Third Party Property is otherwise necessary for the Commonwealth to attain the full benefit of the Supplies or Services in accordance with the terms of the Contract, the Contractor shall gain the written approval of the Commonwealth prior to the use of the Third Party Property or the integration of the Third Party Property into the Supplies or Services. Third Party Property approved by the Commonwealth is hereby licensed to the Commonwealth as necessary to meet the Contract requirements.

- If the Third Party requires a separate license agreement, the license terms shall be acceptable to the Commonwealth and include the applicable provisions set forth in these terms at ***Attachment B, Software/Services License Requirements Agreement Template***.

- If the use or integration of the Third Party Property is not approved in writing under this section, the Third Party Property shall be deemed to be licensed under paragraph (b)(i) above.

- If the Contract expires or is terminated for default pursuant to subsection 28(c) before the Contract requirements are complete, all rights are granted for a duration and for purposes necessary to facilitate Commonwealth's or a Commonwealth-approved vendor's completion of the Supplies, Services or Developed Works under this Contract. The Contractor, in the form used by Contractor in connection with the Supplies, Services, or Developed Works, shall deliver to Commonwealth the object code version of such Contractor Property, the Third Party Property and associated licenses immediately prior to such expiration or termination to allow the Commonwealth to complete such work.

- Where third party users are reasonably anticipated by the Contract, all users are granted the right to access and use Contractor Property for the purposes of and within the scope indicated in the Contract.

(c) The Commonwealth will limit its agents and contractors' use and disclosure of the Contractor Property as necessary to perform work on behalf of the Commonwealth.

(d) The parties agree that the Commonwealth, by acknowledging the Contractor Property, does not agree to any terms and conditions of the Contractor Property agreements that are inconsistent with or supplemental to this Contract.

(e) Reports. When a report is provided under this Contract, but was not developed specifically for the Commonwealth under this Contract, the ownership of the report will remain with the Contractor; provided, however, that the Commonwealth has the right to use, copy and distribute the report within the executive agencies of the Commonwealth.

45. USE OF COMMONWEALTH PROPERTY.

"Commonwealth Property" refers to Commonwealth-owned Software, Data and property (including intellectual property) and third party owned Software and property (including intellectual property) licensed to the Commonwealth.

(a) Confidentiality of Commonwealth Property. All Commonwealth Property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be considered confidential information under **Section 31, Confidentiality, Privacy, and Compliance**.

(b) License grant and restrictions. During the term of this Contract, Commonwealth grants to Contractor and its subcontractors for the limited purpose of providing the Services covered under this Contract, a limited, nonexclusive, nontransferable, royalty-free right (subject to the terms of any third party agreement to which the Commonwealth is a party) to access, use, reproduce, and modify Commonwealth Property in accordance with the terms of the Contract. The Commonwealth's license to Contractor is limited by the terms of this Contract.

- The Contractor hereby assigns to the Commonwealth its rights, if any, in any derivative works resulting from Contractor's modification of the Commonwealth Intellectual Property. Contractor agrees to execute any documents required to evidence this assignment and to waive any moral rights and rights of attribution provided for in Section 106A of Title 17 of the United States Code, the *Copyright Act of 1976,* as amended.

- Neither Contractor nor any of its subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Intellectual Property. Commonwealth hereby represents that it has the authority to provide the license grant and rights set forth in this section.

(c) Reservation of rights. All rights not expressly granted here to Contractor are reserved by the Commonwealth.

(d) Termination of Commonwealth license grant.

- *Rights Cease*. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract, all rights granted to Contractor under this section shall immediately cease.

- *Return Commonwealth Property*. Contractor shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Intellectual Property (including any related source code then in Contractor's possession or under its control) in the form in use as of the Effective Date of such expiration or termination (except that Commonwealth Data shall be turned over in a form acceptable to the Commonwealth).

- *List of utilized Commonwealth Property/Destruction*. Within **15 days** after termination, Contractor shall provide the Commonwealth with a current copy of the list of Commonwealth Intellectual Property in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth, in writing; provided, however, that Contractor may retain one archival copy of such Commonwealth Software, until final resolution of any actively asserted pending disputes between the Parties, such retention being for the sole purpose of resolving such disputes.

(e) Effect of license grant termination. Consistent with the provisions of this section, Contractor shall refrain from manufacturing, copying, marketing, distributing or using any Commonwealth Software or any other work which incorporates the Commonwealth Software.

(f) Commonwealth Property Protection.

- Contractor acknowledges Commonwealth's exclusive right, title and interest, including without limitation copyright and trademark rights, in and to Commonwealth Data, Commonwealth Software and the Developed Works developed under the provisions of this Contract, and Contractor shall not, directly or indirectly, do or cause to be done any act or thing contesting or in any way impairing or tending to impair any part of said right, title, and interest, and shall not use or disclose the Commonwealth Data, Commonwealth Software or the Developed Works without Commonwealth's written consent, which consent may be withheld by the Commonwealth for any reason.

- Contractor shall not, in any manner, represent that Contractor has any ownership interest in the Commonwealth Data, Commonwealth Software or the Developed Works.

46. OWNERSHIP OF DEVELOPED WORKS.

Unless otherwise specified in the Contract's Statement of Work, ownership of all Developed Works shall be in accordance with the provisions set forth in this section.

(a) Rules for usage for Developed Works.

- *Property of Contractor.* If Developed Works modify, improve, contain, or enhance application software programs or other materials generally licensed by the Contractor, then such Developed Works shall be the property of the Contractor, and Contractor hereby grants Commonwealth an irrevocable, nonexclusive, worldwide, fully paid-up license (to include source code and relevant documentation) in perpetuity to use, modify, execute, reproduce, display, perform, prepare derivative works from and distribute, within the Commonwealth, such Developed Works.

  (1) For purposes of distribution under the license grant created by this section, Commonwealth includes any government agency, department, instrumentality, division, unit or other office that is part of the Commonwealth of Pennsylvania, together with the State System of Higher Education (including any of its universities), any county, borough, commonwealth, city, municipality, town, township special purpose district, or other similar type of governmental instrumentality located within the geographical boundaries of the Commonwealth of Pennsylvania.

  (2) If federal funds are used in creation of the Developed Works, the Commonwealth also includes any other state government as well as the federal government.

- *Property of Commonwealth/licensor*. If the Developed Works modify, improve or enhance application software or other materials not licensed to the Commonwealth by the Contractor, then such modifications, improvements and enhancements shall be the property of the Commonwealth or its licensor.

(b) Copyright Ownership.

- *Works made for hire; general*. Except as indicated in paragraph (a)(i), above, Developed Works developed as part of the scope of work for the Project, including Developed Works developed by subcontractors, are the

sole and exclusive property of the Commonwealth and shall be considered "works made for hire" under the *Copyright Act of 1976*, as amended, 17 United States Code.

- *Assignment*. In the event that the Developed Works do not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns, all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such Developed Works to Commonwealth. Contractor further agrees that it will have its subcontractors assign, and upon their authorship or creation, expressly and automatically assigns all copyright interest, proprietary rights, trade secrets, and other right, title, and interest in and to the Developed Works to the Commonwealth.

- *Rights to Commonwealth*. Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the Developed Works in multiple copies, the right to distribute copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Developed Works and the right to display the Developed Works.

- *Subcontracts*. The Contractor further agrees that it will include the requirements of this section in any subcontractor or other agreement with third parties who in any way participate in the creation or development of Developed Works.

- *Completion or termination of Contract*. Upon completion or termination of this Contract, Developed Works, or completed portions thereof, shall immediately be delivered by Contractor to the Commonwealth.

- *Warranty of noninfringement*. Contractor represents and warrants that the Developed Works are original and do not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws and regulations of the United States.

(c) Patent ownership. Contractor and its subcontractors shall retain ownership to patentable items, patents, processes, inventions or discoveries (collectively, the Patentable Items) made by the Contractor during the performance of this Contract. Notwithstanding the foregoing, the Commonwealth shall be granted a nonexclusive, nontransferable, royalty free license to use or practice the Patentable Items. Commonwealth may disclose to third parties any such Patentable Items made by Contractor or any of its subcontractors under the scope of work for the

Project that have been previously publicly disclosed. Commonwealth understands and agrees that any third party disclosure will not confer any license to such Patentable Items.

(d) Federal government interests. Certain funding under this Contract may be provided by the federal government. Accordingly, the rights to Developed Works or Patentable Items of Contractors or subcontractors hereunder will be further subject to government rights as set forth in 37 C.F.R. Part 401, as amended, and other applicable law or regulations.

(e) Usage rights. Except as otherwise covered by this section either Party, in the ordinary course of conducting business, may use any ideas, concepts, know-how, methodologies, processes, components, technologies, algorithms, designs, modules or techniques relating to the Services.

(f) Contractor's copyright notice obligations. Contractor will affix the following Copyright Notice to the Developed Works developed under this section and all accompanying documentation: "*Copyright © [year] by the Commonwealth of Pennsylvania. All Rights Reserved*." This notice shall appear on all versions of the Developed Works delivered under this Contract and any associated documentation. It shall also be programmed into any and all Developed Works delivered hereunder so that it appears at the beginning of all visual displays of such Developed Works.

47. SOURCE CODE AND ESCROW ITEMS OBLIGATIONS.

(a) Source code. Simultaneously with delivery of the Developed Works to Commonwealth, Contractor shall deliver a true, accurate and complete copy of all source codes relating to the Developed Works.

(b) Escrow. To the extent that Developed Works and/or any perpetually-licensed software include application software or other materials generally licensed by the Contractor, Contractor agrees to place in escrow with an escrow agent copies of the most current version of the source code for the applicable software that is included as a part of the Services, including all updates, improvements, and enhancements thereof from time to time developed by Contractor.

(c) Escrow agreement. An escrow agreement must be executed by the parties, with terms acceptable to the Commonwealth, prior to deposit of any source code into escrow.

(d) Obtaining source code. Contractor agrees that upon the occurrence of any event or circumstance which demonstrates with reasonable certainty the inability or unwillingness of Contractor to fulfill its obligations to Commonwealth under this Contract, Commonwealth shall be able to obtain the source code of the then-current

source codes related to Developed Works and/or any Contractor Property placed in escrow under subsection (b), above, from the escrow agent.

48. LOCATION, STATUS AND DISPOSITION OF DATA.

Unless the Solicitation specifies otherwise:

- All Data must be stored within the United States;
- The Contractor shall be responsible for maintaining the privacy, security and integrity of Data in the Contractor's or its subcontractors' possession;
- All Data shall be provided to the Commonwealth upon request, in a form acceptable to the Commonwealth and at no cost;
- Any Data shall be destroyed by the Contractor at the Commonwealth's request; and
- Any Data shall be held for litigation or public records purposes by the Contractor at the Commonwealth's request, and in accordance with the security, privacy and accessibility requirements of this Contract.

49. PUBLICATION RIGHTS AND/OR COPYRIGHTS.

(a) Except as otherwise provided in **Section 46, Ownership of Developed Works**, the Contractor shall not publish any of the results of the work without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

(b) Except as otherwise provided in the Contract, the Commonwealth shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

50. CHANGE OF OWNERSHIP OR INSOLVENCY.

In the event that the Contractor should change ownership for any reason whatsoever, the Commonwealth shall have the exclusive option of continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for the full remaining term of this Contract, or continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for such period of time as is

necessary to replace the products, materials, reports, studies, or computer programs, or immediately terminating this Contract. Nothing in this section limits the Commonwealth's exercise of any rights that the Commonwealth may have under **Section 28, Termination**.

51. OFFICIALS NOT TO BENEFIT.

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

52. COMPLIANCE WITH LAWS.

(a) The Contractor shall comply with all federal, state and local laws, regulations and policies applicable to its Services or Supplies, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation.

(b) If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services or Supplies provided under this Contract, the Parties shall modify this Contract, via **Section 27, Changes**, to the extent reasonably necessary to:

- Ensure that such Services or Supplies will be in full compliance with such laws, regulations and policies; and
- Modify the rates applicable to such Services or Supplies, unless otherwise indicated in the Solicitation.

53. *THE AMERICANS WITH DISABILITIES ACT*.

During the term of this Contract, the Contractor agrees as follows:

(a) Pursuant to federal regulations promulgated under the authority of *The Americans With Disabilities Act*, 28 C.F.R.§ 35.101, *et seq*., the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this Contract or from activities provided for under this Contract. As a condition of accepting and executing this Contract, the Contractor agrees to comply with the *General Prohibitions Against Discrimination*, 28 C.F.R. § 35.130, and all other regulations promulgated under Title II of *The Americans With Disabilities Act* which are applicable to the benefits, services,

programs, and activities provided by the Commonwealth of Pennsylvania through Contracts with outside Contractors.

(b) The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from losses, damages, expenses claims, demands, suits, and actions brought by any party against the Commonwealth of Pennsylvania as a result of the Contractor's failure to comply with the provisions of subsection (a).

54. EXAMINATION OF RECORDS.

(a) The Contractor agrees to maintain, using its standard procedures, and in accordance with Generally Accepted Accounting Principles, books, records, documents, and other evidence pertaining to the charges under this Contract to the extent and in such detail as will properly reflect all charges for which reimbursement is claimed under the provisions of this Contract.

(b) The Contractor agrees to make available at the office of the Contractor at all reasonable times, and upon reasonable written notice, during the term of this Contract and the period set forth in subsection (c) below, any of the records for inspection, audit, or reproduction by any authorized Commonwealth representative. To the extent allowed by applicable laws or regulations, the Commonwealth agrees to maintain any documents so provided in accordance with the confidentiality provisions in **Section 31, Confidentiality, Privacy and Compliance**.

(c) The Contractor shall preserve and make available its records for a period of **three (3) years** from the date of final payment under this Contract.

- If this Contract is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of **three (3) years** from the date of any resulting final settlement.

- Non-privileged records which relate to litigation or the settlement of claims arising out of the performance of this Contract, or charges under this Contract as to which exception has been taken by the auditors, shall be retained by the Contractor until such litigation, claims, or exceptions have been finally resolved.

(d) Except for documentary evidence retained pursuant to paragraph (c)(ii) above, the Contractor may in fulfillment of its obligation to retain its records as required by this section substitute photographs, microphotographs, or other authentic reproductions of such records, after the expiration of **two (2) years** following the last day of the month of reimbursement to the Contractor of the invoice or voucher to which such records relate, unless a shorter period is authorized by the Commonwealth with the concurrence of its auditors.

(e) The provisions of this section shall be applicable to and included in each subcontract hereunder.

55. SINGLE AUDIT ACT OF 1984.

In compliance with the *Single Audit Act of 1984*, as amended, the Contractor agrees to the following:

(a) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in the most current version of *Government Auditing Standards* (Yellow Book).

(b) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984*, as amended, 31 U.S.C. § 7501, *et seq*., and all rules and regulations promulgated pursuant to the Act.

(c) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(d) The Contractor further agrees to comply with requirements that may be issued by the state agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984*, as amended.

56. AGENCY-SPECIFIC SENSITIVE AND CONFIDENTIAL COMMONWEALTH DATA (IF APPLICABLE).

(a) Contractor understands that its level of access may allow or require it to view or access highly sensitive and confidential Commonwealth and third party data. This data is subject to various state and federal laws, regulations and policies that vary from agency to agency, and from program to program within an agency. If applicable, prior to deployment of the Supplies or Services, the Contractor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth agency, including but not limited to, as necessary, HIPAA Business Associate Agreements. This sign-off document, a sample of which is attached as **Attachment C, *Sample Sign-off Document***, will include a description of the nature of the data which may be implicated based on the nature of the Contractor's access, and will incorporate the Business Associate Agreement if it is applicable.

(b) The Contractor hereby certifies and warrants that, after being informed by the Commonwealth agency of the nature of the data which may be implicated and prior to the deployment of the Supplies or Services, the Contractor is and shall remain

compliant with all applicable state and federal laws, regulations and policies regarding the data's protection, and with the requirements memorialized in every completed and signed sign-off document. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract.

(c) This section does not require a Commonwealth agency to exhaustively list the laws, regulations or policies to which implicated data is subject; the Commonwealth agency is obligated only to list the nature of the data implicated by the Contractor's access, to refer the Contractor to its privacy and security policies, and to specify requirements that are not otherwise inherent in compliance with applicable laws, regulations and policies.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Contract, its Exhibits, Appendices and Attachments, having to do with data privacy and security, including but not limited to the requirement that the Contractor comply with all applicable Commonwealth ITPs, which can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx.

(e) Contractor shall conduct additional background checks, in addition to those required in **Section 29, Background Checks**, as may be required by a Commonwealth agency in its sign-off documents. The Contractor shall educate and hold its agents, employees, contractors and subcontractors to standards at least as stringent as those contained in this Contract. The Contractor shall provide information regarding its agents, employees, contractors and subcontractors to the Commonwealth upon request.

57. FEDERAL REQUIREMENTS.

If applicable, the Contractor must receive and sign off on particular federal requirements that a Commonwealth agency may be required to include when utilizing federal funds to procure the Supplies and Services. This sign-off document, in addition to any applicable requirements of **Section 56, Agency-Specific Sensitive and Confidential Commonwealth Data**, will include a description of the required federal provisions, along with the applicable forms necessary for the Contractor and/or Software Licensor to execute, as necessary. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract. A sample sign-off document is attached to these Terms as **Attachment C, *Sample Sign-off Document***.

58. ADDITIONAL FEDERAL PROVISIONS.

Additional contract provisions may be incorporated into this Contract pursuant to federal law, regulation or policy.

59. ENVIRONMENTAL PROTECTION.

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law,* Act of June 22, 1937 (P.L. 1987, No. 394), as amended, 35 P.S. §§ 691.1—691.801; the *Solid Waste Management Act,* Act of July 7, 1980 (P.L. 380, No. 97), as amended, 35 P.S. §§ 6018.101—68.1003; and the *Dam Safety and Encroachment Act,* Act of November 26, 1978 (P.L. 1375, No. 325), as amended, 32 P.S. §§ 693.1—693.27.

60. NONDISCRIMINATION/SEXUAL HARASSMENT CLAUSE.

The Contractor agrees:

(a) In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the *Pennsylvania Human Relations Act* (PHRA) and applicable federal laws, against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

(b) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under the contract.

(c) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, in the provision of services under the contract.

(d) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against employees by reason of participation in or decision to refrain from participating in labor activities protected under the *Public Employee Relations Act*, *Pennsylvania Labor Relations Act* or *National Labor Relations Act*, as applicable and to the extent determined by entities charged with such Acts' enforcement, and shall comply with any provision of law establishing organizations as employees' exclusive representatives.

(e) The Contractor and each subcontractor shall establish and maintain a written nondiscrimination and sexual harassment policy and shall inform their employees

in writing of the policy. The policy must contain a provision that sexual harassment will not be tolerated and employees who practice it will be disciplined. Posting this Nondiscrimination/Sexual Harassment Clause conspicuously in easily-accessible and well-lighted places customarily frequented by employees and at or near where the contracted services are performed shall satisfy this requirement for employees with an established work site.

(f) The Contractor and each subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of PHRA and applicable federal laws, against any subcontractor or supplier who is qualified to perform the work to which the contract relates.

(g) The Contractor and each subcontractor represents that it is presently in compliance with and will maintain compliance with all applicable federal, state, and local laws, regulations and policies relating to nondiscrimination and sexual harassment. The Contractor and each subcontractor further represents that it has filed a Standard Form 100 Employer Information Report ("EEO-1") with the U.S. Equal Employment Opportunity Commission ("EEOC") and shall file an annual EEO-1 report with the EEOC as required for employers' subject to *Title VII* of the *Civil Rights Act of 1964*, as amended, that have 100 or more employees and employers that have federal government contracts or first-tier subcontracts and have 50 or more employees. The Contractor and each subcontractor shall, upon request and within the time periods requested by the Commonwealth, furnish all necessary employment documents and records, including EEO-1 reports, and permit access to their books, records, and accounts by the contracting agency and the Bureau of Diversity, Inclusion and Small Business Opportunities for purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause.

(h) The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.

(i) The Contractor's and each subcontractor's obligations pursuant to these provisions are ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor and each subcontractor shall have an obligation to inform the Commonwealth if, at any time during the term of the contract, it becomes aware of any actions or occurrences that would result in violation of these provisions.

(j) The Commonwealth may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

61. CONTRACTOR INTEGRITY PROVISIONS.

It is essential that those who seek to contract with the Commonwealth of Pennsylvania ("Commonwealth") observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the Commonwealth contracting and procurement process.

(a) Definitions. For purposes of these Contractor Integrity Provisions, the following terms shall have the meanings found in this section:

- "*Affiliate*" means two or more entities where (a) a parent entity owns more than fifty percent of the voting stock of each of the entities; or (b) a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the entities; or (c) the entities have a common proprietor or general partner.

- "*Consent*" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by prequalification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of the execution of this contract.

- "*Contractor*" means the individual or entity, that has entered into this contract with the Commonwealth.

- "*Contractor Related Parties*" means any affiliates of the Contractor and the Contractor's executive officers, Pennsylvania officers and directors, or owners of 5 percent or more interest in the Contractor.

- "*Financial Interest*" means either:

  (1) Ownership of more than a five percent interest in any business; or

  (2) Holding a position as an officer, director, trustee, partner, employee, or holding any position of management.

- "*Gratuity*" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the *Governor's Code of Conduct, Executive Order 1980-18*, the 4 Pa. Code § 7.153(b), shall apply.

- "*Non-bid Basis*" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(b) In furtherance of this policy, Contractor agrees to the following:

- Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or regulations, or other requirements applicable to Contractor or that govern contracting or procurement with the Commonwealth.

- Contractor shall establish and implement a written business integrity policy, which includes, at a minimum, the requirements of these provisions as they relate to the Contractor activity with the Commonwealth and Commonwealth employees and which is made known to all Contractor employees. Posting these Contractor Integrity Provisions conspicuously in easily-accessible and well-lighted places customarily frequented by employees and at or near where the contract services are performed shall satisfy this requirement.

- Contractor, its affiliates, agents, employees and anyone in privity with Contractor shall not accept, agree to give, offer, confer, or agree to confer or promise to confer, directly or indirectly, any gratuity or pecuniary benefit to any person, or to influence or attempt to influence any person in violation of any federal or state law, regulation, executive order of the Governor of Pennsylvania, statement of policy, management directive or any other published standard of the Commonwealth in connection with performance of work under this contract, except as provided in this contract.

- Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material under this contract, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest prior to Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.

- Contractor certifies to the best of its knowledge and belief that within the last **five (5) years** Contractor or Contractor Related Parties have not:

  (1) been indicted or convicted of a crime involving moral turpitude or business honesty or integrity in any jurisdiction;

(2) been suspended, debarred or otherwise disqualified from entering into any contract with any governmental agency;

(3) had any business license or professional license suspended or revoked;

(4) had any sanction or finding of fact imposed as a result of a judicial or administrative proceeding related to fraud, extortion, bribery, bid rigging, embezzlement, misrepresentation or anti-trust; and

(5) been, and is not currently, the subject of a criminal investigation by any federal, state or local prosecuting or investigative agency and/or civil anti-trust investigation by any federal, state or local prosecuting or investigative agency.

If Contractor cannot so certify to the above, then it must submit along with its bid, proposal or contract a written explanation of why such certification cannot be made and the Commonwealth will determine whether a contract may be entered into with the Contractor. The Contractor's obligation pursuant to this certification is ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to immediately notify the Commonwealth in writing if at any time during the term of the contract if becomes aware of any event which would cause the Contractor's certification or explanation to change. Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause if it learns that any of the certifications made herein are currently false due to intervening factual circumstances or were false or should have been known to be false when entering into the contract.

Contractor shall comply with the requirements of the *Lobbying Disclosure Act* (65 Pa. C.S. § 13A01, et seq.) regardless of the method of award. If this contract was awarded on a Non-bid Basis, Contractor must also comply with the requirements of the Section 1641 of the *Pennsylvania Election Code* (25 P.S. § 3260a).

When Contractor has reason to believe that any breach of ethical standards as set forth in law, the Governor's Code of Conduct, or these Contractor Integrity Provisions has occurred or may occur, including but not limited to contact by a Commonwealth officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify the Commonwealth contracting officer or the Office of the State Inspector General in writing.

- Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these Contractor Integrity Provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract, to include any extensions thereof. Contractor shall immediately notify the Commonwealth in writing of any actions for occurrences that would result in a violation of these Contractor Integrity Provisions. Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of the State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the Contractor. Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

- Contractor shall cooperate with the Office of the State Inspector General in its investigation of any alleged Commonwealth agency or employee breach of ethical standards and any alleged Contractor non-compliance with these Contractor Integrity Provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times and places. Contractor, upon the inquiry or request of an Inspector General, shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Office of the State Inspector General to Contractor's integrity and compliance with these provisions. Such information may include, but shall not be limited to, Contractor's business or financial records, documents or files of any type or form that refer to or concern this contract. Contractor shall incorporate this subsection in any agreement, contract or subcontract it enters into in the course of the performance of this contract/agreement solely for the purpose of obtaining subcontractor compliance with this provision. The incorporation of this provision in a subcontract shall not create privity of contract between the Commonwealth and any such subcontractor, and no third party beneficiaries shall be created thereby.

- For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these Provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of

all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise.

62. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS.

The Contractor and the Commonwealth recognize that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are subject to this Contract.

63. WARRANTIES.

Except as otherwise set forth in the Contract, the Contractor warrants that the Services, Supplies and Developed Works will conform in all material respects to the functional specifications for the Services, Supplies and Developed Works and/or the requirements of the Contract. The warranty period for the Services, Supplies and Developed Works shall be **90 days** from final acceptance. If third-party Services, Supplies or Developed Works are subject to a warranty that exceeds **90 days** from final acceptance, the longer warranty period shall apply. The Contractor shall correct any non-conformity within the warranty period specified herein.

(a) Disruption. The Contractor hereby represents and warrants to the Commonwealth that the Contractor will not cause, or take any action that, directly or indirectly, may cause a disruption of the Commonwealth's operations.

(b) Nonconformity. In the event of any nonconformity with the foregoing warranties, the Commonwealth will provide written notification of such nonconformity to the Contractor and the Contractor, at no cost to the Commonwealth, shall within **10 days'** notice of the nonconformity, commence work to remedy the nonconformity and shall work diligently, at no charge to the Commonwealth, until such time as the deliverable conforms, in all material respects, to the Service requirements and/or the functional specifications of the Developed Works set forth in this Contract. The Contractor shall have no obligation with respect to nonconformities arising out of:

- Modifications to Developed Works made by the Commonwealth;
- Use of the Developed Works not in accordance with the documentation or specifications applicable thereto;
- Failure by the Commonwealth to implement any corrections or enhancements made available by the Contractor;

- Combination of the Developed Works with any items not supplied or approved by the Contractor; or

- Failure of any software licensed under a separate license agreement to conform to its specifications or documentation.

(c) Industry standards. The Contractor hereby represents and warrants to the Commonwealth that the Services shall be performed in accordance with industry standards using the utmost care and skill.

(d) Right to perform. The Contractor hereby represents and warrants to the Commonwealth that the Contractor has the necessary legal rights, including licenses to third party products, tools or materials, to perform the Services and deliver the Developed Works under this Contract.

(e) Sole warranties. THE FOREGOING EXPRESS WARRANTIES ARE THE CONTRACTOR'S SOLE AND EXCLUSIVE WARRANTIES AND NO OTHER WARRANTIES, EXPRESS OR IMPLIED, SHALL APPLY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

64. RETAINAGE

(a) Contractor will submit invoices to the Commonwealth for deliverables on the deliverable due date. All deliverables are subject to the inspection and acceptance as given in paragraph 23 of this Contract. The Commonwealth will pay for approved and completed work within 30 calendar days of receipt of an invoice containing all information required for processing.

(b) The Commonwealth will retain 20% of the payment for each accepted deliverable. The Commonwealth will pay Contractor the retainage after final acceptance of all deliverables and includes the Submit Final Implementation Report deliverable.

(c) By accepting this Contract, the Contractor agrees to the delivery and acceptance requirements of this Contract. The delivery dates for the deliverables are listed in the Deliverable Break Down, provided as an attachment to this contract. The Parties may mutually agree to adjust or update any deliverable due date as conditions warrant over the duration of the project. If a deliverable due date is not met or is rejected, payment for the deliverable will be withheld by the Commonwealth. Any missed deliverable due date or deliverable rejection is subject to the conditions as specified in paragraph 23, Inspection and Acceptance, which defines the processes for curing a rejected deliverable. The Contractor will have 30 days to submit the deliverable or cure the rejected deliverable.

(d) If, at the end of the 30-day period specified in subsection (c) above, the Contractor still has not met the requirements for the deliverable associated with the due date, then the Commonwealth, at no additional expense and at its option, may either:

- Immediately terminate the Contract in accordance with Subsection 28(c) and with no opportunity to cure; or

- Order the Contractor to continue with no decrease in effort until the work is completed in accordance with the Contract and accepted by the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, any payment withholding and retainage will also continue until the work is completed.

65. SERVICE LEVELS.

(a) The Contractor shall comply with the procedures and requirements of the Service Level Agreements, if any, which are made part of this Contract.

(b) Where there are expressly defined Service Levels, Contractor shall measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the parties. Regardless of the presence or absence of expressly defined Service Levels, any failure to adequately or timely perform a Service may result in consequences under this Contract, up to and including Contract termination.

(c) The Commonwealth's acceptance of any financial credit incurred by the Contractor in favor of the Commonwealth for a Service Level default ("Service Level Credit") shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation other claims for liquidated damages, injunctive relief and termination rights; provided however, Service Level Credits paid would be credited against any such claims for damages.

66. FORCE MAJEURE.

(a) Neither party will incur any liability to the other if its performance of any obligation under this Contract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, severe weather conditions, civil disorders, natural disasters, fire, epidemics and quarantines, general strikes throughout the trade, and freight embargoes.

(b) The Contractor shall notify the Commonwealth orally within **five (5) days** and in writing within **10 days** of the date on which the Contractor becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance under the contract is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The Contractor shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as the Commonwealth may reasonably request. After receipt of such notification, the Commonwealth may elect to cancel the Contract, or to extend the time for performance as reasonably necessary to compensate for the Contractor's delay.

(c) In the event of a declared emergency by competent governmental authorities, the Commonwealth by notice to the Contractor, may suspend all or a portion of the Contract.

67. PUBLICITY/ADVERTISEMENT.

The Contractor shall not issue news releases, internet postings, advertisements, endorsements, or any other public communication without prior written approval of the Commonwealth, and then only in coordination with the Commonwealth. This includes the use of any trademark or logo.

68. TERMINATION ASSISTANCE.

(a) Upon the Commonwealth's request, Contractor shall provide termination assistance services (Termination Assistance Services) directly to the Commonwealth, or to any vendor designated by the Commonwealth. The Commonwealth may request termination assistance from the Contractor upon full or partial termination of the Contract and/or upon the expiration of the Contract term, including any renewal periods. Contractor shall take all necessary and appropriate actions to accomplish a complete, timely and seamless transition of any Services from Contractor to the Commonwealth, or to any vendor designated by the Commonwealth, without material interruption of or material adverse impact on the Services. Contractor shall cooperate with the Commonwealth and any new contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and timely transition of any Services.

(b) Such Termination Assistance Services shall first be rendered using resources included within the fees for the Services, provided that the use of such resources shall not adversely impact the level of service provided to the Commonwealth; then by resources already included within the fees for the Services, to the extent that the

Commonwealth permits the level of service to be relaxed; and finally, using additional resources at costs determined by the Parties via **Section 27, Changes**.

69. NOTICE.

Any written notice to any party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

70. *RIGHT-TO-KNOW LAW*.

(a) The Pennsylvania *Right-to-Know Law*, 65 P.S. §§ 67.101—3104, *as amended*, ("RTKL") applies to this Contract. For the purpose of this section, the term "the Commonwealth" shall refer to the contracting Commonwealth organization.

(b) If the Commonwealth needs the Contractor's assistance in any matter arising out of the RTKL that is related to this Contract, it shall notify the Contractor using the legal contact information provided in this Contract. The Contractor, at any time, may designate a different contact for such purpose upon reasonable prior written notice to the Commonwealth.

(c) Upon written notification from the Commonwealth that it requires the Contractor's assistance in responding to a request under the RTKL for information related to this Contract that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL ("Requested Information"), the Contractor shall:

- Provide the Commonwealth, within **10 days** after receipt of written notification, access to, and copies of, any document or information in the Contractor's possession arising out of this Contract that the Commonwealth reasonably believes is Requested Information and may be a public record under the RTKL; and

- Provide such other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this Contract.

(d) If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within **seven (7) days** of receiving the written notification, a written

statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

(e) The Commonwealth will rely upon the written statement from the Contractor in denying a RTKL request for the Requested Information unless the Commonwealth determines that the Requested Information is clearly not protected from disclosure under the RTKL. Should the Commonwealth determine that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information within **five (5) business days** of receipt of written notification of the Commonwealth's determination.

(f) If the Contractor fails to provide the Requested Information within the time period required by these provisions, the Contractor shall indemnify and hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

(g) The Commonwealth will reimburse the Contractor for any costs associated with complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL if the fee schedule is inapplicable.

(h) The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts. , however, the Contractor shall indemnify the Commonwealth for any legal expenses incurred by the Commonwealth as a result of such a challenge and shall hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth, regardless of the outcome of such legal challenge. As between the parties, the Contractor agrees to waive all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.

(i) The Contractor's duties relating to the RTKL are continuing duties that survive the expiration of this Contract and shall continue as long as the Contractor has Requested Information in its possession.

71. GOVERNING LAW.

This Contract shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. Except as set forth in **Section 30, Contract Controversies**, Commonwealth and Contractor agree that the courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof. Any legal action relating to this Contract must be

brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

72. CONTROLLING TERMS AND CONDITIONS.

The terms and conditions of this Contract shall be the exclusive terms of agreement between the Contractor and the Commonwealth. Other terms and conditions or additional terms and conditions included or referenced in the Contractor's website, quotations, invoices, business forms, click-through agreements, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Contractor, and not binding on the Commonwealth.

73. SMALL DIVERSE BUSINESS/SMALL BUSINESS COMMITMENT.

The Contractor shall meet and maintain the commitments to small diverse businesses in the Small Diverse Business and Small Business ("SDB/SB") portion of its Proposal. Any proposed change to a SDB/SB commitment must be submitted to the DGS Bureau of Diversity, Inclusion and Small Business Opportunities ("BDISBO"), which will make a recommendation as to a course of action to the Commonwealth Contracting Officer. Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Commonwealth Contracting Officer and BDISBO within **10 business days** at the end of each calendar quarter that the Contract is in effect.

74. POST-CONSUMER RECYCLED CONTENT; RECYCLED CONTENT ENFORCEMENT.

Except as specifically waived by the Department of General Services in writing, any products which are provided to the Commonwealth as a part of the performance of the Contract must meet the minimum percentage levels for total recycled content as specified by the Environmental Protection Agency in its Comprehensive Procurement Guidelines, which can be found at https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program.

The Contractor may be required, after delivery of the Contract item(s), to provide the Commonwealth with documentary evidence that the item(s) was in fact produced with the required minimum percentage of post-consumer and recovered material content.

75. SURVIVAL.

Sections 11, 30, 31, 33, 37, 38, 39, 41, 42, 45, 46, 47, 48, 49, 52, 54, 55, 56, 63, 67, 69, 70, 71 and 75 and any right or obligation of the parties in this Contract which, by its express terms or nature and context is intended to survive termination or expiration of this Contract, will survive any such termination or expiration shall survive the expiration or termination of the Contract.

Attachment A

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

Health Insurance Portability and Accountability Act (HIPAA) Compliance

WHEREAS, the [*name of program and/or Department*] (Covered Entity) and the **Contractor (Business Associate)**, intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be handled, used or disclosed only in accordance with this Business Associate Agreement (BAA), the Underlying Agreement and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**Business Associate Agreement**" or "**BAA**" shall mean this Agreement.

(c) "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(d) "**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended, Pub. L. No. 104-191.

(e) "**HITECH Act**" shall mean the Health Information Technology for Economic and Clinical Health (HITECH) Act, as amended, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(f) "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(g) "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(h) "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(i) "**Underlying Agreement**" shall mean Contract/Purchase Order # _____.

(j) "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. Changes in Law.

Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI.

Except as otherwise limited in this BAA, Business Associate shall be permitted to use or disclose PHI provided by or obtained by or obtained on behalf of Covered Entity to perform those functions, activities, or services for, or on behalf of, Covered Entity which are specified in Appendix A to this BAA, provided that such use or disclosure would not violate the HIPPA Rules if done by Covered Entity. Business Associate agrees to make uses, disclosures and requests for PHI consistent with Covered Entity's minimum policies and procedures.

4. Additional Purposes for Which Business Associate May Use or Disclose Information.

Business Associate shall not use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity for any other purposes except as required by law. Business Associate shall not use PHI to de-identify the information in accordance with 45 CFR § 164.514 (a)—(c) without the Covered Entity's express written authorization(s). Business

Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

5. Business Associate Obligations.

(a) **Limits on Use and Further Disclosure Established by Business Associate Agreement and Law**. Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of, Covered Entity shall not be further used or disclosed other than as permitted or required by BAA or as required by law.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this BAA that reasonably and appropriately protects the confidentiality, integrity, and availability of the PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity as required by Subpart C of 45 CFR Part 164. Appropriate safeguards shall include but are not limited to implementing:

- administrative safeguards required by 45 CFR § 164.308;
- physical safeguards as required by 45 CFR § 164.310;
- technical safeguards as required by 45 CFR § 164.312; and
- policies and procedures and document requirements as required by 45 CFR § 164.316.

(c) **Training and Guidance**. Business Associate shall provide annual training to relevant contractors, Subcontractors, employees, agents and representatives on how to prevent the improper use or disclosure of PHI. Business Associate shall also comply with annual guidance on the most effective and appropriate technical safeguards issued by the Secretary of Health and Human Services.

(d) **Reports of Improper Use or Disclosure or Breach**. Business Associate hereby agrees that it shall notify the Covered Entity's Project Officer and the Covered Entity's Legal Office within **two (2) days** of discovery of any use or disclosure of PHI not provided for or allowed by this BAA, including breaches of unsecured PHI as required by 45 CFR § 164.410. Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. Business Associate shall furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 CFR § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the **first day**

on which it is known to the Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.

(e) Business Associate agrees that if any of its employees, agents, contractors, subcontractors or representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information, Business Associate shall ensure that such employees, agents, contractors, subcontractors and representatives shall receive training on Business Associate's procedure for compliance with the HIPAA Rules. Business Associate Agrees that if any of its employees, agents, contractors, subcontractors or representatives use or disclose PHI received from, or created or received on behalf of, Covered Entity, or any derivative de-identified information in a manner not provided for in this BAA, Business Associate shall ensure that such employees, agents, contractors, subcontractors and representatives are sanctioned or prevented from accessing any PHI Business Associate receives from, or creates or receives on behalf of Covered Entity. Use or disclosure of PHI in a manner contrary to the terms of this BAA shall constitute a material breach of the Underlying Agreement.

(f) **Contractors, Subcontractors, Agents and Representatives**. In accordance with 45 CFR § 164.502(e)(1)(ii) and 45 CFR § 164.308(b)(2), if applicable, ensure that any contractors, subcontractors, agents and representatives that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. The existence of any contractors, subcontractors, agents and representatives shall not change the obligations of Business Associate to the Covered Entity under this BAA.

(g) **Reports of Security Incidents**. Business Associate hereby agrees that it shall notify, in writing, the Department's Project Officer within **two (2) days** of discovery of any Security Incident at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available.

(h) **Right of Access to PHI**. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within **10 business days** of receiving a written request from the Covered Entity or an authorized individual in accordance with the HIPAA Rules. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its contractors, subcontractors, agents or representatives, access to PHI, Business Associate shall notify Covered Entity of same within **five (5) business days**. Business Associate shall further conform with and meet all of the requirements of 45 CFR § 164.524.

(i) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a request from Covered Entity or from the individual for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available to the Covered Entity and incorporate the amendment to enable Covered Entity to comply with 45 CFR § 164.526. If any individual requests an amendment from Business Associate or its contractors, subcontractors, agents or representatives, Business Associate shall notify Covered Entity of same within **five (5) business days**.

(j) **Provide Accounting of Disclosures**. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 CFR § 164.528. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date which is **six (6) years** prior to the request. Business Associate shall make such record available to the individual or the Covered Entity within **10 business days** of a request for an accounting of disclosures and in accordance with 45 CFR § 164.528.

(k) **Access to Books and Records**. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, created or received by Business Associate on behalf of the Covered Entity, available to the Covered Entity and the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules.

(l) **Return or Destruction of PHI**. At termination of this BAA, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this BAA. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this BAA to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(m) **Maintenance of PHI**. Notwithstanding subsection 5(l) of this BAA, Business Associate and its contractors, subcontractors, agents and representatives shall retain all PHI throughout the term of the Underlying Agreement and shall continue to maintain the information required under subsection 5(j) of this BAA for a period of **six (6) years** after termination of the Underlying Agreement, unless Covered Entity and Business Associate agree otherwise.

(n) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this BAA or the HIPAA Rules. Business Associate further agrees to

mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this BAA or the Privacy Rule.

(o) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any contractor, Subcontractor, employee, agent and representative who violates this BAA or the HIPAA Rules.

(p) **Application of Civil and Criminal Penalties**. All Civil and Criminal Penalties under the HIPAA Rules shall apply to Business Associate's violation of any provision contained in the HIPAA Rules.

(q) **Breach Notification**. Business Associate shall comply with the Breach notification requirements of 45 CFR Part 164. In the event of a Breach requiring indemnification in accordance with subsection 5(v), below, Covered Entity may elect to directly comply with Breach notification requirements or require Business Associate to comply with all Breach notifications requirements of 45 CFR Part 164 on behalf of Covered Entity. If Covered Entity requires Business Associate to comply with Breach notification requirements, Business Associate shall provide Covered Entity with a detailed weekly, written report, starting one week following discovery of the Breach. The report shall include, at a minimum, Business Associate's progress regarding Breach notification and mitigation of the Breach. If Covered Entity elects to directly meet the requirements of 45 CFR Part 164, Business Associate shall be financially responsible to Covered Entity for all resulting costs and fees incurred by Covered Entity, including, but not limited to, labor, materials, or supplies. Covered Entity may at its sole option:

- Offset amounts otherwise due and payable to Business Associate under the Underlying Agreement; or
- Seek reimbursement of or direct payment to a third party of Covered Entity's costs and fees incurred under this subsection.

Business Associate shall make payment to Covered Entity (or a third party as applicable) within **30 days** from the date of Covered Entity's written notice to Business Associate.

(r) **Grounds for Breach**. Any non-compliance by Business Associate with this BAA or the HIPAA Rules will automatically be considered to be a breach of the Underlying Agreement.

(s) **Termination by Commonwealth**. Business Associate authorizes termination of this BAA or Underlying Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion that the Business Associate has violated a material term of this BAA.

(t) **Failure to Perform Obligations**. In the event Business Associate including its contractors, Subcontractors, agents and representatives fails, to perform its obligations under this BAA, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this BAA and applicable law.

(u) **Privacy Practices**. The Covered Entity will provide, and Business Associate shall immediately begin using and/or distributing to clients, any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date of this BAA, or as otherwise designated by the Program or Covered Entity. The Covered Entity retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change.

(v) **Indemnification**. Business Associate shall indemnify, defend and hold harmless Covered Entity from and all claims and actions, whether in law or equity, resulting from Business Associate's Breach or other violation of the HIPAA Rules (this includes but is not limited to Breach and violations by Business Associate's contractors, subcontractors, employees, agents and representatives). Additionally, Business Associate shall reimburse Covered Entity for any civil monetary penalties imposed on Covered Entity as a result of a Breach or violation cognizable under this subsection 5(v).

6. Obligations of Covered Entity.

(a) **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR § 164.520 (Appendix A to this BAA), as well as changes to such notice.

(b) **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) **Restrictions**. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR § 164.522 to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

7. Survival.

The requirements, rights and obligations created by this BAA shall survive the termination of the Underlying Agreement.

Appendix A to Attachment A,
Commonwealth of Pennsylvania Business Associate Agreement

Permitted Purposes for the Creation, Receipt, Maintenance, Transmission, Use and/or Disclosure of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of the Underlying Agreement.

2. Information to be disclosed to Business Associate: _____.

3. Use Shall Effectuate Purpose of Underlying Agreement: _____ may use and disclose PHI to the extent contemplated by the Underlying Agreement, and as permitted by law with Commonwealth approval.

Attachment B

PA Supplier ID Number: _____

SOFTWARE/SERVICES LICENSE REQUIREMENTS AGREEMENT
BETWEEN
THE COMMONWEALTH OF PENNSYLVANIA,
ACTING BY AND THROUGH THE GOVERNOR'S OFFICE OF ADMINISTRATION
AND

_____

This Software/Services License Requirements Agreement ("Agreement") by and between _____ (Licensor) and the **Commonwealth of Pennsylvania**, acting by and through the **Governor's Office of Administration** (Commonwealth) is effective the date the Agreement has been fully executed by the Licensor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained.

1. Order of Precedence.

The terms and conditions of this Agreement supplement, and to the extent a conflict exists, supersede and take precedence over the terms and conditions of the attached [insert exhibits that are to be made part of this Agreement]. The parties agree that the terms of this Agreement supersede and take precedence over the terms included in any quote, purchase order, terms of any shrink-wrap agreement included with the Licensed Products, terms of any click through agreement included with the Licensed Products or any other terms purported to apply to the Licensed Products. The products specified in Attachment 1, along with support and services for said products, shall be referred to as "Licensed Products."

2. Enterprise Language.

(a) The parties agree that more than one agency of the Commonwealth ("Commonwealth Agency") may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Commonwealth Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Commonwealth Agency seeking to use the Licensed Products.

(b) The parties agree that, if the licensee is a "Commonwealth Agency" as defined by Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C. S. § 103, the terms and conditions of this Agreement apply to the procurement of Licensed Products made by the Commonwealth, and that the terms and conditions of this Agreement become part of the purchase order or other procurement document without further need for execution.

3. List of Licensed Products.

(a) Attached hereto and made a part of this Agreement by reference is Attachment 1, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Commonwealth, the list of Licensed Products on Attachment 1 may be updated by the Licensor providing the Commonwealth with a revised Attachment 1 that adds the new product to the list. The Commonwealth, in its sole discretion, may consent either via written communication directly to the Licensor or, if applicable, providing the Commonwealth's reseller with a copy of the Licensor's notification to update Attachment 1.

(b) No amendment will be required to add a new Licensed Product to the list. If, however, the Licensor desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

4. Choice of Law/Venue.

This Agreement shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. The courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof.

5. Indemnification/Immunity.

The Commonwealth does not have the authority to and shall not indemnify any entity. The Commonwealth agrees to pay for any loss, liability or expense, which arises out of or relates to the Commonwealth's acts or omissions with respect to its obligations hereunder, where a final determination of liability on the part of the Commonwealth is established by a court of law or where settlement has been agreed to by the Commonwealth. This provision shall not be construed to limit the Commonwealth's rights, claims or defenses that arise as a matter of law or pursuant to any other provision of this Agreement. No provision in this Agreement shall be construed to limit the sovereign immunity of the Commonwealth.

6. Patent, Copyright, Trademark and Trade Secret Protection.

(a) The Licensor shall, at its expense, defend, indemnify and hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States patents, copyrights, trademarks or trade dress, or for a misappropriation of a United States trade secret arising out of performance of this Agreement ("Claim"), including all Licensed Products provided by the Licensor. For the purposes of this Agreement, "indemnify and hold harmless" shall

mean the Licensor's specific, exclusive, and limited obligation to (a) pay any judgments, fines and penalties finally awarded by a court of competent jurisdiction, governmental/administrative body or any settlements reached pursuant to a Claim and (b) reimburse the Commonwealth for its reasonable administrative costs or expenses, including without limitation reasonable attorney's fees, it necessarily incurs in handling the Claim. The Commonwealth agrees to give the Licensor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act,* Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P. S. §§ 732-101—732-506, the Office of Attorney General ("OAG") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion, and under the terms the OAG deems appropriate, may delegate its right of defense of a Claim. If the OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of the Licensor made in the defense of and/or settlement of a Claim. The Licensor shall not, without the Commonwealth's consent, enter into any settlement agreement which (a) states or implies that the Commonwealth has engaged in any wrongful or improper activity other than the innocent use of the material which is the subject of the Claim, (b) requires the Commonwealth to perform or cease to perform any act or relinquish any right, other than to cease use of the material which is the subject of the Claim, or (c) requires the Commonwealth to make a payment which the Licensor is not obligated by this Agreement to pay on behalf of the Commonwealth. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Licensor that, in the event it requests that the Commonwealth provide support to the Licensor in defending any such Claim, the Licensor shall reimburse the Commonwealth for all necessary expenses (including attorneys' fees, if such are made necessary by the Licensor's request) incurred by the Commonwealth for such support. If the OAG does not delegate to the Licensor the authority to control the defense and settlement of a Claim, the Licensor's obligation under this section ceases. The Licensor, at its own expense, shall provide whatever cooperation the OAG requests in the defense of the suit.

(b) The Licensor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Licensor certifies that, in all respects applicable to this Agreement, it has exercised and will continue to exercise due diligence to ensure that all Licensed Products provided under this Agreement do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties.

(c) If the defense of a Claim and the authority to control any potential settlements thereof is delegated to the Licensor, the Licensor shall pay all damages and costs finally awarded therein against the Commonwealth or agreed to by Licensor in any settlement. If information and assistance are furnished by the Commonwealth at the Licensor's written request, it shall be at the Licensor's expense, but the responsibility for such expense shall be only that within the Licensor's written authorization.

(d) If, in the Licensor's opinion, the Licensed Products furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a misappropriation of trade secret, then without diminishing the Licensor's obligation to satisfy any final award, the Licensor may, at its option and expense:

- substitute functional equivalents for the alleged infringing Licensed Products; or
- obtain the rights for the Commonwealth to continue the use of such Licensed Products.

(e) If any of the Licensed Products provided by the Licensor are in such suit or proceeding held to constitute infringement and the use thereof is enjoined, the Licensor shall, at its own expense and at its option:

- procure the right to continue use of such infringing products;
- replace them with non-infringing items; or
- modify them so that they are no longer infringing.

(f) If use of the Licensed Products is enjoined and the Licensor is unable to do any of the preceding set forth in subsection (e) above, the Licensor agrees to, upon return of the Licensed Products, refund to the Commonwealth:

- the license fee paid for the infringing Licensed Products, less the amount for the period of usage of any software; and
- the pro-rated portion of any maintenance fees representing the time remaining in any period of services for which payment was made.

(g) The obligations of the Licensor under this section continue without time limit and survive the termination of this Agreement.

(h) Notwithstanding the above, the Licensor shall have no obligation under this section for:

- modification of any Licensed Products provided by the Commonwealth or a third party acting under the direction of the Commonwealth;
- any material provided by the Commonwealth to the Licensor and incorporated into, or used to prepare any Licensed Products;

- use of any Licensed Product after the Licensor recommends discontinuation because of possible or actual infringement and has provided one of the remedies under subsection (e) or subsection (f) above;

- use of any Licensed Products in other than its specified operating environment;

- the combination, operation, or use of the Licensed Products with other products, services, or deliverables not provided by the Licensor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Licensor did not provide;

- infringement of a non-Licensed Product alone;

- the Commonwealth's use of any Licensed Product beyond the scope contemplated by the Agreement; or

- the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Licensor at no charge.

(i) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Licensor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

7. Virus, Malicious, Mischievous or Destructive Programming.

(a) The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

(b) The Licensor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Licensor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Licensor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of any Licensed Products, the Licensor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

8. Limitation of Liability.

(a) The Licensor's liability to the Commonwealth under this Agreement shall be limited the total dollar amount of purchase orders issued for Licensed Products and services covered by this Agreement during the during the **12-month** period prior to the event giving rise to the damage claim. This limitation does not apply to damages:

- for bodily injury;
- for death;
- for intentional injury;
- to real property or tangible personal property for which the Licensor is legally liable;
- Under Section 6, Patent, Copyright, Trade Secret and Trademark Protection;
- for damages related to a breach of the security of a system maintained or managed by the Licensor, including the costs for notification, mitigation and credit monitoring services required due to such breach; or
- under Section 7, Virus, Malicious, Mischievous or Destructive Programming.

(b) In no event will the Licensor be liable for consequential, indirect, or incidental damages unless otherwise specified in the Agreement.

9. Payment.

The Commonwealth will make purchase and make payment through a reseller contract or another procurement document, which shall control with regard to payment amounts and provisions.

10. Termination.

(a) The Licensor may not terminate for non-payment of an order issued through a reseller contract or another procurement document that controls payment.

(b) The Commonwealth may terminate this Agreement without cause by giving the Licensor **30 calendar days'** prior written notice ("Notice of Termination") whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth ("Termination for Convenience").

11. Background Checks.

(a) Upon prior written request by the Commonwealth, the Licensor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to the Commonwealth's IT facilities, either through on site or remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access by an IT employee and annually thereafter.

(b) Before the Commonwealth will permit an employee access to the Commonwealth's facilities, the Licensor must provide written confirmation to the office designated by the applicable Commonwealth Agency that the background check has been conducted. If, at any time, it is discovered that an employee has a criminal record that includes a felony or misdemeanor involving terrorist threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Licensor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the Commonwealth Agency consents, in writing, prior to the access being provided. The Commonwealth Agency may withhold its consent at its sole discretion. Failure of the Licensor to comply with the terms of this subsection may result in the default of the Licensor under its Agreement with the Commonwealth.

(c) The Commonwealth specifically reserves the right to conduct background checks over and above that described herein.

(d) Access to certain Capitol Complex buildings and other state office buildings is controlled by means of card readers and secured visitors' entrances. Commonwealth contracted personnel who have regular and routine business in Commonwealth worksites may be issued a photo identification or access badge subject to the requirements of the applicable Commonwealth Agency and the Department of General Services set forth in Enclosure 3 of Commonwealth Management Directive 625.10 Amended, *Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings*. The requirements, policy and procedures include a processing fee payable by the Licensor for contracted personnel photo identification or access badges.

12. Confidentiality.

(a) Definition. "Confidential Information:"

- For the Commonwealth. All data and other information of or in the possession of the Commonwealth or any Commonwealth Agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party.

- For the Licensor. All information identified in writing by the Licensor as confidential or proprietary to the Licensor or its subcontractors.

(b) Confidential Information. All Confidential Information of or relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Agreement, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents, subcontractors and personnel and to the officers, agents, subcontractors and personnel of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Agreement; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Agreement by such officers, agents, subcontractors and personnel and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement imposing equally or more stringent requirements for data privacy and security. Except to the extent provided otherwise by any applicable law, the obligations of this subsection (b) shall not apply with respect to information which:

- is developed by the other party without violating the disclosing party's proprietary rights,

- is or becomes publicly known (other than through unauthorized disclosure),

- is disclosed by the owner of such information to a Third Party free of any obligation of confidentiality,

- is already known by such party without an obligation of confidentiality other than pursuant to this Agreement or any confidentiality contract entered into before the Effective Date of the Agreement between the Commonwealth and the Licensor, or

- is rightfully received by the disclosing party free of any obligation of confidentiality.

(c) Obligations. Each party shall:

- Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

- Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

- Use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights.

- Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

(d) Cost of compliance; required disclosure. Each party shall bear the cost it incurs as a result of compliance with this section. The obligations in this section shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such disclosure or order in a timeframe to allow the non-disclosing party to resist the disclosure or order).

(e) Submitting Confidential Information to the Commonwealth. The Licensor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare an un-redacted version of the appropriate document;

- Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret;

- Prepare a signed written statement that states:

  (1) the attached document contains confidential or proprietary information or trade secrets;

(2) the Licensor is submitting the document in both redacted and un-redacted format in accordance with Section 707(b) of the *Right-to-Know Law*, 65 P.S. § 67.707(b); and

(3) the Licensor is requesting that the document be considered exempt under Section 708(b)(11) of the *Right-to-Know Law*, 65 P.S. § 67.708(b)(11) from public records requests; and

- Submit the **two (2)** documents with the signed written statement to the Commonwealth.

(f) Confidential Information at termination. Upon expiration or termination of this Agreement, or a purchase order or other procurement document for Licensed Products governed by the terms of this Agreement, and at any other time at the written request of a party, the other party must promptly return to such party all of such party's Confidential Information and Data (and all copies of this information) that is in the other party's possession or control, in whatever form. With regard to the Commonwealth's Confidential Information and/or Data, the Licensor shall comply with the requirements of subsection (e).

(g) Not confidential. Additionally, neither the Agreement nor any pricing information related to the Agreement, nor purchase orders issued pursuant to the Agreement, will be deemed confidential.

13. Sensitive Information

(a) The Licensor shall not publish or otherwise disclose, except to the Commonwealth or the Licensor's subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

(b) The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Agreement for any purpose not connected with the parties' Agreement responsibilities.

(c) The Licensor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Agreement including by:

- Maintaining a valid and up to date registrations and certifications; and

- Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

14. Agency-specific Sensitive and Confidential Commonwealth Data (If applicable).

(a) The Licensor understands that its level of access may allow it to view or access highly sensitive and confidential Commonwealth and third party data. This data is subject to various state and federal laws and policies that vary from Commonwealth Agency to Commonwealth Agency, and from program to program within a Commonwealth Agency. If applicable, prior to the issuance of a purchase order or other procurement document for a Licensed Product or the deployment of a Licensed Product on any Commonwealth Agency's facilities, the Licensor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth Agency, including but not limited to, as necessary, Business Associate Agreements as required by the *Health Insurance Portability and Accountability Act* (HIPAA), as amended, a sample of which is attached hereto as Attachment 3. This sign-off document (a sample of which is attached hereto as Attachment 4), will include a description of the nature of the data which may be implicated based on the nature of the Licensor's access, and will incorporate the HIPAA Business Associate Agreement if it is applicable.

(b) The Licensor hereby certifies and warrants that, after being informed by the Commonwealth Agency of the nature of the data which may be implicated and prior to the installation of the Licensed Products), the Licensor is and shall remain compliant with all applicable state and federal law and policy regarding the data's protection, and with the requirements memorialized in every completed and signed Sign-Off document. Every sign-off document completed by a Commonwealth Agency and signed by at least one signatory of the Licensor authorized to bind the Licensor is valid and is hereby integrated and incorporated by reference into this Agreement.

(c) This section does not require a Commonwealth Agency to exhaustively list the law to which implicated data is subject; the Commonwealth Agency is obligated only to list the nature of the data implicated by the Licensor's access, to refer the Licensor to its privacy and security policies, and to specify requirements that are not otherwise inherent in compliance with law and policy.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Agreement and its Attachments and Exhibits having to do with data privacy and security, including but not limited to the requirement that the Licensor comply with Attachment 2, *Requirements for Non-Commonwealth Hosting Applications/Services*, and all applicable Commonwealth Information Technology Policies (ITPs), which can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx.

(e) The Licensor shall conduct additional background checks, in addition to those required in Section 11 of this Agreement, as may be required by a Commonwealth Agency in its sign-off documents. The Licensor shall educate and hold its agents, employees, contractors and subcontractors to standards at least as stringent as those

contained in this Agreement. The Licensor shall provide information regarding its agents, employees, contractors and subcontractors to the Commonwealth upon request.

15. Publicity/Advertisement.

The Licensor must obtain written Commonwealth approval prior to mentioning the Commonwealth or a Commonwealth agency in an advertisement, endorsement, or any other type of publicity. This includes the use of any trademark or logo.

16. Portability.

The parties agree that a Commonwealth Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Commonwealth or to a Commonwealth contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Commonwealth Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

17. Taxes-Federal, State and Local Taxes-Federal, State and Local.

(a) The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

(b) The only interest the Commonwealth is authorized to pay is in accordance with Act of December 13, 1982, P.L. 1155, No. 266, as amended, 72 P. S. § 1507, (relating to Interest Penalties on Commonwealth Accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to Interest Penalties for Late Payments).

18. Commonwealth Audit Responsibilities.

(a) The Commonwealth will maintain, and promptly provide to the Licensor upon its request, accurate records regarding use of the Licensed Product by or for the

Commonwealth. If the Commonwealth becomes aware of any unauthorized use of all or any part of the Licensed Product, the Commonwealth will notify the Licensor promptly, providing reasonable details. The limit of the Commonwealth's responsibility for use of the Licensed Products by more individuals than are permitted by the licensing terms applicable to the Licensed Products shall be to purchase additional licenses and Maintenance and Support (if applicable) for such Licensed Products through a reseller contract or another procurement document.

(b) The Commonwealth will perform a self-audit upon the request of the Licensor, which request may not occur more often than annually, and report any change in user count (hereinafter "True up number"). The Commonwealth shall notify the Licensor of the True up number no later than **45 calendar days** after the request that the Commonwealth perform a self-audit. If the user count has increased, the Commonwealth will make an additional purchase of the Licensed Products through a reseller contract or another procurement document, which is equivalent to the additional users. This section sets out the sole license audit right under this Agreement.

19. *Right-to-Know Law*.

The Pennsylvania *Right-to-Know Law*, Act of February 14, 2008, P.L. 6, No. 3, 65 P.S. §§ 67.101—3104 ("RTKL"), applies to this Agreement.

20. Third Party Software.

If the Licensed Product utilizes or includes third party software and other copyrighted material and is subject, therefore, to additional licensing terms, acknowledgements or disclaimers compliance with this Agreement constitutes compliance with those third-party terms. The parties agree that the Commonwealth, by acknowledging third party software, does not agree to any terms and conditions of the third party software agreements that are inconsistent with or supplemental to this Agreement.

21. Attorneys' Fees.

The Commonwealth will not pay attorneys' fees incurred by or paid by the Licensor.

22. Controversies.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Agreement or a purchase order, the Licensor, within **six (6) months** after the claim accrues, must file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Licensor asserts a controversy exists. If the Licensor fails to file a claim or files an untimely claim, the Licensor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office

of General Counsel Dispute Resolution Program, https://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

(b) If the Licensor or the contracting officer requests mediation and the other party agrees, the contracting officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the contracting officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the contracting officer and the Licensor. The contracting officer shall send a written determination to the Licensor. If the contracting officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The contracting officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Licensor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Licensor shall proceed diligently with the performance of the Agreement or purchase order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Licensor pursuant to the terms of the Agreement, purchase order or other procurement document.

23. Insurance.

(a) The Licensor shall maintain at its expense, and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

- Workers' Compensation Insurance for all of the employees engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

- Commercial general liability insurance providing coverage from claims for damages for personal injury, death (including bodily injury), sickness or disease, accidental death and damage to and property of others, including loss of use resulting from any property damage which may arise from the Licensor's operations under this Agreement, whether such operation be by the Licensor, its agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an

amount not less than $500,000 per person and $2,000,000 per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or supplies provided to the Commonwealth.

- Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of $2,000,000, per accident/occurrence/annual aggregate.

- Technology Products Liability/Professional Liability/Errors & Omissions Insurance in the aggregate amount of not less than $2,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Comprehensive crime insurance in an amount of not less than $5,000,000 per claim.

- Information Security and Privacy Liability Insurance including Privacy Notification Costs (including coverage for Technology Professional Liability if not covered under the Licensor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $3,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

(b) Certificate of Insurance. Prior to providing Licensed Products under this Agreement, and annually thereafter, the Licensor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days**' prior written notice has been received by the Commonwealth. Such cancellation or change shall not relieve the Licensor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Licensor agrees to maintain such insurance for the life of any applicable purchase order issued pursuant to the Agreement.

24. Federal Requirements.

If applicable, in addition to the requirements set forth in Section 14 of this Agreement, the Licensor must receive and sign off on particular federal requirements that a Commonwealth agency may be required to include when utilizing federal funds to procure the Licensed Products. This sign-off document, in addition to any applicable requirements of Section 14 of this Agreement, will include a description of the required federal provisions, along with the applicable forms necessary for the Licensor execute, as necessary. The sign-off document, along with attachments, must be attached to the purchase order.

25. Signatures.

The fully executed Agreement may not contain ink signatures by the Commonwealth. In that event, the Licensor understands and agrees that the receipt of an electronically-printed Agreement with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in the Agreement. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

26. Travel.

The Licensor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Agreement or Statement of Work. If not otherwise specified in the Agreement or Statement of Work, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

27. Entire Agreement.

This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter hereof, and supersedes and integrates all prior discussions, agreements and understandings pertaining thereto. No modification of this Agreement will be effective unless in writing and signed by both Parties. Other terms and conditions or additional terms and conditions included or referenced in the Licensor's quotations, invoices, business forms, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Licensor and not binding on the Commonwealth.

28. Notice.

Any written notice to any party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States

mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

29. Survival.

The termination or expiration of this Agreement will not affect any provisions of this Agreement which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, confidentiality, term and termination, effect of termination, intellectual property, license compliance, limitation of liability, indemnification and privacy.

30. Waiver.

Failure to enforce any provision will not constitute a waiver.

31. Severability.

If any provision is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.

32. Nonexclusive Remedy.

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.

33. Integration.

This Agreement, including all Exhibits, Attachments and referenced documents, and any Purchase Orders referencing this Agreement, constitutes the entire agreement between the parties. No agent, representative, employee or officer of the Commonwealth or of the Licensor has authority to make any statement, agreement, or representation, oral or written, in connection with this Agreement, which in any way can be deemed to modify, add to, or detract from, or otherwise change or alter its terms and conditions. No negotiations between the parties, nor any custom or usage, shall be permitted to modify or contradict any of the terms and conditions of this Agreement. No modifications, alterations, changes, or waiver to this Agreement or any of its terms shall be valid or binding unless accomplished by a written amendment executed by the parties.

IN WITNESS WHEREOF, the Parties to this Agreement have executed it, through their respective duly authorized representatives.

Witness:	**Licensor:**
Signature Date	Signature Date
Printed Name	Printed Name
Title	Title

If a corporation, the Chairman, President, Vice-President, Senior Vice-President, Executive Vice-President, Assistant Vice-President, Chief Executive Officer and Chief Operating Officer must sign; if a sole proprietor, then the owner must sign; if a general or limited partnership, a general partner must sign; if a limited liability company, then a member must sign, unless it is a managed by a manager, then the manager must sign; otherwise a resolution indicating authority to bind the corporation must be attached to this Agreement.

COMMONWEALTH OF PENNSYLVANIA

GOVERNOR'S OFFICE OF ADMINISTRATION

See Section 25
Agency Head or Designee

APPROVED AS TO FORM AND LEGALITY:

See Section 25 Office of Chief Counsel	*See Section 25* Office of General Counsel

See Section 25
Office of Attorney General

APPROVED:

See Section 25
Office of the Budget, Office of Comptroller Operations

ATTACHMENT 1

LIST OF LICENSED PRODUCTS

With the consent of the Commonwealth, the Licensor may add additional Licensed Products to this attachment by providing Commonwealth with a new copy of this Attachment 1.

Licensed Product:

The Licensed Product includes (list all titles covered by this agreement):

ATTACHMENT 2
Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this Attachment 2 is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements.

1. The Licensor or its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Quote and Statement of Work.

2. The Licensor shall provide secure access to applicable levels of users via the internet.

3. The Licensor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4. The Licensor or its subcontractors shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements.

5. The Licensor shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **two (2) business days**. In the event of any impermissible disclosure unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one (1) hour** of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. The Licensor or the Licensor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and within at least **three (3) business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Licensor or the Licensor's subcontractor shall locate servers in a climate-controlled environment. The Licensor or the Licensor's contractor shall house all servers and equipment in an operational environment that meets industry standards

including climate control, fire and security hazard detection, electrical needs, and physical security.

9. The Licensor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The Licensor shall completely test and apply patches for all third-party software products in the server environment before release.

11. The Licensor shall comply with Attachment 2-B, SOC Reporting Requirements.

B. Security Requirements.

1. The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense on an annual basis.

2. The Licensor shall comply with the Commonwealth's directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.

3. The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4. The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The Licensor shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. The Licensor shall limit access to Commonwealth-specific systems and services and provide access only to those staff that must have access to provide services proposed.

7. The Licensor shall provide the Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in Attachment 2-A, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

C. Data Storage.

1. The Licensor shall store all Commonwealth data in the United States.

2. The Licensor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk. The Licensor shall protect their operational systems with applicable anti-virus, host

intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Licensor shall be solely responsible for applicable data storage required.

4. The Licensor shall take all commercially viable and applicable measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

5. The Licensor agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or a Licensor-owned electronic device.

6. The Licensor shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

D. Adherence to Policy.

1. The Licensor's support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Licensor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment 2-A.

3. The Licensor shall comply with all pertinent federal and state privacy regulations.

E. Closeout.

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency to the Commonwealth Software Reseller within **sixty (60) days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

ATTACHMENT 2-A

Information Technology Policies (ITPs)
for
Outsourced/Licensor(s)-hosted Solutions

ITP Number-Name	Policy Link
ITP_ACC001-Accessibility Policy	https://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030-Active Directory Architecture	https://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007-Enterprise Service Catalog	https://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010-Business Process Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS011-Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_bus011.pdf
ITP_BUS012-Artificial Intelligence General Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000-Enterprise Data and Information Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001-Database Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006-Commonwealth County Code Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009-e-Discovery Technology Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010-Business Intelligence Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011-Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012-Dashboard Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001-The Life Cycle of Records: General Policy Statement	https://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004-Management of Web Records	https://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005-System Design Review of Electronic Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006-Electronic Document Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1-Electronic Commerce Formats and Standards	https://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2-Electronic Commerce Interface Guidelines	https://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006-Business Engine Rules	https://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004-Internet Protocol Address Standards	https://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005-Commonwealth External and Internal Domain Name Services (DNS)	https://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001-Commonwealth of Pennsylvania Electronic Information Privacy Policy	https://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000-Information Security Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC002-Internet Accessible Proxy Servers and Services	https://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003-Enterprise Security Auditing and Monitoring	https://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004-Enterprise Web Application Firewall	https://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006-Commonwealth of Pennsylvania Electronic Signature Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007-Minimum Standards for IDs, Passwords and Multi-Factor Authentication	https://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008-Enterprise E-mail Encryption	https://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf

ITP Number-Name	Policy Link
ITP_SEC009-Minimum Contractor Background Checks Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf
ITP_SEC010-Virtual Private Network Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf
ITP_SEC011-Enterprise Policy and Software Standards for Agency Firewalls	https://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC013-Identity Protection and Access Management (IPAM) Architectural Standard and Identity Management Services	https://www.oa.pa.gov/Policies/Documents/itp_sec013.pdf
ITP_SEC015-Data Cleansing	https://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC017-Copa Policy for Credit Card Use for e-Government	https://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019-Policy and Procedures for Protecting Commonwealth Electronic Data	https://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC020-Encryption Standards for Data at Rest	https://www.oa.pa.gov/Policies/Documents/itp_sec020.pdf
ITP_SEC021-Security Information and Event Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023-Information Technology Security Assessment and Testing Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024-IT Security Incident Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025-Proper Use and Disclosure of Personally Identifiable Information (PII)	https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029-Physical Security Policy for IT Resources	https://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031-Encryption Standards for Data in Transit	https://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032-Enterprise Data Loss Prevention (DLP) Compliance Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034-Enterprise Firewall Rule Set	https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC037-Identity Proofing of Online Users	https://www.oa.pa.gov/Policies/Documents/itp_sec037.pdf
ITP_SEC038-Commonwealth Data Center Privileged User IAM Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP_SFT000-Software Development Life Cycle (SDLC) Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001-Software Licensing	https://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002-Commonwealth of PA Website Standards	https://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003-Geospatial Enterprise Service Architecture	https://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004-Geospatial Information Systems (GIS)	https://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005-Managed File Transfer (MFT)	https://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007-Office Productivity Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008-Enterprise Resource Planning (ERP) Management	https://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009-Application Development	https://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003-Off-Site Storage for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004-Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006-Commonwealth IT Resources Patching Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008-Server Virtualization Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010-Enterprise Services Maintenance Scheduling	https://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

ATTACHMENT 2-B

SOC Reporting Requirements

(a) Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to, engage, on an annual basis, an independent auditing firm to conduct each the following:

(i) A SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions;

(ii) A SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access or contain Commonwealth Data; and

(iii) A SOC for Cybersecurity report with respect to controls used by the Contractor setting forth the description and effectiveness of the Contractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

Pennsylvania's fiscal year begins July 1 and ends on June 30. Audits shall be submitted annually no later than July 31 of the current year. All reports shall reflect the conduct of the Contractor during the **12 months** of the Commonwealth's previous fiscal year, unless otherwise agreed to in writing by the Commonwealth.

(b) SOC 2 Type II report reports shall address the following:

(i) Security of Information and Systems;

(ii) Availability of Information and Systems;

(iii) Processing Integrity;

(iv) Confidentiality;

(v) Privacy; and

(vi) If applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

(c) At the request of the Commonwealth, the Contractor shall complete additional SOC for Cybersecurity audits in the event:

(i) repeated non-conformities are identified in any SOC report required by subsection (a); or

(ii) if the Contractor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.);

The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

(d) The Commonwealth may specify other or additional standards, certifications or audits it requires under any Purchase Orders or within an ITP.

(e) The Contractor shall adhere to SSAE 18 audit standards. The Contractor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Contractor shall comply with such updates which shall be reflected in the next annual report.

(f) In the event an audit reveals any non-conformity to SSAE standards, the Contractor shall provide the Commonwealth, within **45 calendar days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity. The corrective action plan shall provide, in detail:

(i) clear responsibilities of the personnel designated to resolve the non-conformity;

(ii) the remedial action to be taken by the Contractor or its subcontractor(s);

(iii) the dates when each remedial action is to be implemented; and

(iv) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

(g) The Commonwealth may in its sole discretion agree, in writing, to accept alternative and equivalent reports or certifications in lieu of a SOC report.

ATTACHMENT 3

COMMONWEALTH OF PENNSYLVANIA
***SAMPLE* BUSINESS ASSOCIATE AGREEMENT**
(Business Associate Agreements as provided by Agencies may differ)

WHEREAS, the _____ (Covered Entity) and _____(Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be handled, used or disclosed only in accordance with this Agreement, and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(c) "**HIPAA**" shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.

(d) "**HITECH Act**" shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV

of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(e) "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(f) "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(g) "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(h) "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. Changes in Law.

Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI.

The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

_____
_____
_____
_____
_____
_____
_____
_____
_____

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

4. BUSINESS ASSOCIATE OBLIGATIONS.

(a) **Limits on Use and Further Disclosure**. Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity other than as permitted or required by this Addendum, as requested by Covered Entity, or as required by law and agency guidance.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

(c) **Reports of Improper Use or Disclosure**. Business Associate hereby agrees that it shall report to _____at _____, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

(d) **Reports on Security Incidents**. In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* ("HITECH Act"), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____, **within two (2) days** of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.

(e) **Subcontractors and Agents**. At any time PHI is provided or made available to Business Associate subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

(f) **Right of Access to PHI**. Business Associate shall allow, for any PHI maintained in a designated record set, Covered Entity to have access to and copy an individual's PHI within **five (5) business days** of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and Covered Entity. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within **five (5) business days**. Business Associate shall further conform with all of the requirements of 45 C.F.R. § 164.524 and other applicable laws, including the HITECH Act, as amended, related regulations and agency guidance. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(f).

(g) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a written request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act , as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within **five (5) business days**.

(h) **Provide Accounting of Disclosures**. Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended) in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the Covered Entity within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(h).

(i) **Requests for Restriction**. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health

plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) **Access to Books and Records**. Business Associate shall make its internal practices, books and records relating to the use or disclosure of PHI received from, or created or received, by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.

(k) **Return or Destruction of PHI**. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(l) **Maintenance of PHI**. Notwithstanding subsection 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.

(n) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.

(o) **Grounds for Breach**. Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-

compliance. Commonwealth may elect to terminate Business Associate's contract for such breach.

(p) **Termination by Commonwealth**. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

(q) **Failure to Perform Obligations**. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.

(r) **Privacy Practices**. Covered Entity will provide Business Associate with all applicable forms, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

5. OBLIGATIONS OF COVERED ENTITY.

(a) **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change.

(b) **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware if such changes affect Business Associate's permitted or required uses and disclosures.

(c) **Restrictions**. Covered Entity shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) **Requests**. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule, all as amended, if done by Covered Entity.

6. MISCELLANEOUS.

(a) **Regulatory References**. A reference in this Addendum to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.

(b) **Amendment**. The parties agree to take such action as is necessary to amend this Addendum from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.

(c) **Conflicts**. In the event that any terms of this Agreement are inconsistent with the terms of the Agreement, then the terms of this Agreement shall control.

ATTACHMENT 4

Sign-Off Document No. ____, under Agreement No. _____
Between
[Licensor_____] and the Commonwealth of PA, [Agency]

[Licensor_____] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Software/Services License Requirements Agreement No. _____ between the Commonwealth and _____ (Licensor), and is subject to the terms of that Agreement.

1. Scope of Deployment (need not be entire agency):

1. Nature of Data implicated or potentially implicated:

2. Agency Policies to which Licensor. is subject (incorporated by reference):

3. Background checks (describe if necessary):

4. Additional requirements (describe with specificity):

5. Is Licensor a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person Signature and Date: _____

[Licensor_____]
Authorized Signatory and Date: _____

Attachment C

Sign-Off Document No. ____, under Agreement No. _____
Between
[Contractor_____] and the Commonwealth of PA, [Agency]

[Contractor_____] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Agreement No. _____ between the Commonwealth and _____ (Contractor), and is subject to the terms of that Agreement.

1. Scope of Deployment (need not be entire agency):

2. Nature of Data implicated or potentially implicated:

3. Agency Policies to which Contractor is subject (incorporated by reference):

4. Background checks (describe if necessary):

5. Additional requirements (describe with specificity):

6. Is Contractor a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person Signature and Date: _____

[Contractor_____]
Authorized Signatory and Date: _____

EXHIBIT B
TO
CONTRACT NO. 4400023325

Final Negotiated Technical Documents and Clarifications

This document contains aspects of the Contractor's Technical Submittal and the RFP that have been negotiated by the Commonwealth and the Contractor.

1. Software License.

The Commonwealth and the Contractor have negotiated and agreed upon a software license agreement which has been memorialized and incorporated as Attachment 1 to this Exhibit B.

2. Final Project Schedule

The Commonwealth and the Contractor have negotiated and agreed upon a final project schedule which has been memorialized and incorporated as Attachment 2 to this Exhibit B.

3. Project Deliverables

The Commonwealth and the Contractor have negotiated and agreed upon a final breakdown of project deliverables which has been memorialized and incorporated as Attachment 3 to this Exhibit B.

ATTACHMENT 1
to
EXHIBIT B

SOFTWARE/SERVICES LICENSE REQUIREMENTS AGREEMENT BETWEEN THE COMMONWEALTH OF PENNSYLVANIA AND BPro Inc.

This Software/Services License Requirements Agreement ("Agreement") by and between **BPro Inc.** (Licensor) and the **Commonwealth of Pennsylvania** (Commonwealth) is effective the date the Agreement has been fully executed by the Licensor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained.

1. Order of Precedence.

The terms and conditions of this Agreement supplement, the terms and conditions of Contract No. 4400023325. The parties agree that the terms of this Agreement supersede and take precedence over the terms included in any quote, purchase order, terms of any shrink-wrap agreement included with the Licensed Products, terms of any click through agreement included with the Licensed Products or any other terms purported to apply to the Licensed Products. The products specified in Appendix A, along with support and services for said products, shall be referred to as "Licensed Products."

2. Enterprise Language.

(a) The parties agree that more than one agency of the Commonwealth ("Commonwealth Agency") may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Commonwealth Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Commonwealth Agency seeking to use the Licensed Products.

(b) The parties agree that, if the licensee is a "Commonwealth Agency" as defined by Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C. S. § 103, the terms and conditions of this Agreement apply to the procurement of Licensed Products made by the Commonwealth, and that the terms and conditions of this Agreement become part of the purchase order or other procurement document without further need for execution.

3. List of Licensed Products.

(a) Attached hereto and made a part of this Agreement by reference is Appendix A, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Commonwealth, the list of Licensed Products on Appendix A may be updated by the Licensor providing the Commonwealth with a revised

Appendix A that adds the new product to the list. The Commonwealth, in its sole discretion, may consent either via written communication directly to the Licensor or, if applicable, providing the Commonwealth's reseller with a copy of the Licensor's notification to update Appendix A.

(b) No amendment will be required to add a new Licensed Product to the list. If, however, the Licensor desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

4. Choice of Law/Venue.

This Agreement shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. The courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof.

5. Indemnification/Immunity.

The Commonwealth does not have the authority to and shall not indemnify any entity. The Commonwealth agrees to pay for any loss, liability or expense, which arises out of or relates to the Commonwealth's acts or omissions with respect to its obligations hereunder, where a final determination of liability on the part of the Commonwealth is established by a court of law or where settlement has been agreed to by the Commonwealth. This provision shall not be construed to limit the Commonwealth's rights, claims or defenses that arise as a matter of law or pursuant to any other provision of this Agreement. No provision in this Agreement shall be construed to limit the sovereign immunity of the Commonwealth.

6. Patent, Copyright, Trademark and Trade Secret Protection.

(a) The Licensor shall, at its expense, defend, indemnify and hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States patents, copyrights, trademarks or trade dress, or for a misappropriation of a United States trade secret arising out of performance of this Agreement ("Claim"), including all Licensed Products provided by the Licensor. For the purposes of this Agreement, "indemnify and hold harmless" shall mean the Licensor's specific, exclusive, and limited obligation to (a) pay any judgments, fines and penalties finally awarded by a court of competent jurisdiction, governmental/administrative body or any settlements reached pursuant to a Claim and (b) reimburse the Commonwealth for its reasonable administrative costs or expenses, including without limitation reasonable attorney's fees, it necessarily incurs in handling the Claim. The Commonwealth agrees to give the Licensor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth*

Attorneys Act, Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P. S. §§ 732-101—732-506, the Office of Attorney General ("OAG") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion, and under the terms the OAG deems appropriate, may delegate its right of defense of a Claim. If the OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of the Licensor made in the defense of and/or settlement of a Claim. The Licensor shall not, without the Commonwealth's consent, enter into any settlement agreement which (a) states or implies that the Commonwealth has engaged in any wrongful or improper activity other than the innocent use of the material which is the subject of the Claim, (b) requires the Commonwealth to perform or cease to perform any act or relinquish any right, other than to cease use of the material which is the subject of the Claim, or (c) requires the Commonwealth to make a payment which the Licensor is not obligated by this Agreement to pay on behalf of the Commonwealth. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Licensor that, in the event it requests that the Commonwealth provide support to the Licensor in defending any such Claim, the Licensor shall reimburse the Commonwealth for all necessary expenses (including attorneys' fees, if such are made necessary by the Licensor's request) incurred by the Commonwealth for such support. If the OAG does not delegate to the Licensor the authority to control the defense and settlement of a Claim, the Licensor's obligation under this section ceases. The Licensor, at its own expense, shall provide whatever cooperation the OAG requests in the defense of the suit.

(b) The Licensor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Licensor certifies that, in all respects applicable to this Agreement, it has exercised and will continue to exercise due diligence to ensure that all Licensed Products provided under this Agreement do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties.

(c) If the defense of a Claim and the authority to control any potential settlements thereof is delegated to the Licensor, the Licensor shall pay all damages and costs finally awarded therein against the Commonwealth or agreed to by Licensor in any settlement. If information and assistance are furnished by the Commonwealth at the Licensor's written request, it shall be at the Licensor's expense, but the responsibility for such expense shall be only that within the Licensor's written authorization.

(d) If, in the Licensor's opinion, the Licensed Products furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a misappropriation of trade secret, then without diminishing the Licensor's obligation to satisfy any final award, the Licensor may, at its option and expense:

- substitute functional equivalents for the alleged infringing Licensed Products; or

- obtain the rights for the Commonwealth to continue the use of such Licensed Products.

(e) If any of the Licensed Products provided by the Licensor are in such suit or proceeding held to constitute infringement and the use thereof is enjoined, the Licensor shall, at its own expense and at its option:

- procure the right to continue use of such infringing products;

- replace them with non-infringing items; or

- modify them so that they are no longer infringing.

(f) If use of the Licensed Products is enjoined and the Licensor is unable to do any of the preceding set forth in subsection (e) above, the Licensor agrees to, upon return of the Licensed Products, refund to the Commonwealth:

- the license fee paid for the infringing Licensed Products, less the amount for the period of usage of any software; and

- the pro-rated portion of any maintenance fees representing the time remaining in any period of services for which payment was made.

(g) The obligations of the Licensor under this section continue without time limit and survive the termination of this Agreement.

(h) Notwithstanding the above, the Licensor shall have no obligation under this section for:

- modification of any Licensed Products provided by the Commonwealth or a third party acting under the direction of the Commonwealth;

- any material provided by the Commonwealth to the Licensor and incorporated into, or used to prepare any Licensed Products;

- use of any Licensed Product after the Licensor recommends discontinuation because of possible or actual infringement and has provided one of the remedies under subsection (e) or subsection (f) above;

- use of any Licensed Products in other than its specified operating environment;

- the combination, operation, or use of the Licensed Products with other products, services, or deliverables not provided by the Licensor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Licensor did not provide;

- infringement of a non-Licensed Product alone;

- the Commonwealth's use of any Licensed Product beyond the scope contemplated by the Agreement; or

- the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Licensor at no charge.

(i) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Licensor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

7. Virus, Malicious, Mischievous or Destructive Programming.

(a) The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

(b) The Licensor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Licensor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Licensor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of any Licensed Products, the Licensor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

8. Limitation of Liability.

(a) The Licensor's liability to the Commonwealth under this Agreement shall be limited the total dollar amount of purchase orders issued for Licensed Products and services covered by this Agreement during the during the **12-month** period prior to

the event giving rise to the damage claim. This limitation does not apply to damages:

- for bodily injury;
- for death;
- for intentional injury;
- to real property or tangible personal property for which the Licensor is legally liable;
- Under Section 6, Patent, Copyright, Trade Secret and Trademark Protection;
- for damages related to a breach of the security of a system maintained or managed by the Licensor, including the costs for notification, mitigation and credit monitoring services required due to such breach; or
- under Section 7, Virus, Malicious, Mischievous or Destructive Programming.

(b) In no event will the Licensor be liable for consequential, indirect, or incidental damages unless otherwise specified in the Agreement.

9. Payment.

The Commonwealth will make purchase and make payment through a reseller contract or another procurement document, which shall control with regard to payment amounts and provisions.

10. Termination.

(a) The Licensor may not terminate for non-payment of an order issued through a reseller contract or another procurement document that controls payment.

(b) The Commonwealth may terminate this Agreement without cause by giving the Licensor **30 calendar days'** prior written notice ("Notice of Termination") whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth ("Termination for Convenience").

11. Background Checks.

(a) Upon prior written request by the Commonwealth, the Licensor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to the Commonwealth's

IT facilities, either through on site or remote access. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access by an IT employee and annually thereafter.

(b) Before the Commonwealth will permit an employee access to the Commonwealth's facilities, the Licensor must provide written confirmation to the office designated by the applicable Commonwealth Agency that the background check has been conducted. If, at any time, it is discovered that an employee has a criminal record that includes a felony or misdemeanor involving terrorist threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Licensor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the Commonwealth Agency consents, in writing, prior to the access being provided. The Commonwealth Agency may withhold its consent at its sole discretion. Failure of the Licensor to comply with the terms of this subsection may result in the default of the Licensor under its Agreement with the Commonwealth.

(c) The Commonwealth specifically reserves the right to conduct background checks over and above that described herein.

(d) Access to certain Capitol Complex buildings and other state office buildings is controlled by means of card readers and secured visitors' entrances. Commonwealth contracted personnel who have regular and routine business in Commonwealth worksites may be issued a photo identification or access badge subject to the requirements of the applicable Commonwealth Agency and the Department of General Services set forth in Enclosure 3 of Commonwealth Management Directive 625.10 Amended, *Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings*. The requirements, policy and procedures include a processing fee payable by the Licensor for contracted personnel photo identification or access badges.

12. Confidentiality.

(a) Definition. "Confidential Information:"

- For the Commonwealth. All data and other information of or in the possession of the Commonwealth or any Commonwealth Agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party.

- For the Licensor. All information identified in writing by the Licensor as confidential or proprietary to the Licensor or its subcontractors.

(b) Confidential Information. All Confidential Information of or relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Agreement, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents, subcontractors and personnel and to the officers, agents, subcontractors and personnel of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Agreement; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Agreement by such officers, agents, subcontractors and personnel and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement imposing equally or more stringent requirements for data privacy and security. Except to the extent provided otherwise by any applicable law, the obligations of this subsection (b) shall not apply with respect to information which:

- is developed by the other party without violating the disclosing party's proprietary rights,
- is or becomes publicly known (other than through unauthorized disclosure),
- is disclosed by the owner of such information to a Third Party free of any obligation of confidentiality,
- is already known by such party without an obligation of confidentiality other than pursuant to this Agreement or any confidentiality contract entered into before the Effective Date of the Agreement between the Commonwealth and the Licensor, or
- is rightfully received by the disclosing party free of any obligation of confidentiality.

(c) Obligations. Each party shall:

- Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

- Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

- Use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights.

- Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

(d) Cost of compliance; required disclosure. Each party shall bear the cost it incurs as a result of compliance with this section. The obligations in this section shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such disclosure or order in a timeframe to allow the non-disclosing party to resist the disclosure or order).

(e) Submitting Confidential Information to the Commonwealth. The Licensor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare an un-redacted version of the appropriate document;

- Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret;

- Prepare a signed written statement that states:

  (1) the attached document contains confidential or proprietary information or trade secrets;

  (2) the Licensor is submitting the document in both redacted and un-redacted format in accordance with Section 707(b) of the *Right-to-Know Law*, 65 P.S. § 67.707(b); and

(3) the Licensor is requesting that the document be considered exempt under Section 708(b)(11) of the *Right-to-Know Law*, 65 P.S. § 67.708(b)(11) from public records requests; and

- Submit the **two (2)** documents with the signed written statement to the Commonwealth.

(f) Confidential Information at termination. Upon expiration or termination of this Agreement, or a purchase order or other procurement document for Licensed Products governed by the terms of this Agreement, and at any other time at the written request of a party, the other party must promptly return to such party all of such party's Confidential Information and Data (and all copies of this information) that is in the other party's possession or control, in whatever form. With regard to the Commonwealth's Confidential Information and/or Data, the Licensor shall comply with the requirements of subsection (e).

(g) Not confidential. Additionally, neither the Agreement nor any pricing information related to the Agreement, nor purchase orders issued pursuant to the Agreement, will be deemed confidential.

13. Sensitive Information

(a) The Licensor shall not publish or otherwise disclose, except to the Commonwealth or the Licensor's subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

(b) The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Agreement for any purpose not connected with the parties' Agreement responsibilities.

(c) The Licensor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Agreement including by:

- Maintaining a valid and up to date registrations and certifications; and

- Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

14. Agency-specific Sensitive and Confidential Commonwealth Data (If applicable).

(a) The Licensor understands that its level of access may allow it to view or access highly sensitive and confidential Commonwealth and third party data. This data is

subject to various state and federal laws and policies that vary from Commonwealth Agency to Commonwealth Agency, and from program to program within a Commonwealth Agency. If applicable, prior to the issuance of a purchase order or other procurement document for a Licensed Product or the deployment of a Licensed Product on any Commonwealth Agency's facilities, the Licensor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth Agency, including but not limited to, as necessary, Business Associate Agreements as required by the *Health Insurance Portability and Accountability Act* (HIPAA), as amended, a sample of which is attached hereto as Appendix C. This sign-off document (a sample of which is attached hereto as Appendix D), will include a description of the nature of the data which may be implicated based on the nature of the Licensor's access, and will incorporate the HIPAA Business Associate Agreement if it is applicable.

(b) The Licensor hereby certifies and warrants that, after being informed by the Commonwealth Agency of the nature of the data which may be implicated and prior to the installation of the Licensed Products), the Licensor is and shall remain compliant with all applicable state and federal law and policy regarding the data's protection, and with the requirements memorialized in every completed and signed Sign-Off document. Every sign-off document completed by a Commonwealth Agency and signed by at least one signatory of the Licensor authorized to bind the Licensor is valid and is hereby integrated and incorporated by reference into this Agreement.

(c) This section does not require a Commonwealth Agency to exhaustively list the law to which implicated data is subject; the Commonwealth Agency is obligated only to list the nature of the data implicated by the Licensor's access, to refer the Licensor to its privacy and security policies, and to specify requirements that are not otherwise inherent in compliance with law and policy.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Agreement and its Appendices having to do with data privacy and security, including but not limited to the requirement that the Licensor comply with Appendix B, *Requirements for Non-Commonwealth Hosting Applications/Services*, and all applicable Commonwealth Information Technology Policies (ITPs), which can be found at https://www.oa.pa.gov/Policies/Pages/itp.aspx.

(e) The Licensor shall conduct additional background checks, in addition to those required in Section 11 of this Agreement, as may be required by a Commonwealth Agency in its sign-off documents. The Licensor shall educate and hold its agents, employees, contractors and subcontractors to standards at least as stringent as those contained in this Agreement. The Licensor shall provide information regarding its agents, employees, contractors and subcontractors to the Commonwealth upon request.

15. Publicity/Advertisement.

The Licensor must obtain written Commonwealth approval prior to mentioning the Commonwealth or a Commonwealth agency in an advertisement, endorsement, or any other type of publicity. This includes the use of any trademark or logo.

16. Portability.

The parties agree that a Commonwealth Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Commonwealth or to a Commonwealth contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Commonwealth Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

17. Taxes-Federal, State and Local Taxes-Federal, State and Local.

(a) The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

(b) The only interest the Commonwealth is authorized to pay is in accordance with Act of December 13, 1982, P.L. 1155, No. 266, as amended, 72 P. S. § 1507, (relating to Interest Penalties on Commonwealth Accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to Interest Penalties for Late Payments).

18. Commonwealth Audit Responsibilities.

(a) The Commonwealth will maintain, and promptly provide to the Licensor upon its request, accurate records regarding use of the Licensed Product by or for the Commonwealth. If the Commonwealth becomes aware of any unauthorized use of all or any part of the Licensed Product, the Commonwealth will notify the Licensor promptly, providing reasonable details. The limit of the Commonwealth's responsibility for use of the Licensed Products by more individuals than are

permitted by the licensing terms applicable to the Licensed Products shall be to purchase additional licenses and Maintenance and Support (if applicable) for such Licensed Products through a reseller contract or another procurement document.

(b) The Commonwealth will perform a self-audit upon the request of the Licensor, which request may not occur more often than annually, and report any change in user count (hereinafter "True up number"). The Commonwealth shall notify the Licensor of the True up number no later than **45 calendar days** after the request that the Commonwealth perform a self-audit. If the user count has increased, the Commonwealth will make an additional purchase of the Licensed Products through a reseller contract or another procurement document, which is equivalent to the additional users. This section sets out the sole license audit right under this Agreement.

19. *Right-to-Know Law*.

The Pennsylvania *Right-to-Know Law*, Act of February 14, 2008, P.L. 6, No. 3, 65 P.S. §§ 67.101—3104 ("RTKL"), applies to this Agreement.

20. Third Party Software.

If the Licensed Product utilizes or includes third party software and other copyrighted material and is subject, therefore, to additional licensing terms, acknowledgements or disclaimers compliance with this Agreement constitutes compliance with those third-party terms. The parties agree that the Commonwealth, by acknowledging third party software, does not agree to any terms and conditions of the third party software agreements that are inconsistent with or supplemental to this Agreement.

21. Attorneys' Fees.

Each Party is responsible for their own attorneys' fees subject to other provisions of this License Agreement and Contract No. 4400023325.

22. Controversies.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Agreement or a purchase order, the Licensor, within **six (6) months** after the claim accrues, must file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Licensor asserts a controversy exists. If the Licensor fails to file a claim or files an untimely claim, the Licensor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, https://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

(b) If the Licensor or the contracting officer requests mediation and the other party agrees, the contracting officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the contracting officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the contracting officer and the Licensor. The contracting officer shall send a written determination to the Licensor. If the contracting officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The contracting officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Licensor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Licensor shall proceed diligently with the performance of the Agreement or purchase order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Licensor pursuant to the terms of the Agreement, purchase order or other procurement document.

23. Insurance.

(a) The Licensor shall maintain at its expense, and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

- Workers' Compensation Insurance for all of the employees engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

- Commercial general liability insurance providing coverage from claims for damages for personal injury, death (including bodily injury), sickness or disease, accidental death and damage to and property of others, including loss of use resulting from any property damage which may arise from the Licensor's operations under this Agreement, whether such operation be by the Licensor, its agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than $500,000 per person and $2,000,000 per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the

Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or supplies provided to the Commonwealth.

- Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of $2,000,000, per accident/occurrence/annual aggregate.

- Technology Products Liability/Professional Liability/Errors & Omissions Insurance in the aggregate amount of not less than $2,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

- Comprehensive crime insurance in an amount of not less than $5,000,000 per claim.

- Information Security and Privacy Liability Insurance including Privacy Notification Costs (including coverage for Technology Professional Liability if not covered under the Licensor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $3,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

(b) Certificate of Insurance. Prior to providing Licensed Products under this Agreement, and annually thereafter, the Licensor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days**' prior written notice has been received by the Commonwealth. Such cancellation or change shall not relieve the Licensor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Licensor agrees to maintain such insurance for the life of any applicable purchase order issued pursuant to the Agreement.

24. Federal Requirements.

If applicable, in addition to the requirements set forth in Section 14 of this Agreement, the Licensor must receive and sign off on particular federal requirements that a

Commonwealth agency may be required to include when utilizing federal funds to procure the Licensed Products. This sign-off document, in addition to any applicable requirements of Section 14 of this Agreement, will include a description of the required federal provisions, along with the applicable forms necessary for the Licensor execute, as necessary. The sign-off document, along with attachments, must be attached to the purchase order.

25. Travel.

The Licensor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Agreement or Statement of Work. If not otherwise specified in the Agreement or Statement of Work, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

26. Entire Agreement.

This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter hereof, and supersedes and integrates all prior discussions, agreements and understandings pertaining thereto. No modification of this Agreement will be effective unless in writing and signed by both Parties. Other terms and conditions or additional terms and conditions included or referenced in the Licensor's quotations, invoices, business forms, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Licensor and not binding on the Commonwealth.

27. Notice.

Any written notice to any party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

28. Survival.

The termination or expiration of this Agreement will not affect any provisions of this Agreement which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, confidentiality, term and termination, effect of termination, intellectual property, license compliance, limitation of liability, indemnification and privacy.

29. Waiver.

Failure to enforce any provision will not constitute a waiver.

30. Severability.

If any provision is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.

31. Nonexclusive Remedy.

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.

APPENDIX A

LIST OF LICENSED PRODUCTS

With the consent of the Commonwealth, the Licensor may add additional Licensed Products to this attachment by providing Commonwealth with a new copy of this Appendix A.

Licensed Product:

The Licensed Product includes (list all titles covered by this agreement):

1. 1 TotalVote, comprised of the following functional modules:
    - 1.1. Voter registration
    - 1.2. Election Management
    - 1.3. Notice Management
    - 1.4. Data Generator - Reports
    - 1.5. Utilities & Roles & Permissions
    - 1.6. Interfaces
    - 1.7. Petition with e-signature capture
    - 1.8. Election Night Reporting (years 1-4 cost is $97,200.00/year)
    - 1.9. Accessible Ballot Marking
    - 1.10. Campaign Finance
    - 1.11. Lobbying Disclosure
    - 1.12. SMS/E-Mail Notification
2. TotalAddress

APPENDIX B
Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this ~~Attachment 2~~Appendix B is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements.

1. The Licensor or its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Quote and Statement of Work.

2. The Licensor shall provide secure access to applicable levels of users via the internet.

3. The Licensor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4. The Licensor or its subcontractors shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements.

5. The Licensor shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **two (2) business days**. In the event of any impermissible disclosure unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one (1) hour** of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. The Licensor or the Licensor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and within at least **three (3) business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Licensor or the Licensor's subcontractor shall locate servers in a climate-controlled environment. The Licensor or the Licensor's contractor shall house all servers and equipment in an operational environment that meets industry standards

including climate control, fire and security hazard detection, electrical needs, and physical security.

9. The Licensor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The Licensor shall completely test and apply patches for all third-party software products in the server environment before release.

11. The Licensor shall comply with ~~Attachment 2 B~~Appendix B-2, SOC Reporting Requirements.

B. Security Requirements.

1. The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense on an annual basis.

2. The Licensor shall comply with the Commonwealth's directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.

3. The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4. The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The Licensor shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. The Licensor shall limit access to Commonwealth-specific systems and services and provide access only to those staff that must have access to provide services proposed.

7. The Licensor shall provide the Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in ~~Attachment 2 A~~Appendix B-1, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

C. Data Storage.

1. The Licensor shall store all Commonwealth data in the United States.

2. The Licensor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk. The Licensor shall protect their operational systems with applicable anti-virus, host intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Licensor shall be solely responsible for applicable data storage required.

4. The Licensor shall take all commercially viable and applicable measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

5. The Licensor agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or a Licensor-owned electronic device.

6. The Licensor shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

D. Adherence to Policy.

1. The Licensor's support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Licensor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as ~~Attachment 2 A~~Appendix B-1.

3. The Licensor shall comply with all pertinent federal and state privacy regulations.

E. Closeout.

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency to the Commonwealth Software Reseller within **sixty (60) days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

~~ATTACHMENT~~ APPENIDX ~~2~~B-~~1A~~

Information Technology Policies (ITPs)
for
Outsourced/Licensor(s)-hosted Solutions

ITP Number-Name	Policy Link
ITP_ACC001-Accessibility Policy	https://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030-Active Directory Architecture	https://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007-Enterprise Service Catalog	https://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010-Business Process Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS011-Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_bus011.pdf
ITP_BUS012-Artificial Intelligence General Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000-Enterprise Data and Information Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001-Database Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006-Commonwealth County Code Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009-e-Discovery Technology Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010-Business Intelligence Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011-Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012-Dashboard Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001-The Life Cycle of Records: General Policy Statement	https://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004-Management of Web Records	https://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005-System Design Review of Electronic Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006-Electronic Document Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1-Electronic Commerce Formats and Standards	https://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2-Electronic Commerce Interface Guidelines	https://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006-Business Engine Rules	https://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004-Internet Protocol Address Standards	https://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005-Commonwealth External and Internal Domain Name Services (DNS)	https://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001-Commonwealth of Pennsylvania Electronic Information Privacy Policy	https://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000-Information Security Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC002-Internet Accessible Proxy Servers and Services	https://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003-Enterprise Security Auditing and Monitoring	https://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004-Enterprise Web Application Firewall	https://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006-Commonwealth of Pennsylvania Electronic Signature Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007-Minimum Standards for IDs, Passwords and Multi-Factor Authentication	https://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008-Enterprise E-mail Encryption	https://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf

ITP Number-Name	Policy Link
ITP_SEC009-Minimum Contractor Background Checks Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf
ITP_SEC010-Virtual Private Network Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf
ITP_SEC011-Enterprise Policy and Software Standards for Agency Firewalls	https://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC013-Identity Protection and Access Management (IPAM) Architectural Standard and Identity Management Services	https://www.oa.pa.gov/Policies/Documents/itp_sec013.pdf
ITP_SEC015-Data Cleansing	https://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC017-Copa Policy for Credit Card Use for e-Government	https://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019-Policy and Procedures for Protecting Commonwealth Electronic Data	https://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC020-Encryption Standards for Data at Rest	https://www.oa.pa.gov/Policies/Documents/itp_sec020.pdf
ITP_SEC021-Security Information and Event Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023-Information Technology Security Assessment and Testing Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024-IT Security Incident Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025-Proper Use and Disclosure of Personally Identifiable Information (PII)	https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029-Physical Security Policy for IT Resources	https://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031-Encryption Standards for Data in Transit	https://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032-Enterprise Data Loss Prevention (DLP) Compliance Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034-Enterprise Firewall Rule Set	https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC037-Identity Proofing of Online Users	https://www.oa.pa.gov/Policies/Documents/itp_sec037.pdf
ITP_SEC038-Commonwealth Data Center Privileged User IAM Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP_SFT000-Software Development Life Cycle (SDLC) Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001-Software Licensing	https://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002-Commonwealth of PA Website Standards	https://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003-Geospatial Enterprise Service Architecture	https://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004-Geospatial Information Systems (GIS)	https://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005-Managed File Transfer (MFT)	https://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007-Office Productivity Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008-Enterprise Resource Planning (ERP) Management	https://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009-Application Development	https://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003-Off-Site Storage for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004-Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006-Commonwealth IT Resources Patching Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008-Server Virtualization Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010-Enterprise Services Maintenance Scheduling	https://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

~~ATTACHMENT 2 B~~APPENDIX B-2

SOC Reporting Requirements

(a) Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to, engage, on an annual basis, an independent auditing firm to conduct each the following:

(i) A SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions;

(ii) A SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access or contain Commonwealth Data; and

(iii) A SOC for Cybersecurity report with respect to controls used by the Contractor setting forth the description and effectiveness of the Contractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

Pennsylvania's fiscal year begins July 1 and ends on June 30. Audits shall be submitted annually no later than July 31 of the current year. All reports shall reflect the conduct of the Contractor during the **12 months** of the Commonwealth's previous fiscal year, unless otherwise agreed to in writing by the Commonwealth.

(b) SOC 2 Type II report reports shall address the following:

(i) Security of Information and Systems;

(ii) Availability of Information and Systems;

(iii) Processing Integrity;

(iv) Confidentiality;

(v) Privacy; and

(vi) If applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

(c) At the request of the Commonwealth, the Contractor shall complete additional SOC for Cybersecurity audits in the event:

(i) repeated non-conformities are identified in any SOC report required by subsection (a); or

(ii) if the Contractor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.);

The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

(d) The Commonwealth may specify other or additional standards, certifications or audits it requires under any Purchase Orders or within an ITP.

(e) The Contractor shall adhere to SSAE 18 audit standards. The Contractor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Contractor shall comply with such updates which shall be reflected in the next annual report.

(f) In the event an audit reveals any non-conformity to SSAE standards, the Contractor shall provide the Commonwealth, within **45 calendar days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity. The corrective action plan shall provide, in detail:

(i) clear responsibilities of the personnel designated to resolve the non-conformity;

(ii) the remedial action to be taken by the Contractor or its subcontractor(s);

(iii) the dates when each remedial action is to be implemented; and

(iv) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

(g) The Commonwealth may in its sole discretion agree, in writing, to accept alternative and equivalent reports or certifications in lieu of a SOC report.

~~ATTACHMENT~~ APPENDIX C~~3~~

COMMONWEALTH OF PENNSYLVANIA
***SAMPLE* BUSINESS ASSOCIATE AGREEMENT**
(Business Associate Agreements as provided by Agencies may differ)

WHEREAS, the _____ (Covered Entity) and _____(Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be handled, used or disclosed only in accordance with this Agreement, and the standards established by HIPAA, the HITECH Act and related regulations, and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

(a) "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(b) "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(c) "**HIPAA**" shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.

(d) "**HITECH Act**" shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV

of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(e) "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(f) "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(g) "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(h) "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2. Changes in Law.

Business Associate agrees that it will comply with any changes in the HIPAA Rules by the compliance date established by any such changes and will provide the Covered Entity with written certification of such compliance.

3. Stated Purposes for Which Business Associate May Use or Disclose PHI.

The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

_____
_____
_____
_____
_____
_____
_____
_____
_____

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

4. BUSINESS ASSOCIATE OBLIGATIONS.

(a) **Limits on Use and Further Disclosure**. Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity other than as permitted or required by this Addendum, as requested by Covered Entity, or as required by law and agency guidance.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

(c) **Reports of Improper Use or Disclosure**. Business Associate hereby agrees that it shall report to _____at _____, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

(d) **Reports on Security Incidents**. In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* ("HITECH Act"), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____, **within two (2) days** of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.

(e) **Subcontractors and Agents**. At any time PHI is provided or made available to Business Associate subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

(f) **Right of Access to PHI**. Business Associate shall allow, for any PHI maintained in a designated record set, Covered Entity to have access to and copy an individual's PHI within **five (5) business days** of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and Covered Entity. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within **five (5) business days**. Business Associate shall further conform with all of the requirements of 45 C.F.R. § 164.524 and other applicable laws, including the HITECH Act, as amended, related regulations and agency guidance. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(f).

(g) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a written request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act , as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within **five (5) business days**.

(h) **Provide Accounting of Disclosures**. Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended) in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the Covered Entity within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(h).

(i) **Requests for Restriction**. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health

plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) **Access to Books and Records**. Business Associate shall make its internal practices, books and records relating to the use or disclosure of PHI received from, or created or received, by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.

(k) **Return or Destruction of PHI**. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(l) **Maintenance of PHI**. Notwithstanding subsection 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.

(n) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.

(o) **Grounds for Breach**. Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-

compliance. Commonwealth may elect to terminate Business Associate's contract for such breach.

(p) **Termination by Commonwealth**. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

(q) **Failure to Perform Obligations**. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.

(r) **Privacy Practices**. Covered Entity will provide Business Associate with all applicable forms, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

5. OBLIGATIONS OF COVERED ENTITY.

(a) **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change.

(b) **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware if such changes affect Business Associate's permitted or required uses and disclosures.

(c) **Restrictions**. Covered Entity shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) **Requests**. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule, all as amended, if done by Covered Entity.

6. MISCELLANEOUS.

(a) **Regulatory References**. A reference in this Addendum to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.

(b) **Amendment**. The parties agree to take such action as is necessary to amend this Addendum from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.

(c) **Conflicts**. In the event that any terms of this Agreement are inconsistent with the terms of the Agreement, then the terms of this Agreement shall control.

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1		**Pennsylvania DOS TotalVote Project**	**1300 days**	**Mon 1/4/21**	**Thu 1/22/26**		
2		*Deliverable 0: Initial License Fee*	*0 days*	*Mon 1/4/21*	*Mon 1/4/21*		PA DOS
3		**Project Management**	570 days	**Fri 1/8/21**	**Thu 4/13/23**		
4		*Deliverable B.1: Status Report*	*515 days*	*Mon 1/11/21*	*Thu 1/26/23*	*9*	BPro PM
5		Project Status Meetings	515 days	Mon 1/11/21	Thu 1/26/23	9	BPro PM
6		*Deliverable B.2: Submit Final Implementation Report*	*3 days*	*Fri 1/27/23*	*Tue 1/31/23*	*4,2*	BPro PM
7		**Project Initiation**	**8 days**	**Mon 1/4/21**	**Wed 1/13/21**		BPro PM,PA DOS
8		**Project Kick-off Meeting**	**8 days**	**Mon 1/4/21**	**Wed 1/13/21**		
9		Schedule Project Kick-off Meeting	2 days	**Mon 1/4/21**	Tue 1/5/21		BPro PM
10		Conduct Project Kick-off Meeting	0.5 days	Wed 1/13/21	Wed 1/13/21	9FS+5 days	BPro PM
11		Provide scrum training if requested	0.5 days	Wed 1/13/21	Wed 1/13/21	10	BPro PM
12		**Project Members**	**2 days**	**Wed 1/6/21**	**Thu 1/7/21**		
13		Establish Project Stakeholders	0.5 days	Wed 1/6/21	Wed 1/6/21	9	
14		Establish Project Team	0.5 days	Wed 1/6/21	Wed 1/6/21	13	
15		Establish Project Team Roster	0.5 days	Thu 1/7/21	Thu 1/7/21	14	
16		Establish Core Team Members	0.5 days	Thu 1/7/21	Thu 1/7/21	15	
17		**Project Schedule**	**4 days**	**Fri 1/8/21**	**Wed 1/13/21**		
18		Establish Requirements Analysis Schedule	3 days	Fri 1/8/21	Tue 1/12/21	16	
19		Communicate Schedule to Core Team	1 day	Wed 1/13/21	Wed 1/13/21	18	
20		**Project Planning**	**95 days**	**Mon 1/4/21**	**Mon 5/17/21**		
21		**Project Management Plan**	**45 days**	**Mon 1/4/21**	**Mon 3/8/21**		
22		*Deliverable A.1: Finalized Implementation Plan*	10 days	Mon 1/4/21	Fri 1/15/21		BPro PM
23		**Finalize Project Management Plan (PMP)**	**35 days**	**Tue 1/19/21**	**Mon 3/8/21**	**22**	BPro PM,PA DOS
24		Finalize Project Schedule	5 days	Tue 1/19/21	Mon 1/25/21		
25		Develop Requirements Management Plan	5 days	Tue 1/19/21	Mon 1/25/21	19	
26		Develop Risk Management Plan	5 days	Tue 1/26/21	Mon 2/1/21	25	
27		Develop Issue Management Plan	5 days	Tue 2/2/21	Mon 2/8/21	26	
28		Develop Change Control Management Plan	5 days	Tue 2/9/21	Mon 2/15/21	27	

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
29		Develop Communications Management Plan	5 days	Tue 2/16/21	Mon 2/22/21	28	
30		Develop Quality Management Plan	5 days	Tue 2/23/21	Mon 3/1/21	29	
31		Develop Time Management Plan	5 days	Tue 3/2/21	Mon 3/8/21	30	
32		**Requirements Analysis and Specifications**	**66 days**	**Thu 1/14/21**	**Fri 4/16/21**		
33		Requirements Gap Analysis to TotalVote Baseline	30 days	Thu 1/14/21	Thu 2/25/21	19	BPro Team,PA DOS
34		**Create acceptance criteria for identified user stories and enter user stories into TFS**	**46 days**	**Fri 1/22/21**	**Fri 3/26/21**		
35		Enter user stories into TFS - VR Module	5 days	Fri 1/22/21	Thu 1/28/21	19FS+5 days	PA DOS
36		Enter user stories into TFS - EM Module	5 days	Fri 1/29/21	Thu 2/4/21	35	PA DOS
37		Enter user stories into TFS - Notice Management Module	2 days	Fri 2/5/21	Mon 2/8/21	36	PA DOS
38		Enter user stories into TFS - Data Generator Module	5 days	Tue 2/9/21	Mon 2/15/21	37	PA DOS
39		Enter user stories into TFS - Utilities & Roles & Permissions Module	1 day	Tue 2/16/21	Tue 2/16/21	38	PA DOS
40		Enter user stories into TFS - Interfaces Module	5 days	Wed 2/17/21	Tue 2/23/21	39	PA DOS
41		Enter user stories into TFS - Petition Module	3 days	Wed 2/24/21	Fri 2/26/21	40	PA DOS
42		Enter user stories into TFS - TotalAddress Module	3 days	Mon 3/1/21	Wed 3/3/21	41	PA DOS
43		Enter user stories into TFS - ENR Module	3 days	Thu 3/4/21	Mon 3/8/21	42	PA DOS
44		Enter user stories into TFS - Accessible Ballot Marking Module	3 days	Tue 3/9/21	Thu 3/11/21	43	PA DOS
45		Enter user stories into TFS - Campaign Finance Module	3 days	Fri 3/12/21	Tue 3/16/21	44	PA DOS
46		Enter user stories into TFS - Lobbying Module	3 days	Wed 3/17/21	Fri 3/19/21	45	PA DOS
47		Enter user stories into TFS - SMS/Email Notification Module	2 days	Mon 3/22/21	Tue 3/23/21	46	PA DOS

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
48		Enter user stories into TFS - Petition E-Signature Module	3 days	Wed 3/24/21	Fri 3/26/21	47	PA DOS
49		*Deliverable C.2: Requirements Traceability Matrix*	*5 days*	*Mon 3/29/21*	*Fri 4/2/21*	*33,34*	BPro BA
50		*Deliverable C.3: GAP analysis document*	*5 days*	*Mon 4/5/21*	*Fri 4/9/21*	*49*	BPro BA
51		*Deliverable C.1: Finalized Requirement documents*	*5 days*	*Mon 4/12/21*	*Fri 4/16/21*	*50*	BPro BA
52		*Deliverable E.1: Solution Interface and Design Document*	***20 days***	*Mon 4/19/21*	*Fri 5/14/21*	*32*	BPro BA,BPro CIO
53		**Software Development Life Cycle (SDLC) Plans**	**30 days**	**Tue 3/9/21**	**Mon 4/19/21**		
54		*Deliverable H.1: Develop Data Migration, Conversion, and Validation Plan (See Data Conversion Block for the map)*	*10 days*	*Tue 3/9/21*	*Mon 3/22/21*	*23*	BPro PM
55		*Deliverable G.1: Develop Test Plan*	*10 days*	*Tue 3/23/21*	*Mon 4/5/21*	*54*	BPro PM
56		*Deliverable K.1: Develop Configuration and Release Management Plan*	*10 days*	*Tue 4/6/21*	*Mon 4/19/21*	*55*	*BPro PM*
57		**Transformation Management Plans**	**20 days**	**Tue 4/20/21**	**Mon 5/17/21**		
58		*Deliverable I.1: Develop COOP/Disaster Recovery Plan*	*10 days*	*Tue 4/20/21*	*Mon 5/3/21*	*56*	BPro CIO
59		*Deliverable J.1: Develop Training Plan*	*10 days*	*Tue 5/4/21*	*Mon 5/17/21*	*58*	BPro PM
60		**System Modificaton & Customization**	**218 days**	**Thu 1/14/21**	**Mon 11/22/21**		
61		**Infrastructure - Configuration of Environments**	**218 days**	**Thu 1/14/21**	**Mon 11/22/21**		BPro CIO
62		**Development Environment**	**15 days**	**Thu 1/14/21**	**Thu 2/4/21**		
63		Configure and Set-up Development Environment	10 days	Thu 1/14/21	Thu 1/28/21	7	BPro Dev Team
64		*Deliverable D.1: Submit Configuration Confirmation Report - Development*	*5 days*	*Fri 1/29/21*	*Thu 2/4/21*	*63*	BPro PM
65		**Staging Environment**	**15 days**	**Fri 2/12/21**	**Thu 3/4/21**		
66		Configure and Set-up Staging Environment	10 days	Fri 2/12/21	Thu 2/25/21	64FS+5 days	BPro Dev Team
67		*Deliverable D.1: Submit Configuration Confirmation Report - Staging*	*5 days*	*Fri 2/26/21*	*Thu 3/4/21*	*66*	BPro PM
68		**Training Environment**	**15 days**	**Mon 10/11/21**	**Fri 10/29/21**		

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
69		Configure and Set-up Training Environment	10 days	Mon 10/11/21	Fri 10/22/21	120	BPro Dev Team
70		*Deliverable D.1: Submit Configuration Confirmation Report - Training*	*5 days*	*Mon 10/25/21*	*Fri 10/29/21*	*69*	BPro PM
71		**Production Environment**	**15 days**	**Mon 11/1/21**	**Mon 11/22/21**		
72		Configure and Set-up Production Environment	10 days	Mon 11/1/21	Mon 11/15/21	69FS+5 days	BPro Dev Team
73		*Deliverable D.1: Submit Configuration Confirmation Report - Production*	*5 days*	*Tue 11/16/21*	*Mon 11/22/21*	*72*	BPro PM
74		**Data Conversion and Validation**	**218 days**	**Thu 1/14/21**	**Mon 11/22/21**	**7**	
75		**Initial Data Collection and Clean-up**	**40 days**	**Thu 1/14/21**	**Thu 3/11/21**		
76		Get Initial Datasets from PA DOS & Counties	10 days	Thu 1/14/21	Thu 1/28/21		PA DOS PM
77		Data Staging, Analysis	10 days	Fri 1/29/21	Thu 2/11/21	76	BPro SQL DBA
78		Data Clean-up with Counties and DOS	10 days	Fri 2/12/21	Thu 2/25/21	77	BPro SQL DBA,PA
79		Analysis and Clarification Sessions	20 days	Fri 2/12/21	Thu 3/11/21	77	BPro SQL DBA
80		**Data Migration and Conversion**	**198 days**	**Fri 2/12/21**	**Mon 11/22/21**		
81		*Deliverable H.1: Develop Data Mapping and Translation Documents (Data Dictionary)*	*20 days*	*Fri 2/12/21*	*Thu 3/11/21*	*77*	BPro SQL DBA
82		*Deliverable H.2: Develop Data Conversion Schedule*	*5 days*	*Tue 3/23/21*	*Mon 3/29/21*	*54*	BPro SQL DBA
83		Data Migration and Conversion - Dev Environment	6 days	Fri 3/12/21	Fri 3/19/21	81	BPro SQL DBA
84		Review and check data - Dev Environment	3 days	Mon 3/22/21	Wed 3/24/21	83	PA DOS
85		Data Migration and Conversion - Staging Environment	5 days	Thu 3/25/21	Wed 3/31/21	66,84	BPro SQL DBA
86		Review and check data - Staging Environment	3 days	Thu 4/1/21	Mon 4/5/21	85	PA DOS
87		Data Migration and Conversion - Training Environment	5 days	Mon 10/25/21	Fri 10/29/21	69,85	BPro SQL DBA
88		Review and check data - Training Environment	5 days	Mon 11/1/21	Fri 11/5/21	87	PA DOS

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
89		*Deliverable H.3: Submit Final Conversion Test Results (After success conversion to Staging & Training)*	5 days	Mon 11/8/21	Mon 11/15/21	88	BPro PM
90		Data Migration and Conversion - Production Environment	5 days	Tue 11/16/21	Mon 11/22/21	72,87	BPro SQL DBA
91		**Development Construction & Customization (MVP Phase)**	**157 days**	**Mon 3/22/21**	**Fri 10/29/21**		
92		Sprint 0 - Prep the System for Development	10 days	Mon 3/22/21	Fri 4/2/21	63,83	BPro Dev Team
93		**Sprint 1**	**15 days**	**Mon 4/5/21**	**Fri 4/23/21**	**92,35,85**	
94		Develop Iteration 1	14 days	Mon 4/5/21	Thu 4/22/21	92,35	BPro Dev Team
95		User Sprint Review and Testing	1 day	Fri 4/23/21	Fri 4/23/21	94	BPro BA,PA DOS
96		*Election Blackout Days*	*15 days*	*Fri 5/7/21*	*Fri 5/28/21*		*PA DOS*
97		**Sprint 2**	**15 days**	**Mon 4/26/21**	**Fri 5/14/21**	**93**	
98		Develop Iteration 2	14 days	Mon 4/26/21	Thu 5/13/21	93	BPro Dev Team
99		User Review and Testing	1 day	Fri 5/14/21	Fri 5/14/21	98	BPro BA,PA DOS
100		**Sprint 3**	**14 days**	**Mon 5/17/21**	**Fri 6/4/21**	**97**	
101		Develop Iteration 3	13 days	Mon 5/17/21	Thu 6/3/21		BPro Dev Team
102		User Sprint Review and Testing	1 day	Fri 6/4/21	Fri 6/4/21	101	BPro BA,PA DOS
103		**Sprint 4**	**15 days**	**Mon 6/7/21**	**Fri 6/25/21**	**100**	
104		Develop Iteration 4	14 days	Mon 6/7/21	Thu 6/24/21		BPro Dev Team
105		User Sprint Review and Testing	1 day	Fri 6/25/21	Fri 6/25/21	104	BPro BA,PA DOS
106		**Sprint 5**	**14 days**	**Mon 6/28/21**	**Fri 7/16/21**	**103**	
107		Develop Iteration 5	13 days	Mon 6/28/21	Thu 7/15/21		BPro Dev Team
108		User Sprint Review and Testing	1 day	Fri 7/16/21	Fri 7/16/21	107	BPro BA,PA DOS
109		*Deliverable F.1.VR.1: MVP VR (45% of Priority 1 & 2)*	*0 days*	*Sun 8/1/21*	*Sun 8/1/21*		
110		**Sprint 6**	**15 days**	**Mon 7/19/21**	**Fri 8/6/21**	**106**	
111		Develop Iteration 6	14 days	Mon 7/19/21	Thu 8/5/21		BPro Dev Team
112		User Review and Testing	1 day	Fri 8/6/21	Fri 8/6/21	111	BPro BA,PA DOS
113		**Sprint 7**	**15 days**	**Mon 8/9/21**	**Fri 8/27/21**	**110**	
114		Develop Iteration 7	14 days	Mon 8/9/21	Thu 8/26/21		BPro Dev Team

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
115		User Sprint Review and Testing	1 day	Fri 8/27/21	Fri 8/27/21	114	BPro BA,PA DOS
116		*Deliverable F.1.EM.1: MVP EM (45% of Priority 1 & 2)*	*0 days*	*Wed 9/1/21*	*Wed 9/1/21*		
117		**Sprint 8**	**14 days**	**Mon 8/30/21**	**Fri 9/17/21**	**113**	
118		Develop Iteration 8	13 days	Mon 8/30/21	Thu 9/16/21		BPro Dev Team
119		User Sprint Review and Testing	1 day	Fri 9/17/21	Fri 9/17/21	118	BPro BA,PA DOS
120		**Sprint 9**	**15 days**	**Mon 9/20/21**	**Fri 10/8/21**	**117**	
121		Develop Iteration 9	14 days	Mon 9/20/21	Thu 10/7/21		BPro Dev Team
122		User Sprint Review and Testing	1 day	Fri 10/8/21	Fri 10/8/21	121	BPro BA,PA DOS
123		**Sprint 10**	**15 days**	**Mon 10/11/21**	**Fri 10/29/21**	**120**	
124		Develop Iteration 10	14 days	Mon 10/11/21	Thu 10/28/21		BPro Dev Team
125		User Review and Testing	1 day	Fri 10/29/21	Fri 10/29/21	124	BPro BA,PA DOS
126		**System Documentation**	**20 days**	**Mon 8/9/21**	**Fri 9/3/21**		
127		Prepare Interface and Service Diagram	5 days	Mon 8/9/21	Fri 8/13/21	110	BPro CIO
128		Prepare database model and schema for core tables	5 days	Mon 8/16/21	Fri 8/20/21	127	BPro SQL DBA
129		Prepare high-level security architecture diagram	5 days	Mon 8/23/21	Fri 8/27/21	128	BPro CIO
130		Prepare application architecture diagram	5 days	Mon 8/30/21	Fri 9/3/21	129	BPro CIO
131		**Security and IT Policy Compliance**	**35 days**	**Tue 9/7/21**	**Mon 10/25/21**		
132		Prepare Security Design Checklist	5 days	Tue 9/7/21	Mon 9/13/21	130	BPro CIO
133		Provide Application Security Assessment Support	10 days	Tue 9/14/21	Mon 9/27/21	132	BPro CIO
134		Collaborate with PA DOS IT to evaluate and prioritize security vulnerabilities	20 days	Tue 9/28/21	Mon 10/25/21	133	BPro CIO
135		Provide documentation of security coding practices	5 days	Tue 9/28/21	Mon 10/4/21	133	BPro CIO
136		*Election Blackout Days*	*15 days*	*Sat 10/23/21*	*Fri 11/12/21*		*PA DOS*
137		**Training**	**57 days**	**Mon 9/20/21**	**Fri 12/10/21**		
138		Update Training Plan	5 days	Mon 9/20/21	Fri 9/24/21	117	BPro PM
139		Coordinate Training Locations, Schedule, and Organization	5 days	Mon 9/27/21	Fri 10/1/21	138	BPro PM

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
140		*Deliverable G.1: Develop Test Scenarios*	*30 days*	*Mon 9/20/21*	*Fri 10/29/21*	*117*	*BPro BA*
141		Update Training Materials	9 days	Mon 11/1/21	Fri 11/12/21	140,124	BPro BA
142		*Deliverable J.2: Provide Training Documentation & Materials*	*0 days*	*Fri 11/12/21*	*Fri 11/12/21*	*141*	BPro BA
143		*Deliverable J.4: Conduct DOS User Training Sessions*	*5 days*	*Mon 11/15/21*	*Fri 11/19/21*	*142*	BPro BA
144		*Deliverable J.3: Conduct County User Training Sessions*	*10 days*	*Mon 11/29/21*	*Fri 12/10/21*	*143FS+3 days*	BPro BA
145		**Formal Testing Events**	**25 days**	**Mon 12/13/21**	**Wed 1/19/22**		
146		**User Acceptance Testing (UAT) #1**	**10 days**	**Mon 12/13/21**	**Mon 12/27/21**		
147		UAT Testing Support	5 days	Mon 12/13/21	Fri 12/17/21	144	BPro Team
148		Prepare UAT Results and Completion Report	5 days	Mon 12/20/21	Mon 12/27/21	147	BPro PM
149		Incorporate UAT Test Feedback into TotalVote	15 days	Mon 12/13/21	Tue 1/4/22	147SS	BPro Dev Team
150		**User Acceptance Testing (UAT) #2**	**10 days**	**Wed 1/5/22**	**Wed 1/19/22**		
151		UAT Testing Support	5 days	Wed 1/5/22	Tue 1/11/22	**149**	BPro Team
152		Prepare UAT Results and Completion Report	5 days	Wed 1/12/22	Wed 1/19/22	151	BPro PM
153		Incorporate UAT Test Feedback into TotalVote	10 days	Wed 1/5/22	Wed 1/19/22	151SS	BPro Dev Team
154		***Deliverable L.1: Provide Stress and Load Testing Support***	***5 days***	***Tue 12/28/21***	***Tue 1/4/22***		
155		Load and Stress Test Readiness	5 days	Tue 12/28/21	Tue 1/4/22	146	BPro Dev Team
156		**Implementation to Production State**	**273 days**	**Mon 1/4/21**	**Wed 2/2/22**		
157		TotalVote System Approval	1 day	Thu 1/20/22	Thu 1/20/22	153	PA DOS PM
158		**Deployment Readiness**	**232 days**	**Mon 1/4/21**	**Thu 12/2/21**		
159		Update Implementation and Deployment Plan	10 days	Mon 1/4/21	Fri 1/15/21		BPro PM
160		Prepare Systems Operations Documentation	10 days	Mon 11/15/21	Tue 11/30/21	142	BPro CIO
161		Conduct training to state technical staff	2 days	Wed 12/1/21	Thu 12/2/21	160	BPro CIO
162		*Deliverable F.1.VR.2, EM.2, Notice Mgt, Data Generator, Utilities & Roles & Permissions, Interfaces, Petition, & TotalAddress*	*0 days*	*Fri 12/31/21*	*Fri 12/31/21*		
163		*Deliverable F.1.Automated Testing*	*0 days*	*Fri 12/31/21*	*Fri 12/31/21*		*BPro Test Team*
164		**Production Deployment**	**9 days**	**Fri 1/21/22**	**Wed 2/2/22**		

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
165		Review production readiness checklist	1 day	Fri 1/21/22	Fri 1/21/22	157	BPro CIO
166		Data cut-over from legacy system	3 days	Mon 1/24/22	Wed 1/26/22	165	PA DOS
167		Production Data Conversions	3 days	Mon 1/24/22	Wed 1/26/22	165	BPro SQL DBA
168		Production Application Cutover	3 days	Mon 1/24/22	Wed 1/26/22	166SS	BPro CIO
169		*Deliverable F.1: Fully Configured Solution and Interfaces*	*5 days*	*Fri 1/21/22*	*Thu 1/27/22*	*91,157*	BPro PM
170		*Deliverable K.2: Submit Final Release Package*	*5 days*	*Thu 1/27/22*	*Wed 2/2/22*	*168*	BPro CIO
171		County and State Testing of Implemented Sites	2 days	Thu 1/27/22	Fri 1/28/22	168	PA DOS
172		Go-Live Support	5 days	Thu 1/27/22	Wed 2/2/22	168	BPro Dev Team
173		**Phase 2**	**242 days**	**Mon 2/14/22**	**Tue 1/31/23**		
174		**System Modificaton & Customization (Phase 2)**	**242 days**	**Mon 2/14/22**	**Tue 1/31/23**		
175		**Development Construction & Customization (Phase 2)**	**242 days**	**Mon 2/14/22**	**Tue 1/31/23**	**172FS+7 days**	
176		**ENR Sprint**	**15 days**	**Mon 2/14/22**	**Fri 3/4/22**		
177		Development Sprint Work	14 days	Mon 2/14/22	Thu 3/3/22		BPro Dev Team
178		User Sprint Review and Testing	1 day	Fri 3/4/22	Fri 3/4/22	177	BPro BA,PA DOS
179		*Deliverable F.1.ENR*	*0 days*	*Tue 3/15/22*	*Tue 3/15/22*		
180		**Accessible Ballot Marking Sprint**	**15 days**	**Mon 3/7/22**	**Fri 3/25/22**	**176**	
181		Development Sprint Work	14 days	Mon 3/7/22	Thu 3/24/22		BPro Dev Team
182		User Sprint Review and Testing	1 day	Fri 3/25/22	Fri 3/25/22	181	BPro BA,PA DOS
183		*Deliverable F.1.Accessible Ballot Marking*	*0 days*	*Fri 4/1/22*	*Fri 4/1/22*		
184		**MVP Update 1 Sprint 1**	**15 days**	**Mon 3/28/22**	**Fri 4/15/22**	**180**	
185		Development Sprint Work	14 days	Mon 3/28/22	Thu 4/14/22		BPro Dev Team
186		User Sprint Review and Testing	1 day	Fri 4/15/22	Fri 4/15/22	185	BPro BA,PA DOS
187		*Election Blackout Days*	*16 days*	*Fri 5/6/22*	*Fri 5/27/22*		*PA DOS*
188		**MVP Update 1 Sprint 2**	**15 days**	**Mon 4/18/22**	**Fri 5/6/22**	**184**	
189		Development Sprint Work	14 days	Mon 4/18/22	Thu 5/5/22		BPro Dev Team
190		User Sprint Review and Testing	1 day	Fri 5/6/22	Fri 5/6/22	189	BPro BA,PA DOS

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
191		*Deliverable F.1.MVP Update 1*	*0 days*	*Wed 6/1/22*	*Wed 6/1/22*		
192		**Campaign Finance Sprint 1**	**15 days**	**Mon 5/9/22**	**Fri 5/27/22**	**188**	
193		Development Sprint Work	14 days	Mon 5/9/22	Thu 5/26/22		BPro Dev Team
194		User Sprint Review and Testing	1 day	Fri 5/27/22	Fri 5/27/22	193	BPro BA,PA DOS
195		**Campaign Finance Sprint 2**	**14 days**	**Tue 5/31/22**	**Fri 6/17/22**	**192**	
196		Development Sprint Work	13 days	Tue 5/31/22	Thu 6/16/22		BPro Dev Team
197		User Sprint Review and Testing	1 day	Fri 6/17/22	Fri 6/17/22	196	BPro BA,PA DOS
198		*Deliverable F.1.Campaign Finance*	*0 days*	*Fri 7/1/22*	*Fri 7/1/22*		
199		**Lobbying Disclosure Sprint 1**	**14 days**	**Mon 6/20/22**	**Fri 7/8/22**	**195**	
200		Development Sprint Work	13 days	Mon 6/20/22	Thu 7/7/22		BPro Dev Team
201		User Sprint Review and Testing	1 day	Fri 7/8/22	Fri 7/8/22	200	BPro BA,PA DOS
202		**Lobbying Disclosure Sprint 2**	**15 days**	**Mon 7/11/22**	**Fri 7/29/22**	**199**	
203		Development Sprint Work	14 days	Mon 7/11/22	Thu 7/28/22		BPro Dev Team
204		User Sprint Review and Testing	1 day	Fri 7/29/22	Fri 7/29/22	203	BPro BA,PA DOS
205		*Deliverable F.1.Lobbying Disclosure*	*0 days*	*Mon 8/1/22*	*Mon 8/1/22*		
206		**MVP Update 2 Sprint 1**	**15 days**	**Mon 8/1/22**	**Fri 8/19/22**	**202**	
207		Development Sprint Work	14 days	Mon 8/1/22	Thu 8/18/22		BPro Dev Team
208		User Sprint Review and Testing	1 day	Fri 8/19/22	Fri 8/19/22	207	BPro BA,PA DOS
209		**MVP Update 2 Sprint 2**	**14 days**	**Mon 8/22/22**	**Fri 9/9/22**	**206**	
210		Development Sprint Work	13 days	Mon 8/22/22	Thu 9/8/22		BPro Dev Team
211		User Sprint Review and Testing	1 day	Fri 9/9/22	Fri 9/9/22	210	BPro BA,PA DOS
212		*Deliverable F.1.MVP Update 2*	*0 days*	*Fri 9/16/22*	*Fri 9/16/22*		
213		**SMS / Email Notification Sprint**	**15 days**	**Mon 9/12/22**	**Fri 9/30/22**	**209**	
214		Development Sprint Work	14 days	Mon 9/12/22	Thu 9/29/22		BPro Dev Team
215		User Sprint Review and Testing	1 day	Fri 9/30/22	Fri 9/30/22	214	BPro BA,PA DOS
216		*Deliverable F.1.SMS/Email Notification*	*0 days*	*Mon 10/3/22*	*Mon 10/3/22*		
217		**Petition E-Signature Sprint**	**15 days**	**Mon 10/3/22**	**Fri 10/21/22**	**213**	
218		Development Sprint Work	14 days	Mon 10/3/22	Thu 10/20/22		BPro Dev Team
219		User Sprint Review and Testing	1 day	Fri 10/21/22	Fri 10/21/22	218	BPro BA,PA DOS
220		*Deliverable F.1.Petition E-Signature*	*0 days*	*Fri 10/28/22*	*Fri 10/28/22*		

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
221		*Election Blackout Days*	*15 days*	*Fri 10/28/22*	*Fri 11/18/22*		*PA DOS*
222		**MVP Update 3 Sprint 1**	**19 days**	**Mon 10/24/22**	**Fri 11/18/22**	**217**	
223		Development Sprint Work	18 days	Mon 10/24/22	Thu 11/17/22		BPro Dev Team
224		User Sprint Review and Testing	1 day	Fri 11/18/22	Fri 11/18/22	223	PA DOS,BPro BA
225		**MVP Update 3 Sprint 2**	**18 days**	**Mon 11/21/22**	**Fri 12/16/22**	**222**	
226		Development Sprint Work	17 days	Mon 11/21/22	Thu 12/15/22		BPro Dev Team
227		User Sprint Review and Testing	1 day	Fri 12/16/22	Fri 12/16/22	226	PA DOS,BPro BA
228		**MVP Update 3 Sprint 3**	**18 days**	**Mon 12/19/22**	**Fri 1/13/23**	**225**	
229		Development Sprint Work	17 days	Mon 12/19/22	Thu 1/12/23		BPro Dev Team
230		User Sprint Review and Testing	1 day	Fri 1/13/23	Fri 1/13/23	229	PA DOS,BPro BA
231		*Deliverable F.1.MVP Update 3*	*0 days*	*Tue 1/31/23*	*Tue 1/31/23*		
232		**Transition to Maintenance - Project Closeout**	**21 days**	**Tue 1/17/23**	**Tue 2/14/23**		
233		Update all system documentation for project closeout	5 days	Tue 1/17/23	Mon 1/23/23	228	BPro PM
234		Prepare and Process Project Closeout Checklist	5 days	Tue 1/31/23	Mon 2/6/23	231	BPro CIO
235		*Deliverable H.4: Submit Final Conversion Report*	*1 day*	*Tue 2/7/23*	*Tue 2/7/23*	*234*	BPro PM
236		Complete warranty and transition to maintenance and operations	5 days	Wed 2/8/23	Tue 2/14/23	235	BPro PM
237		**Maintenance and Support Annual Tasks**	**774 days**	**Tue 1/31/23**	**Fri 1/16/26**	**231**	
238		Application Stablization Support	4 wks	Tue 1/31/23	Mon 2/27/23	231	BPro Dev Team
239		Maintenance period entrance	0 days	Mon 2/27/23	Mon 2/27/23	238	
240		**Yearly Maintenance**	**754 days**	**Tue 2/28/23**	**Fri 1/16/26**		
241		Provide maintenance and release schedule	5 days	Tue 2/28/23	Mon 3/6/23	239	BPro CIO
242		Update COOP/Disaster Recovery Plan	5 days	Tue 3/7/23	Mon 3/13/23	241	BPro CIO
243		Provide maintenance and release schedule in early January	5 days	Mon 1/8/24	Fri 1/12/24		BPro CIO
244		Update COOP/Disaster Recovery Plan	5 days	Mon 1/15/24	Fri 1/19/24	243	BPro CIO
245		Provide maintenance and release schedule in early January	5 days	Mon 1/6/25	Fri 1/10/25		BPro CIO
246		Update COOP/Disaster Recovery Plan	5 days	Mon 1/13/25	Fri 1/17/25	245	BPro CIO

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
247		Provide maintenance and release schedule in early January	5 days	Mon 1/5/26	Fri 1/9/26		BPro CIO
248		Update COOP/Disaster Recovery Plan	5 days	Mon 1/12/26	Fri 1/16/26	247	BPro CIO

Neil McClure
August 14, 2020

BPro Inc
Deliverable Breakdown

Vendor Name	BPro Inc
Vendor ID Number	347081
Vendor TIN	46-0446113

Deliverables					
Task	**Deliverable - Appendix P**	**Total Cost**	**Deliverable RFP Technical Submittal Document**	**Individual Deliverable Cost**	**Target Date**
	Initial License Fee: 18.5% of the Implementation Cost				**1/4/2021**
Implementation Planning	Finalized Implementation Plan Approved by DOS	$ 125,000.00			1/15/2021
					4/19/2021
					1/26/2023
Implementation of the Solution	Requirements Package	$ 150,000.00			
					4/16/2021
					4/2/2021
					4/9/2021
	Configuration Confirmation Report for all agreed to environment reviewed and approved by DOS	$ 150,000.00			
					2/4/2021
					3/4/2021
					10/29/2021
					11/22/2021
	Detailed Solution and Interface Design Document and Interface Delivery Specification	$ 175,000.00			5/14/2021
	Fully Configured solution and interfaces reviewed and accepted by DOS.	$ 3,750,000.00			1/27/2022
					8/1/2021
					12/31/2021
					9/1/2021
					12/31/2021
					12/31/2021
					12/31/2021
					12/31/2021
					12/31/2021
					12/31/2021
					12/31/2021
					12/31/2021
					3/15/2022
					4/1/2022
					6/1/2022
					7/1/2022
					8/1/2022
					9/16/2022
					10/3/2022
					10/28/2022
					1/31/2023
	Test Plan and Test Scenarios	$ 250,000.00			
					4/5/2021
					10/29/2021
					1/4/2022
	Final Implementation Report	$ 75,000.00			1/31/2023
					2/2/2022
					5/3/2021
Data Conversion and Validation	Data Conversion and Validation Plan Approved by DOS	$ 100,000.00			
					3/22/2021
					3/11/2021
	Data Conversion Schedule	$ 45,000.00			3/29/2021
	Final Conversion Test Results	$ 25,000.00			
					11/15/2021
	Final Data Conversion Report	$ 25,000.00			2/7/2023
Training	Finalized Training Plan	$ 75,000.00			5/17/2021
	Training Documentation	$ 125,000.00			11/12/2021
	County User Training Session(s)	$ 75,000.00			12/10/2021
	DOS User Training Session(s)	$ 25,000.00			11/19/2021
Exit From Hosting	Hosting Transition Plan	$ 35,000.00			
	Test Plan	$ 45,000.00			
	Test Results	$ 25,000.00			
	Final Hosting Migration Results Report	$ 15,000.00			
Outgoing Transition	Outgoing Transition Plan Reviewed and Accepted by DOS	$ 75,000.00			
	Final Report Showing the Successful Completion of Turnover Activities	$ 25,000.00			

EXHIBIT C

DOS SURE RFP Cost Submittal

Appendix P - Cost Submittal Vendor Hosted Instructions

1	All sheets must be filled out completely. Fill out all yellow highlighted cells on each worksheet.
2	Formulas are imbedded in the Worksheets. Offeror's must verify that all calculations, subtotal costs and grand total costs are accurate.
3	Rate Card: Offerors shall enter the hourly rate for the applicable positions listed in the rate card table. Offerors may add additional positions to the table. A blended rate will be calculated based on the information entered. The blended rate will populate the Enhancement Hours table listed.
4	Deliverables Worksheet: Provide the total cost for each deliverable. All other information is linked and will calculate automatically.
5	M&S Worksheet: Provide the costs for the COTS/MOTS/SaaS licensing, hosting, and annual maintenance and support of the solution.
6	Releases Worksheet: Enter the cost for each deliverable identified.
7	Enhancement Worksheet: This worksheet will automatically calculate based on the Blended Rate of the Rate Card worksheet.
8	Stress & Load Testing Worksheet: Enter the cost for each semi-annual test.
10	Optional Services: Enter the costs for the optional services listed.
11	Summary: All information is linked and will calculate automatically. The cost to host the solution will be entered by the Commonwealth and will be based in the information provided.
12	Please contact the Issuing Officer with any questions or concerns.
13	Payment for services under this contract are fixed cost per unit. The volumes listed are for evaluation purposes only and will not be binding on the Commonwealth.
14	No assumptions or modifications shall be included in the cost matrix with the exception of the Rate Card worksheet. Empty cells/values shall be considered zero dollars($0).

Offeror Information

OFFEROR NAME	CONTACT PERSON	
BPro Inc	George Munro	
OFFEROR ADDRESS	**EMAIL ADDRESS**	
102 East 6th Avenue	george@bpro.com	
Fort Pierre, SD 57532	**PHONE NUMBER**	**FAX NUMBER**
	605-224-8114	605-224-1665
	VENDOR NUMBER	**FEDERAL ID OR SSN**
	347081	46-0446113

Vendor Name	BPro Inc
Vendor ID Number	347081
Vendor TIN	46-0446113

Rate Card

Position	Hourly Rate Years 1-4	Hourly Rate Years 5-7
Project Manager	$ 150.00	$ 165.00
Solution Architect	$ 150.00	$ 165.00
Testing Lead	$ 125.00	$ 135.00
Account Manager	$ 125.00	$ 135.00
Business Analyst Lead	$ 125.00	$ 135.00
Development Lead	$ 125.00	$ 135.00
Training Lead	$ 125.00	$ 135.00
Infrastructure and Security Lead	$ 125.00	$ 135.00
Database Analyst	$ 125.00	$ 135.00
System Analyst	$ 125.00	$ 135.00
Systems Engineer	$ 125.00	$ 135.00
Total Blended Rate	**$ 129.55**	**$ 140.45**

NOTE: The rate card shall be used for calculating annual Enhancement hours as required by DOS. DOS has allotted for a rate increase in Year 4.

NOTE: Offeror(s) may add additional positions.

	BPro Inc
	347081
	46-0446113

Maintenance, Support, and Hosting

Maintenance, Support, and Hosting Base Years							
	Cost Per Month	Cost Per Year	Maintenance	Cost Per Month	Cost Per Year	Hosting	Cost Per Month
	$ *60,000.00*	$ 720,000.00	Monthly Cost Year 1	$ -	$ -	Monthly Cost Year 1	$ 25,000.00
	$ 61,000.00	$ 732,000.00	Monthly Cost Year 2	$ -	$ -	Monthly Cost Year 2	$ 25,000.00
	$ 62,000.00	$ 744,000.00	Monthly Cost Year 3	$ -	$ -	Monthly Cost Year 3	$ 27,500.00
	$ 63,000.00	$ 756,000.00	Monthly Cost Year 4	$ -	$ -	Monthly Cost Year 4	$ 27,500.00
	$ 246,000.00	**$ 2,952,000.00**	**Total Base Years**	$ -	**$** -	**Total Base Years**	$ 105,000.00

Maintenance, Support, and Hosting Renewal Years							
nse	Cost Per Month	Cost Per Year	Maintenance	Cost	Cost Per Year	Hosting	Cost
	$ 65,000.00	$ 780,000.00	Monthly Cost Year 5	$ -	$ -	Monthly Cost Year 5	$ 28,000.00
	$ 66,000.00	$ 792,000.00	Monthly Cost Year 6	$ -	$ -	Monthly Cost Year 6	$ 28,000.00
	$ 67,000.00	$ 804,000.00	Monthly Cost Year 7	$ -	$ -	Monthly Cost Year 7	$ 29,000.00
	$ 198,000.00	**$ 2,376,000.00**	**Total Renewal Years**	$ -	**$** -	**Total Renewal Years**	$ 85,000.00

parate for license, maintenance, and hosting based on the selected Offeror's cost model, Offeror can enter the combined cost under the

or Name	BPro Inc
or ID Number	347081
or TIN	46-0446113

Releases

Item		Quantity	Cost Per Release	Estimated QTY Per Year	Total Cost Per
Releases Base Years 1-4	Release Plan	1	$ -	4	$
	Final Release Package	1	$ -	4	$
	Training Documentation as needed	1	$ -	4	$
	Training Delivery as needed	1	$ -	4	$
				Total Cost Per Year	$
				Total Cost All Base Years	$

Item		Quantity	Cost Per Release	Estimated QTY Per Year	Total Cost Per
ases Renewal Base Years 5-7	Release Plan	1	$ -	4	$
	Final Release Package	1	$ -	4	$
	Training Delivery as needed	1	$ -	4	$
	Training Documentation as needed	1	$ -	4	$
				Total Cost Per Renewal Year	$
				Total Cost All Renewal Years	$

or Name	BPro Inc
or ID Number	347081
or TIN	46-0446113

Deliverables

Task	Deliverable	Quantity	Total Cost
Implementation Planning	Finalized Implementation Plan Approved by DOS	1	$ 125,00
Implementation of the Solution	Requirements Package	1	$ 150,00
	Configuration Confirmation Report for all agreed to environment reviewed and approved by DOS	1	$ 150,00
	Detailed Solution and Interface Design Document and Interface Delivery Specification	1	$ 175,00
	Fully Configured solution and interfaces reviewed and accepted by DOS.	1	$ 3,750,00
	Test Plan and Test Scenarios	1	$ 250,00
	Final Implementation Report	1	$ 75,00
Data Conversion and Validation	Data Conversion and Validation Plan Approved by DOS	1	$ 100,00
	Data Conversion Schedule	1	$ 45,00
	Final Conversion Test Results	1	$ 25,00
	Final Data Conversion Report	1	$ 25,00
Training	Finalized Training Plan	1	$ 75,00
	Training Documentation	1	$ 125,00
	County User Training Session(s)	1	$ 75,00
	DOS User Training Session(s)	1	$ 25,00
Exit From Hosting	Hosting Transition Plan	1	$ 35,00
	Test Plan	1	$ 45,00
	Test Results	1	$ 25,00
	Final Hosting Migration Results Report	1	$ 15,00
Outgoing Transition	Outgoing Transition Plan Reviewed and Accepted by DOS	1	$ 75,00
	Final Report Showing the Successful Completion of Turnover Activities	1	$ 25,00

		46-0446113

Optional Services			
ears 1-4	Cost Per Month	Cost Per Year	Total Cost Base Years
ht Reporting	$ 8,100.00	$ 97,200.00	$ 388,800.00
ed Testing	$ 7,500.00	$ 90,000.00	$ 360,000.00

Years 5-7	Cost Per Month	Cost Per Year	Total Cost Renewal Years
ht Reporting	$ -	$ -	$ -
ed Testing	$ 5,000.00	$ 60,000.00	$ 180,000.00

her Offerings of Services of Interest to the Department		
iption	QTY	Cost
		$ -
		$ -
		$ -
		$ -
		$ -
		$ -
		$ -
		$ -

Service costs are not carried over to the Summary Tab. The cost of Optional Services is not included in the Cost Evalu

Vendor Name	BPro Inc
Vendor ID Number	347081
Vendor TIN	46-0446113

Enhancements		
Item	**Quantity**	**Cost**
Enhancement Hours Year 1	500	$ 64,772.73
Enhancement Hours Year 2	500	$ 64,772.73
Enhancement Hours Year 3	500	$ 64,772.73
Enhancement Hours Year 4	500	$ 64,772.73
Total Base Years		**$ 259,090.91**
Item	**Quantity**	**Cost**
Enhancement Hours Year 5	500	$ 70,227.27
Enhancement Hours Year 6	500	$ 70,227.27
Enhancement Hours Year 7	500	$ 70,227.27
Total Renewal Years		**$ 210,681.82**

NOTE: Enhancement costs are for evaluation purposes only and do not guarantee work to be performed or payment of services. Enhancement hours for the blended rate up to 3000 will be allotted for DOS annually. DOS will be charged for actual hours of work performed.

Vendor Name		BPro Inc
Vendor ID Number		347081
Vendor TIN		46-0446113

Stress and Load Testing			
Base Years 1-4	**Cost Per Test**	**QTY**	**Total Cost Base Years**
Semi Annual Test	$ 10,000.00	8	$ 80,000.00

Renewal Years 5-7	**Cost Per Test**	**QTY**	**Total Cost Renewal Years**
Semi Annual Test	$ 12,000.00	6	$ 72,000.00

Vendor Name	BPro Inc
vendor ID Number	347081
Vendor TIN	46-0446113

Cost Summary

Total Cost Base Years		
Total Deliverables Costs	$	5,390,000.00
Total Cost Releases	$	-
Total M&S Costs	$	4,212,000.00
Total Enhancement Costs	$	259,090.91
Stress and Load Testing	$	80,000.00
Total Costs Base Years	**$**	**9,941,090.91**

Total Cost Renewal Years		
Total Cost Releases	$	-
Total M&S Costs	$	3,396,000.00
Total Enhancement Costs	$	210,681.82
Stress and Load Testing	$	72,000.00
Total Costs Renewal Years	**$**	**3,678,681.82**

Total Cost Base & Renewal Years		
Total Costs	**$**	**13,619,772.73**

EXHIBIT D

SMALL DIVERSE BUSINESS AND SMALL BUSINESS PARTICIPATION SUBMITTAL

A. General Information. The Issuing Office encourages participation by Small Diverse Businesses (SDB) and Small Businesses (SB) as prime contractors and encourages all prime contractors to make significant commitments to use SDBs and SBs as subcontractors and suppliers.

A SB must meet each of the following requirements:

Δ The business must be for-profit, United States business;

Δ The business must be independently owned;

Δ The business may not be dominant in its field of operation;

Δ The business may not employ more than 100 full-time or full-time equivalent employees;

Δ The business may not exceed an average of $38.5 million in gross annual revenues over the preceding three years.

For credit in the RFP scoring process, a SB must complete the Department of General Services (DGS)/Bureau of Diversity, Inclusion and Small Business Opportunities (BDISBO) self-certification process. Additional information on this process can be found here:
Small Business Self-Certification.

A SDB is a DGS-verified minority-owned small business, woman-owned small business, veteran-owned small business, service-disabled veteran-owned small business, LGBT-owned small business, Disability-owned small business, or other small businesses as approved by DGS, that are owned and controlled by a majority of persons, not limited to members of minority groups, who have been deprived of the opportunity to develop and maintain a competitive position in the economy because of social disadvantages.

For credit in the RFP scoring process, a SDB must complete the DGS verification process. Additional information on this process can be found here:
Small Diverse Business Verification.

An Offeror that qualifies as a SDB or SB and submits a proposal as a prime contractor is not prohibited from being included as a subcontractor in separate proposals submitted by other Offerors. A SDB or SB may be included as a subcontractor with as many prime contractors as it chooses in separate proposals.

The Department's directory of self-certified SBs and DGS/BDISBO-verified SDBs can be accessed here:
Find Small and Small Diverse Businesses.

B. SDB and SB Participation Evaluation. BDISBO has established the minimum evaluation weight for the SDB and SB Participation criterion for this RFP as 20% of the total points.

1) The SDB and SB point allocation is based entirely on the percentage of the contract

cost committed to SDB and SB participation. If the proposer is a SDB, 100% of the contract cost is allocated to SDB participation. If the proposer is a SB, 100% of the contract cost is allocated to SB participation.

2) A total combined SDB/SB commitment less than one percent (1%) of the total contract cost is considered de minimis and will receive no SDB or SB points.

3) Based on a maximum total of 200 available points for the SDB/SB Participation Submittal, the scoring mechanism is as follows:

SDB and SB Raw Score =
*200 (SDB% + (1/3 * SB %))*

4) The SDB and SB Raw Score is capped at 200.

The Offeror with the highest raw score will receive 200 points. Each Offeror's raw score will be pro-rated against the Highest Offeror's raw score by applying the formula set forth here: RFP Scoring Formula.

5) The Offeror's prior performance in meeting its contractual obligations, SDBs and SBs will be considered by BDISBO during the scoring process. To the extent the Offeror has failed to meet prior contractual commitments, BDISBO may recommend to the Issuing Office that the Offeror be determined non-responsible for the the limited purpose of eligibility to receive SDB and SB points.

Questions regarding the SDB and SB Programs, including questions about the self-certification and verification processes can be directed to:

Department of General Services
Bureau of Diversity, Inclusion and Small Business Opportunities (BDISBO)
Room 601, North Office Building
Harrisburg, PA 17125
Phone: (717) 783-3119
Fax: (717) 787-7052
Email: RA-BDISBOVerification@pa.gov
Website: www.dgs.pa.gov

C. SDB/SB Participation Submittal. All Offerors are required to submit the attached SDB/SB Participation Submittal Form in its entirety and related Letter(s) of Intent. **To receive points for SDB or SB participation commitments, the SDB or SB must be listed in the Department's directory of self-certified SBs and DGS/BDISBO-verified SDBs as of the proposal due date and time. BDISBO reserves the right to adjust overall SDB or SB commitments to correctly align with the SDB or SB status of a prime contractor or subcontractor as of the solicitation due date and time, and also to reflect the correct sum of individual subcontracting commitments listed within the Letters of Intent.**

If there are multiple Letters of Intent, please combine them into one document and upload them with your response. The Letter(s) of Intent must be signed by both the Offeror and the SDB or SB for each of the identified SDB or SB subcontractors. Please use the attached Letter of Intent template and include all highlighted information.

Each SDB or SB commitment credited by BDISBO along with the overall percentage of SDB and SB commitments will become contractual obligations of the selected Offeror.

Offerors will not receive credit for any commitments for which information as above is not included in the SDB/SB Participation Submittal. Offerors will not receive credit for stating that they will find a SDB or SB after the contract is awarded.

Equal employment opportunity and contract compliance statements referring to company equal employment opportunity policies or past contract compliance practices do not constitute proof of SDB and/or SB Status or entitle an Offeror to receive credit for SDB or SBparticipation.

D. Contract Requirements.

All contracts containing SDB and SB Participation must contain the following contract provisions to be maintained through the initial contract term and any subsequent options or renewals:

1. Each SDB and SB commitment which was credited by BDISBO and the total percentage of such SDB and SB commitments made at the time of proposal submittal, BAFO, or contract negotiations, as applicable, become contractual obligations of the selected Offeror upon execution of its contract with the Commonwealth.

2. For purposes of monitoring compliance with the selected Offeror's SDB or SB commitments, the contract cost is the total amount paid to the selected Offeror throughout the initial contract term.

3. All SDB and SB subcontractors credited by BDISBO must perform at least 50% of the work subcontracted to them.

4. The individual percentage commitments made to SDBs and SBs cannot be altered without written approval from BDISBO.

5. SDB and SB commitments must be maintained in the event the contract is assigned to another prime contractor.

6. The selected Offeror and each SDB and SB for which a commitment was credited by BDISBO must submit a final, definitive subcontract agreement signed by the selected Offeror and the SDB and/or SB to BDISBO within 30 days of the final execution date of the Commonwealth contract. A Model Subcontract Agreement which may be used to satisfy this requirement is provided as an attachment – **Model Form of Small Diverse and Small Business Subcontract Agreement.** The subcontract must contain:

a) The specific work, supplies or services the SDB and/or SB will perform; location for work performed; how the work, supplies or services relate to the project; and the specific timeframe during the initial term and any extensions, options and renewals of the prime contract when the work, supplies or services will be provided or performed.

b) The fixed percentage commitment and associated estimated dollar value that each SDB and/or SB will receive based on the final negotiated cost for the initial term of the prime contract.

c) Payment terms indicating that the SDB and/or SB will be paid for work satisfactorily completed within 14 days of the selected Offeror's receipt of payment from the Commonwealth for such work.

d) Commercially reasonable terms for the applicable business/industry that are no less favorable than the terms of the selected Offeror's contract with the Commonwealth and that do not place disproportionate risk on the SDB and/or SB relative to the nature and level of the SDB's and/or SB's participation in the project.

7. If the subcontract terms omit any of the information required in paragraph 6, and that information is otherwise reflected within the selected Offeror's SDB and SB Participation Submittal or LOI, that information is incorporated into the subcontract agreement.
To the extent that any subcontract terms conflict with the requirements of paragraph 6 or information contained within the selected Offeror's SDB and SB Participation Submittal or LOI, the order of precedence is as follows: 1) the requirements of paragraph 6, 2) the selected Offeror's SDB and SB Participation Submittal, and 3) the terms of the subcontract agreement.

8. If the selected Offeror and a SDB or SB credited by BDISBO cannot agree upon a definitive subcontract within 30 days of the final execution date of the Commonwealth contract, the selected Offeror must notify BDISBO.

9. The Selected Offeror shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the contracting officer of the Issuing Office and BDISBO within ten (10) business days at the end of each quarter of the contract term and any subsequent options or renewals. This information will be used to track and confirm the actual dollar amount paid to SDB and SB subcontractors and suppliers and will serve as a record of fulfillment of the the contractual commitment. If there was no activity during the quarter, the form must be completed by stating "No activity in this quarter." A late fee of $100.00 per day may be assessed against the Selected Offeror if the Utilization Report is not submitted in accordance with the schedule above.

10. The Selected Offeror shall notify the Contracting Officer of the Issuing Office and BDISBO when circumstances arise that may negatively impact the selected Offeror's ability to comply with SDB and/or SB commitments and to provide a corrective action plan. Disputes will be decided by the Issuing Office and DGS.

11. If the Selected Offeror fails to satisfy its SDB and/or SB commitment(s), it may be subject to a range of sanctions BDISBO deems appropriate. Such sanctions include, but are not limited to, one or more of the following: a determination that the selected Offeror is not responsible under the Contractor Responsibility Program; withholding of payments; suspension or termination of the contract together with consequential damages; revocation of the selected Offeror's SDB and/or SB status; and/or suspension or debarment from future contracting opportunities with the Commonwealth.

SMALL DIVERSE BUSINESS (SDB) AND SMALL BUSINESS (SB) PARTICIPATION SUBMITTAL

Project Description:	*Statewide Uniform Registry of Electors (SURE) System*
RFP #:	*6100044816*
Proposal Due Date:	*BAFO due February 21, 2020*
Commonwealth Agency Name:	*Department of State*

OFFEROR (Prime Contractor) INFORMATION

Offeror Company's Name:	*BPro Inc*		
Offeror Contact Name:	*George Munro*	**Email:**	*george@bpro.com*
Title:	*Government Outreach Director*	**Phone:**	*605-224-8114*

Is your firm a DGS-Verified Small Diverse Business? NO ▾ **Verif Exp:**

Is your firm a DGS-Self-Certified Small Business? YES ▾ **Cert Exp:** *10/30/2021*

To confirm your company's SDB/SB status and expiration, please click or use the following link:
http://www.dgs.pa.gov/Businesses/Small Diverse Business Program/Small-Diverse-Business-Verification/Pages/Finding-Small-Diverse-Businesses.aspx#.WVPvzp3D-

SUBCONTRACTING INFORMATION

Percentage Commitment for SDB and SB Subcontracting Participation

Commitment percentages will automatically calculate in the SDB/SB fields below after you have completed the SDB and SB Subcontractor Listing on the "Listing" tab.

After examination of the contract documents, which are made a part hereof as if fully set forth herein, the Offeror commits to the following percentages of the total contract cost for Small Diverse Business and Small Business subcontracting participation.

Small Diverse Business Subcontracting percentage commitment:

0.000%

Small Business Subcontracting percentage commitment:

0.000%

Revised 01-16-2018

SMALL DIVERSE BUSINESS (SDB) AND SMALL BUSINESS (SB)
PARTICIPATION SUBMITTAL

Listing SDB and SB Subcontractors

The Offeror must list in the chart below the SDBs and SBs that will be used to meet the percentage commitments provided above, along with the requested information about each SDB and SB Subcontractor. Include as many pages as necessary. Offerors must also include a Letter of Intent (LOI) for each SDB/SB listed. **To receive points for SDB or SB participation commitments, the SDB or SB must be listed in the Department's directory of self-certified SBs and DGS/BDISBO-verified SDBs as of the proposal due date.** The directory of self-certified SBs and DGS/BDISBO-verified SDBs can be accessed at the following link:

http://www.dgs.pa.gov/Businesses/Small Diverse Business Program/Small-Diverse-Business-Verification/Pages/Finding-Small-Diverse-Businesses.aspx#.WVPvzp3D-

SDB/SB name, percent commitment to SDB/SB, and estimated $ value of commitment will automatically populate in the LOI tabs.

Offeror Company's Name:	**BPro Inc**					
SDB/SB Subcontractor Name	**SDB or SB**	**Primary Contact Name**	**Description of Services or Supplies to be Provided**	**% of Total Contract Cost Committed**	**Estimated $ Value of Commitment for Initial Contract Term**	**Will SDB/SB be used for Options/ Renewals? (YES/NO)**
Total SDB % Commitment:	**0.000%**					
Total SB % Commitment:	**0.000%**					

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State** on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

Revised 01-16-2018

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State**
on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State**
on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State** on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

Revised 01-16-2018

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State**
on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State**
on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State** on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

MM/DD/YYYY

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]
[Address]
[City, State, Zip]
[Email]
[Phone #]

Offeror: BPro Inc
RFP: 6100044816

Dear: [SDB/SB Contact Name]

This letter serves as confirmation of the intent of this offeror to utilize
on the above-referenced RFP issued by **Department of State**

If Offeror is the successful vendor, the referenced SDB/SB shall perform the following work, goods or services during the initial term of the prime contract and during any extensions, options or renewal periods of the prime contract exercised by the Commonwealth, as more specifically set forth below:

[Identify the specific time periods during the initial contract term and any extensions, options and renewals when the work, goods or services will be provided or performed]

Identify the specific work, goods or services the SDB/SB will perform below:

[Identify the specific work, goods or services the SDB/SB will perform]

These services represent of the total cost in the Offeror's cost submittal for the initial term of the contract. Dependent on final negotiated contract pricing and actual contract usage or volume, it is expected that above-referenced SDB/SB will receive an estimated during the initial contract term.

The above-referenced SDB/SB represents that it meets the small or small diverse business requirements set forth in the RFP and all required documentation has been provided to the Offeror for its SDB/SB submission.

We look forward to the opportunity to serve **Department of State**
on this project. If you have any questions concerning our small business or small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

X

George Munro
Government Outreach Director
BPro Inc
605-224-8114

Acknowledged,

X

[SDB/SB Contact Name]
[Title]
[SDB/SB Company Name]

Election RFP Technical Submittal

I. Project Description. The Commonwealth of Pennsylvania (Commonwealth), Department of State (DOS), along with the 67 county boards of elections in Pennsylvania, are seeking a vendor hosted Commercial off the Shelf (COTS), Modified Off the Shelf (MOTS) or Software as a Service (SAS) solution from a professional Offeror with a high degree of skill and knowledge that will meet, at a minimum, the DOS election administration business needs in providing and implementing a modern election management and disclosure system to replace the current aging system. The DOS is operating its current systems on aging platforms and is interested in modern solutions that support and augment the current election organization and mandated processes/deliverables at the national, state, and county levels. This RFP will be awarded to a single Offeror. For more information about the existing systems, see **Appendix A, Current State**. The DOS seeks to replace the current Voter Registration System as well as the current DOS Campaign Finance and Lobbying Disclosure and Registration and Reporting systems. The primary services to be included, but are not limited to the following:

A. Services for a voter registration system and elections management solution, which shall be an enhancement or replacement of the following applications currently in use by the DOS Statewide Voter Registration System (SURE):

1. Statewide Voter Registration System (currently known as "SURE");
2. SURE Data Warehouse;
3. SURE Portals**;**
4. PA Voter Services;
5. PA Online Voter Registration;
6. Voter Registration;
7. Voter Registration API**;**
8. Elections system;
9. Petitions system;
10. Election Night Returns system;
11. Provisional Ballot Phone System (external application);
12. Online Absentee Applications; and
13. Data exchanges and dependencies or application functions between the voter registration and election management system and the campaign finance and lobbying disclosure systems.

The proposed solution shall serve as the official Voter Registration System used by the Commonwealth of Pennsylvania, through the Pennsylvania Secretary of State's Office, and all 67 counties in Pennsylvania. This RFP seeks to implement a uniform and interactive platform that is utilized by the DOS and each of the 67 county election offices and other authorized state and local officials.

B. Services for a Campaign Finance and Lobbying Disclosure and Registration and Reporting solution shall be an enhancement or replacement of the following applications currently in use by the DOS Campaign Finance System:

1. Campaign Finance System;
2. Campaign Finance Online and Reporting System;
3. Lobbying Disclosure System;
4. Lobbying Disclosure Registration and Reporting Online System; and
5. Data exchanges and dependences or application functions between the campaign finance and lobbying disclosure systems and the voter registration and election management system.

The proposed solution shall also serve as the official Campaign Finance reporting system and the official Lobbying Disclosure reporting system used by the Commonwealth of Pennsylvania, through the Pennsylvania Secretary of State's Office. This RFP seeks to implement a uniform and interactive platform that is utilized by the DOS and can be extended to all 67 county offices and other authorized state and local officials.

II. Objectives.

A. General. The DOS is seeking a solution and application modernization to reduce costs, create efficiencies, and expand constituent confidence in the election process and related components. The DOS is seeking a new solution to increase registration rates across all business areas, improve accuracy of voter information, promote faster processing times, improve the filing and administrative process for voter registration, campaign finance, and lobbying disclosure registrants, strengthen disclosure and transparency for campaign finance and lobbying disclosure registrants and other business areas through openness, accountability and honesty, curb opportunities for fraud, and provide savings to the Commonwealth in the form of reduced costs and maximizing value in support and services to constituents.

1. **Security.** The solution implementation, enhancements, and maintenance must be driven by a "security first" perspective that focuses on securing critical election infrastructure. The Offeror and DOS recognize that trust in elections and disclosure is vital.

2. **On-time and on-budget.** The DOS is seeking a solution that will be implemented, available, and functional within the agreed upon project schedule and budget.

3. **Operational Support.** One objective of this procurement is to implement an operational model that maximizes limited resources and limits or reduces maintenance costs to the DOS.

4. **Minimal Customization.** The DOS is seeking a solution that will achieve a majority of Pennsylvania's functional requirements without the need to customize the base code of the proposed solution. The proposed solution shall provide the ability for configuration over customization to enable rapid system changes.

5. **Modern.** The solution architecture shall be modern and robust. The underlying technology stack must consist of widely used components with a long-term viable product roadmap.

6. **Integration.** Provide the DOS with efficient integration with external systems that monitors interface transactions to ensure quality data. The solution shall also provide integrations with PA Department of Transportation, including the HAVA exchange, PA Voter Registration API, PA Department of Health, other NVRA state agencies, PA Election Returns with all county boards of election, Electronic Information Registration Center (ERIC), Voter Information Project (VIP), and easily be extendable to accommodate additional interfaces in the future.

7. **Continuity of Operations.** The solution shall provide the appropriate architecture, processes and environments to provide solution availability and continuity of solution functionality through environmental and infrastructure incidents, including disaster recovery.

III. Statement of the Project. State in succinct terms your understanding of the project presented, or the service required by this RFP. Then, please describe how your proposed solution meets or exceeds the requested service in this RFP. The Department prefers a centralized database approach with county users participating in the proposed solution that meets the needs of approximately 8.4 million active and inactive registered voters, approximately 1,200 active candidates, and roughly 8,720 campaign finance and lobbying disclosure users.

Offeror Response

For over a decade, BPro has been building election systems that help ensure all voters are correctly registered, all political donations and expenditures are properly tracked and publicly available, and all election results are available on accessible, user-friendly web-based applications. BPro was founded in 1985 and began building election systems in 2007, when the State of South Dakota sought a better way to report state, county, and local election results. BPro's Election Night Reporting website was launched in time for South Dakota's 2008 elections and received the Election Center's 2009 State Technology Award. Today, BPro-built systems are available to almost 20 million registered voters in 15 states.

In BPro's 12 years building election technologies, our team has partnered with urban and rural counties with diverse cultures, unique language requirements and various understandings of technology. This experience helps BPro understand how to partner with state and county election officials to deliver successful election solutions, on time and on budget. BPro built South Dakota's Voter Registration and Election Management System (TotalVote VR/EMS) in 2012. Since the first deployment, TotalVote VR/EMS has been deployed around the country as a modern system configured to meet each individual states' laws governing elections and voter registration. BPro currently provides statewide VR/EMS systems in six states (Arizona, Hawaii, New Mexico, North Dakota, South Dakota and Washington), with another statewide system (Montana) and one county-

based, “bottom-up” system (Travis County, TX) scheduled to go live in the coming months. Each successful deployment demonstrates BPro’s ability to deliver highly individualized systems using configurable parameters. Some of these configurations include building a version of TotalVote VR/EMS to accommodate Washington state’s Vote by Mail laws and building a VR/EMS for North Dakota, a state that (proudly) does not require voter registration but does need a centralized system to verify a voter’s eligibility on Election Day.

BPro's TotalVote suite of products was designed to cover every aspect of Voter Registration and Election Management. With BPro's experience providing Voter Registration and Election Management systems around the country, we have a full comprehension of the significant effort to manage voter registrations, and how thoroughly vetted, well-maintained voter records are an integral part of the overall success of every election. We integrate data across all TotalVote modules to provide seamless management of voter districts with Candidate Filing, Elections and Petition Management, Ballot Entitlement, Ballot Styles, Voter Engagement and Election Night Reporting.

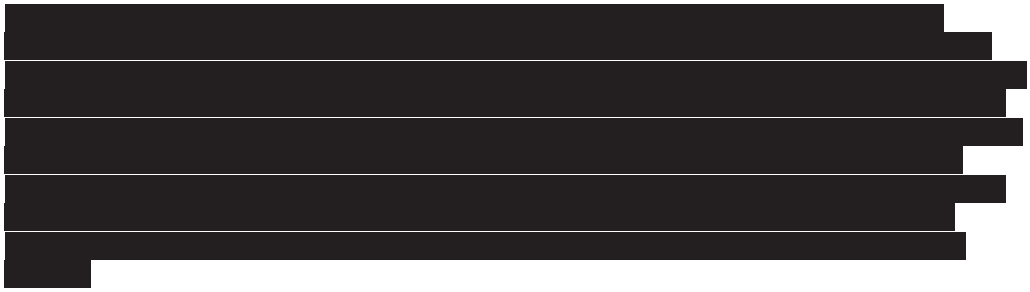
BPro has also developed, deployed, supported and enhanced campaign finance/lobbyist systems in North Dakota and South Dakota since 2013. While not as widely adopted as other TotalVote modules, these statewide systems have streamlined the reporting process for candidates, political committees and lobbyists and increased transparency of political donations and expenditures by providing a reporting system that is user-friendly and searchable by any citizen. As part of successfully delivering both systems, BPro has built data exchanges between the campaign finance and lobbying disclosure systems and the voter registration and election management system, in order to streamline the flow of information and ensure that all systems comply with applicable federal and state laws and regulations.

“Voter registration databases are a target for cyberattack.” Pennsylvania’s Blue Ribbon Commission on Election Security was 100% correct and at BPro, security is a top priority. Elections are the backbone of our democracy and any security breach could undermine the public’s confidence in the electoral process. With the focus hackers put on Voter Registration systems in the 2016 election cycle, BPro has continued to enhance system security to ensure our systems and our customers stay ahead of those who wish to destabilize our democracy. Thus, BPro understands that security is a critical concern for the development, implementation and management of the SURE system replacement. Our strategy for addressing this concern is two-fold, first, focusing on adhering to secure coding practices to ensure that the code is structurally sound and free of any major structural issues that could cause the data, applications, or systems to be exposed to a high-level of risk and, second, to implement an active, dynamic security architecture consisting of technology and process that creates an active, operational paradigm for managing security and mitigating risks.

To ensure voter records are well maintained, BPro has developed seamless interfaces with federal and state agencies throughout the country. Some interfaces communicate in real time and some are scheduled on a regular cadence. These interfaces will allow Pennsylvania’s voter records to be checked against an assortment of other data, including death records, felon records, and both in-state and cross-state moves. Interfaces are built using a team approach with the DOS team members and BPro’s technical resources. BPro uses standard web services to communicate with other entities, which provides a secure, well-known and flexible means of exchanging information.

Five of BPro's current TotalVote VR/EMS system deployments are centralized, "top-down" systems that allow each county to connect to a central statewide system. BPro's Arizona deployment is a hybrid model, with 13 out of 15 counties using TotalVote VR/EMS and the state's two largest counties keeping their legacy VR/EMS system. In BPro's South Dakota and Washington deployments, we helped our customers transition from a "bottom-up" architecture, in order to better synchronize data. This effort was crucial in Washington, where new automatic and same-day voter registration laws made it impossible to support elections using a bottom- up architecture. TotalVote VR/EMS is now ensuring Washington voters can register and vote on Election Day, with real-time data synchronization in place to prevent anyone from registering and voting in more than one county.

BPro's proposed solution for Pennsylvania is a complete replacement of the SURE system with BPro's TotalVote suite of products. The TotalVote system has been well received by a wide range of state and local election officials for over a decade and meets the vast majority of Pennsylvania's RFP requirements "out of the box." This includes large, urban jurisdictions and small, rural jurisdictions, similar to the makeup of Pennsylvania's diverse group of counties. Through this response, BPro will demonstrate TotalVote capabilities and provide real life examples from our previous system deployments.



In every project, BPro is 100% committed to remaining on-time and on-budget. Every BPro system deployed to date has remained 100% on-budget. However, elections administrators understand that there are unforeseen events that will impact schedules. In addition to new or changed requirements and legislation changes, election results, special elections, recalls, retirements and a myriad of other events can take place that will cause a deployment schedule to change. This has been the case with every BPro VR/EMS system deployment to date. Using the [redacted] provides BPro with the flexibility to adjust timelines in order to best serve our customers. BPro's proven ability work closely with our customers to make schedule adjustments has ensured the successful deployment of BPro systems around the country. BPro will continue to provide this flexibility in Pennsylvania, with a goal of maintaining the schedule contained within this response and the knowledge that if the schedule does change, our previous experiences will help ensure the project remains focused and on track for a successful deployment.

IV. Qualifications.

A. **Company Overview.** Include company name, parent company if applicable, and a company overview and why you should be selected for this RFP based on your capabilities. The Offeror shall include any industry standards certifications or awards held by its proposed team and the level of certifications possessed. Also, disclose whether the organization's headquarters is located within the continental United States or not. If there is any other information you wish to add that is pertinent to your organization doing business with the Commonwealth or the DOS, please describe it in detail.

Offeror Response

BPro Inc is headquartered in Pierre, SD, and provides election systems around the United States of America. BPro is owned by Brandon and Abbey Campea. All BPro employees are United States citizens and all work developing and supporting BPro systems is conducted in the United States of America.

BPro currently provides centralized, statewide VR/EMS systems in states (Hawaii, New Mexico, North Dakota, South Dakota and Washington) and one hybrid VR/EMS system in Arizona, with 13 of 15 counties using BPro's centralized VR/EMS system. Many of our statewide VR/EMS customers share similarities with Pennsylvania and, through our 10+ years of elections experience, we have worked with urban and rural counties with diverse cultures, unique language requirements and various understandings of technology. This array of experience helps BPro successfully partner with state and local election officials to deliver systems and solutions, on time and on budget.

BPro is a supporting member of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a founding member of the Election Infrastructure Subsector Coordinating Council (EISCC), and a corporate member of the National Association of Secretaries of States Election Cybersecurity Task Force. Additionally, BPro is a Microsoft Silver Partner with Cloud Competency.

TotalVote received the Election Center's 2009 *State Technology Award* and was a finalist for the National Association of Secretaries of States *Ideas Award* in 2014. These awards are not why BPro should be selected to build a replacement of Pennsylvania's SURE system. BPro should be selected because of our company's proven success helping states around the country develop their election technology portfolio. BPro has listed every current VR/EMS customer as references. Except for our newest systems (Arizona and Washington), every BPro reference has selected BPro to build an initial election system and has extended the scope of BPro's services to build additional systems and features. These extensions are the result of BPro's ability to successfully deploy the system we were originally hired to build; our collaborative approach, which ensures our customers have control of the system throughout the entirety of the project; and BPro's user-friendly systems, which help election administrators save time while improving the accuracy of voter registration, election management and campaign finance records.

In Pennsylvania, BPro has completed the Department of General Services' process for self-certification as a small business under the Commonwealth 's Small Business Contracting Program. BPro is certified as a small business provider of Information Technology Goods & Services (Certification Number: 347081-2019-10-SB).

BPro personnel also have certifications that will be beneficial to the success of the project. Nissa Burger is a 2009 graduate of the Election Center's Certified Elections Registration Administrator (CERA) program. Josh Daws is a Lean Six Sigma Black Belt in IT, a Certified Scrum Product Owner and a Microsoft Certified Systems Engineer.

B. Company History. The Offeror shall provide the number of years established and a short history of business offerings specific to support solutions and operational hosting.

Offeror Response

Bowers Programming was founded by Kent and Sandy Bowers in 1985 in Pierre, SD. The company was incorporated as BPro, Inc. in 1997 and Sandy Bowers sold the company to Brandon and Abbey Campea in 2009. Before purchasing the company, Brandon and Abbey both worked for BPro.

BPro, Inc. began our first election project in 2007 for the South Dakota Secretary of State's office and today TotalVote systems are available to almost 20 million registered voters in 15 states. In Arizona, Hawaii, Montana, Nebraska, New Mexico, North Dakota, Oregon, South Dakota and Washington, BPro has statewide contracts. In California, Minnesota, Nevada, Ohio, Pennsylvania and Texas, BPro works with individual county election offices.

C. Organizational Structure. The Offeror shall describe their organizational structure for the Department. This shall include the total number of employees as well as the number of employees at each geographic location of offices or facilities. Please also describe the physical and logical security requirements, handling of sensitive materials, and emergency and disaster backup provisions. Describe how you will manage various work locations from the perspective of election security. This includes adherence to requirements that all work, data transmission, and data storage must be maintained in the United States, as applicable.

Offeror Response

BPro currently has 21 full time employees, with 13 employees and the company's owners (Brandon and Abbey Campea) based in BPro's Pierre, SD headquarters. Six employees work remotely around the country and, with the exception of Hawaii, employees are located in either the jurisdiction or time zone of a BPro customer to provide quick responses at any time. During BPro's Hawaii system deployment, BPro provided fulltime staff on location.

BPro's Pierre headquarters is a fully secured building. All building access is controlled by unique key cards and cameras ensure that all building entrants are recorded. BPro is in the process of moving to a new building, which will have comparable building security. Additionally, BPro is initiating a Clean Desk Policy as part of the move to new office space. A clean desk policy instructs that all employees must clear their desks at the end of each workday. Following a clean desk policy will reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.

[redacted] Microsoft has demonstrated a commitment to securing elections through the company's Defending Democracy program.

D. **Failure to Complete.** The Offeror shall disclose whether the Offeror (or any subcontractor or joint venture with the Offeror) has failed to complete a similar project by the original agreed upon timeline. If so, please list the commencement date of the project and the entity for which the project was to be performed, and an explanation why the project was not completed on time.

Offeror Response

As a successful election system provider, BPro has proven the ability to adapt to changes throughout the lifecycle of our election systems. It is BPro's experience that all deployment timelines are subject to changes that are out of our control. The Agile Development Methodology allows for changes to occur, with a continued focus on building the best system that meets every customer requirement. While BPro will do everything in our power to keep to the original schedule presented in this response, our experience leads us to believe your project to be no different.

BPro's three most recent VR/EMS deployments have all required schedule changes and none of the changes have resulted in a failure of the project. Instead, BPro has worked closely with our customers to revise the timeline to ensure the project continues moving forward.

Washington – As the project entered the final stages of development, the VoteWA team decided more time was necessary to train state and county elections personnel before the deployment. Working with BPro, the schedule was changed to add additional training time. The VoteWA system was successfully launched in June 2019 with a Minimum Viable Product (MVP) and the state successfully conducted their 2019 Primary and General elections using VoteWA.

Arizona – The initial project schedule called for system testing during key county election periods. With the lack of time for testing and a mock election, BPro worked with the customer to build in additional time to test the new system. By adapting the schedule, the system received adequate testing and was successfully launched in November 2019.

Montana – In an effort to maximize their 2018 HAVA funds, Montana added BPro's VR system to their existing BPro contract for Election Management and Election Night Reporting. This decision was reached without significant input from counties and the tight implementation timeline received pushback from county election administrators, who worried about launching a new system before 2020. BPro worked with the Secretary of State's office and Montana county election administrators to revise the timeline to ensure all Montana's counties were 100% committed to the implementation timeline and that BPro had the resources available to support their system development, which is now scheduled for 2021 go-live.

E. **Disclosure of Litigation**. The Offeror shall explain in detail whether the Offeror (or any subcontractor or joint venture with the Offeror) is currently or previously part of any litigation related to the implementation of a software and/or service solution, Data Center hosting, or breach of sensitive data.

Offeror Response

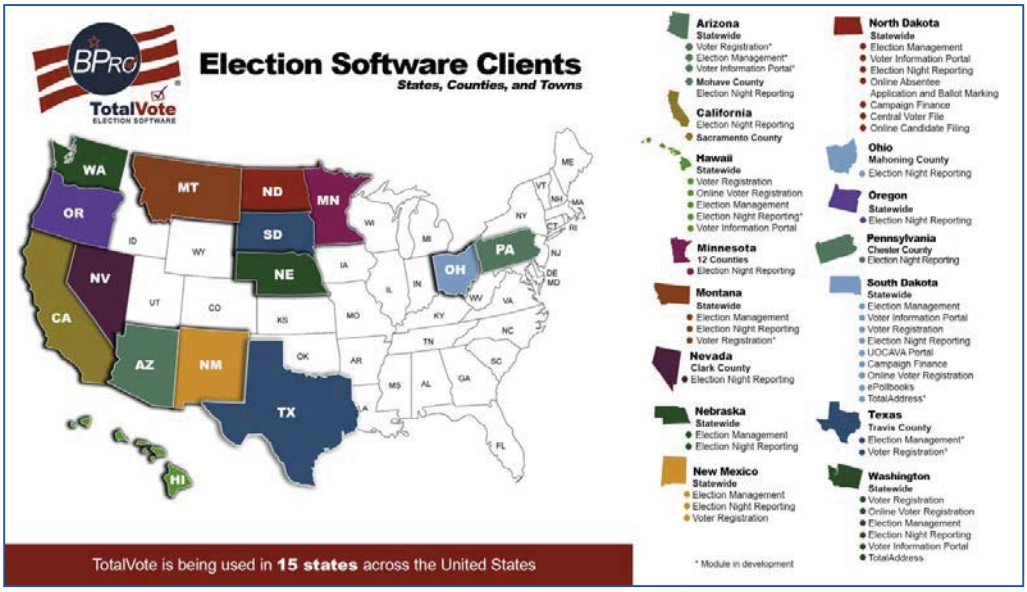
BPro has never been part of any litigation related to the implementation of a software and/or service solution, Data Center hosting, or breach of sensitive data.

F. Prior Experience. DOS requires an Offeror with a successful track record of implementing and maintaining an electronic statewide solution for the collection and management of voter registrations, election management, campaign finance, and lobbying disclosure, including the length of time supporting the application in each state.

1. Provide a minimum of 3 clients for whom similar professional services described in this RFP have been provided. Include the organization/jurisdiction name, address, organization/jurisdiction size, jurisdiction's registered voter population (where applicable), and average number of solution transactions per year. Studies or projects referred to must be identified and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted. Offeror(s) shall complete **Appendix B, Project References**.

Offeror Response

BPro has provided all six current TotalVote VR/EMS customers as references. BPro's references include both state and county level stakeholders for a full range of perspectives about our systems and our personnel. Additionally, North Dakota and South Dakota also use BPro's Campaign Finance Disclosure system. Below is a map of all current BPro election customers:



2. At a minimum, DOS is seeking an Offeror with a solution that has been used in at least 1 successful primary election and 1 successful general election in a similar size jurisdiction of the Commonwealth of Pennsylvania. Studies or projects referred to must be identified and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted. Offeror(s) shall complete **Appendix B, Project References**.

Offeror Response

Five of BPro's six references meet these criteria. Only Arizona, which went live in November 2019, has not completed 1 successful primary election and 1 successful general election using BPro's system.

3. Relevant Business Experience. The Offeror shall provide adequate detail, including contacts of any state where you performed a multijurisdictional implementation of your proposed solution and served as the prime contractor. Each implementation referenced must be in production. If the proposed solution has not be implemented in a production environment (i.e. implementation in process, etc), please provide whatever information you can for this section regarding your business experience in the elections and disclosure arena. Please reference **Appendix C, Glossary of Terms**.

Offeror Response

All six BPro references included in this proposal are multijurisdictional implementations of our proposed solution and are currently in production. We have included both state and county level personnel as references, to provide a full perspective of experiences working with BPro. BPro served as the prime contractor in five of six of the included references. Arizona required a system integrator to serve as the prime contractor and BPro was a subcontractor to Sutherland Global. It is BPro's experience that using a System Integrator, typically a massive, multinational company with limited understanding of elections administration, will increase the cost and timeline of the project, while providing very few tangible benefits.

4. Prior proposals. The Offeror must disclose any election system or disclosure system projects in which the Offeror has submitted bids or proposals (as a prime or sub) for consideration by a state or territory between August 2012 and the date of this RFP. At a minimum, this information must include:

a) State or territory
b) Contact name, telephone and email address
c) Date proposal submitted
d) Result of your bid
e) Brief description of your proposal

Offeror Response

In addition to the references that BPro has included in this response, below is a list of jurisdictions that did not select BPro for similar RFPs:

A. State of Delaware
B.
C. Submitted: January 16, 2018
D. BPro was not selected as a subcontractor to ElecTec Inc.
E. Voter Registration and Election Management system

A. State of Idaho
B.
C. Submitted: July 10, 2018
D. BPro was not selected
E. Voter Registration and Election Management system

A. State of Tennessee
B.
C. Submitted: December 1, 2016
D. BPro was not selected
E. Online Voter Registration system

A. Cook County, IL
B.
C. Submitted: January 30, 2015
D. BPro was not selected
E. Voter Registration and Election Management system

A. Shelby County, TN
B.
C. Submitted: March 9, 2017
D. BPro was not selected
E. Voter Registration and Election Management system

G. Lobbyist and Lobbying Disclosure. The Offeror shall list all person(s) or entities that have made lobbying contacts on your behalf with respect to this proposal or existing Department of State or Pennsylvania county contracts, systems, applications, or proposals. The Offeror must include the name and address of the lobbying entity or person(s).

Offeror Response

BPro has made no lobbying contacts in Pennsylvania with respect to this proposal. BPro currently has one county contract in Pennsylvania, providing an Election Night Reporting system to Chester County, PA. 2019 is our first year providing these services in Chester County. https://pennsylvania.totalvote.com/Chester

For more information, please contact , Chester County Commissioners' Office .

H. Firm Disclosure. The integrity of the DOS applications is paramount. The DOS, therefore, must assess the competency, integrity, character, reputation and background of the firm. Offeror(s) shall provide the following:

1. The details of any felony conviction within the last 10 years, gross or first-degree misdemeanor or offense of a criminal nature within the last 5 years, state or federal, of the firm or any person whose name and addresses are:

- Required by the RFP; or
- Are otherwise employees, major partners, officers, five (5) percent (or greater) stockholders, investors, or directors of the firm.

Offeror Response

BPro Inc and, to the best of BPro Inc's knowledge, BPro Inc's officers, directors or employees proposed to provide work on this RFP, have not been convicted of, pled guilty to, or pled no contest to any felony or first-degree misdemeanor within the last 10 years.

2. The details of any civil adjudication of fraud, state or federal, of the firm or any person whose names and addresses are:

- Required by the RFP; or
- Who are otherwise employees, major partners, officers, 5 percent (or greater) stockholders, or directors of the firm, regardless of the nature of fraud.

Offeror Response

BPro Inc and, to the best of BPro Inc's knowledge, BPro Inc's officers, directors or employees proposed to provide work on this RFP, have not been convicted of, pled guilty to, or pled no contest to any fraud charges.

3. A disclosure of details of any bankruptcy, insolvency, pending sale, reorganization, material litigation concerning the firm of any proposed subcontractor.

Offeror Response

BPro Inc has never filed (or had filed against it) any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors.

4. A disclosure of details of any foreign ownership or financing pertaining to the Offeror, any proposed subcontractor, or any employee, major partners, officers, stockholders, investors, or directors of the firm.

Offeror Response

BPro is wholly owned by Brandon and Abbey Campea, all BPro employees are U.S. citizens and all development is done 100% in the United States of America.

5. A disclosure of all countries in which your organization operates.

Offeror Response

BPro only operates in the United States of America.

6. Describe the corporate structure and ownership.

Offeror Response

BPro is an S-Corp wholly owned by Brandon (52%) and Abbey (48%) Campea. BPro has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Contracting Program, with the Information Technology Goods & Services designation. BPro's Small Business Certification (certificate number 347081-2019-10-SB) is included as part of this response.

7. If applicable, disclose all board members or any entity with more than 5% ownership in the organization.

Offeror Response

N/A

8. A disclosure of any foreign ownership and/or financing or investors. If there is no foreign ownership and/or financing or investors, the Offeror shall clearly state as such.

Offeror Response

BPro is wholly owned by Brandon and Abbey Campea and has no domestic or foreign ownership, financing or investors.

I. Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, programmers, consultants, quality assurance personnel, operational support staff (hardware & software), trainer(s) and technical writer(s) etc., who will be engaged in the project. Show where these personnel will be physically located during the time they are engaged in the Project.

For key personnel, Offeror shall complete **Appendix D, Personnel Experience by Key Position.** Key Personnel shall be dedicated to this project and shall not fulfil multiple roles unless as designated under

the RFP requirements. Indicate the responsibilities each person will have in this Project and how long each has been with your company.

Also, please outline your methodology for providing the services as defined in this RFP based on the skill set of the team you are submitting. The Offeror shall also make note of how the team may look during implementation and post-implementation. Additionally, please describe security training requirements for all personnel. If key personnel are located offsite, they must be available during the core business hours of 8:00am to 5:00pm within the eastern standard time zone or other hours, during critical support periods, as requested and outlined in this RFP. This would include descriptions for various types of personnel (i.e. developers, system administrators, etc). The Offeror shall also include resumes and support information to demonstrate the experience of the team for the proposed solution. Finally, the Offeror shall include an organizational chart to demonstrate team hierarchy and design to meet the needs of the RFP.

i. Key Positions

1. Project Manager

- **a.** Dedicated 100% to DOS. The Project Manager may not be diverted from this project to other projects without approval from DOS. This individual may also serve as the Scrum Master.
- **b.** Minimum of seven (7) years of experience in managing projects of this nature and scope.
- **c.** Experience in managing multiple, simultaneous, application, operational, development and infrastructure projects through complete lifecycles.
- **d.** Experience in development of project scope and optimizing project processes.
- **e.** Experience in project estimation, developing and successful deliver of complex project plans, involving 3rd party or external entities.
- **f.** Experience in defining milestones, monitoring to team performance and project reporting
- **g.** Experience in planning, organizing, prioritizing, and managing multiple work efforts across application teams.
- **h.** Experience in identifying and managing project risks and mitigation to acceptable risk levels
- **i.** Experience in baselining of projects and reporting variances, risk mitigation efforts
- **j.** Experience in managing multiple work orders in scope and performance once designated as an approved work package.
- **k.** Excellent written and verbal communication skills with team members, users, stakeholders and management.
- **l.** Experience in providing Project Management services within an agile environment
- **m.** PMI Certified or equivalent certification or experience
- **n.** Knowledge of PMBOK principles, MS Project, SharePoint, Project Server, TFS

2. **Account Manager.** The selected Offeror shall provide account management after the solution is placed into production. The account manager shall serve as the single point of contact for the Commonwealth and will ensure effective communication and coordination of releases and upgrades to its solution.

3. **Solutions Architect**
    a. The solutions architect is responsible for:
        i. Designing the solution architecture for the businesses.
        ii. Ensuring compliance to solution architectural design in the implementation of the project.
        iii. Providing architectural guidance to the project team.
        iv. Explaining technical issues and IT solution strategies to stakeholders and other IT professionals.
        v. Keeping an accurate record of materials used, expected deliverables, and milestones achieved.
        vi. Ensuring that solution milestones are accomplished on time and within budget.
        vii. Ensuring that solution architecture (software and programs) designed are in sync with the needs of the business and the business's hardware.
        viii. Reviewing the proposal of vendors and suppliers to ensure that quality inputs are delivered at the least possible cost.
        ix. Monitoring the activities of external developers on IT solution projects.
        x. Identifying and mitigating existing business risks associated with solution architecture.
    b. Product development experience
    c. Minimum of five (5) years of experience designing, developing and evaluating large logical and physical data models (500+ tables) using tools similar to and including Erwin/ERX and IBM Rational Rose
    d. Five (5) years of experience in database development and administration
    e. Five (5) years of experience providing database modeling/DBA services on high availability, multi-tiered, distributed computing systems as part of multi-year systems development projects
    f. Five (5) years of experience performing tuning/troubleshooting of database management systems
    g. Five (5) years of experience conducting database design reviews, reviewing project requirements, identifying entities, attributes and relationship and determining impacts of database changes
    h. Five (5) years of experience developing and enforcing database standards
    i. Preferred education: Bachelor's degree in Computer Science, Information Technology, or related field.

4. **Testing Lead**
    a. The Testing Lead defines, plans and coordinates all types of testing. He/she identifies, plans and manages test resources,

tasks/activities, issues, and risks throughout the project's software development lifecycle. He/she documents and manages risks and issues related to testing and ensures defects are properly documented and tracked to closure. The Testing Lead creates comprehensive project test plans, test cases, and scripts that ensure the system meets all approved requirements. He/she ensures tests scripts are traced back to requirements and all requirements are accounted for in testing.

b. Relevant experience:
   i. Five (5) years or more experience with designing and developing product testing and quality processes.
   ii. Demonstrated experience reviewing defects, assessing product quality, and reviewing requirements and design quality.

5. Functional or BA Lead

a. The Functional or BA Lead is responsible for:
   i. Tasks and techniques used to work as a liaison among stakeholders in order to understand the structure, policies, and operations of an organizations.
   ii. Recommending solutions that enable the organization to achieve its goals.
   iii. The Functional or BA Lead works with other assigned staff to gain general familiarity with overall systems functions and analyze defects and requests for change.
   iv. They will also provide general and technical design guidance and assistance.

b. Relevant experience:
   i. Experience in functional and technical requirements gathering.
   ii. Demonstrated experience of the SDLC.
   iii. Five (5) years' experience leading information gathering sessions to capture and document business requirements, business processes, and technical considerations.
   iv. Five (5) years of experience performing complex task analysis to evaluate task flow for applications and web sites
   v. Five (5) years of experience producing technical documents such as business requirements documents, use cases, and business specifications.
   vi. Five (5) years of experience leading review sessions to discuss draft documentation and determine the appropriate revisions.
   vii. Preferred education: 4-year college degree or equivalent technical study

6. Training Lead

a. The Training Lead is responsible for:
   i. The Training coordinator is responsible for coordinating all training requirements and tasks, including:

ii. Interacting with project and program staff to understand the business area, such as participating in design and development
iii. Developing training materials
iv. Scheduling training
v. Ensuring training rooms and equipment meet the minimum requirements
vi. Developing individual training/knowledge transfer plans and monitoring individual progress, including conducting knowledge transfer assessments and providing quarterly assessment reports identifying staff development status
vii. Creating, distributing, collecting, and reviewing training/mentoring session feedback and modifying materials as appropriate.
viii. Maintaining quality service by establishing and enforcing organization standards.
ix. Designing system training manuals or supporting solution documentation by identifying and describing information needs, submitting initial versions for DOS review, and revising and editing the final copy of the training materials.

b. Experience shall be as described for the position of "Training Lead"

Offeror Response

BPro's proposed team for Pennsylvania has a combined 20 years of experience working with BPro systems and has played key roles in the successful deployment of multiple TotalVote VR/EMS/Campaign Finance systems around the country. Additionally, several members of the proposed Pennsylvania team came to BPro from the client side and have an additional 25 years of combined experience working with BPro systems from the customer side. This unique experience gives our team the insight to understand both sides of the deployment process and work closely with customers to keep projects on time and on budget.

Using the Agile Development Methodology provides flexibility and allows BPro to best serve our customers. The Agile-based approach follows the principle that the highest priority is to satisfy the customer through early and continuous delivery of working software. BPro's proposed team has a combined two decades of experience deploying TotalVote systems using the Agile-based methodology.

Our proposed project leadership team has experience in delivering large technology changes to elections including Voter Registration and Election Management, Election Night Reporting, and Campaign Finance systems. For the day-to-day execution of the project, BPro proposes:

- **Project Manager** – With almost twenty years' project management experience, Kari Stulken will serve as the Project Manager for BPro and her #1 job will be to administer the project to a successful outcome. Kari will be 100% committed to the project and will coordinate all activity and issues from the BPro project team. The BPro Project Manager will be the focal point of communication and coordination for all team members. The BPro PM is expected to be in continuous communication with

the DOS Project Manager. Kari is also a Certified Scrum Master and will fill that role in Pennsylvania. While Kari only started working for BPro in 2018, her first experience working with BPro was in 1998 as part of a Requirements Gathering effort while she worked for the South Dakota Attorney General's Office. Since 1998, she has filled various roles alongside BPro staff when BPro was contracted with multiple South Dakota state agencies on several projects.

- **Account Manager** – After the Pennsylvania system is live, Kari Stulken will continue to be involved in the project as the Account Manager. As Project Manager, Kari will develop relationships with DOS and county election officials. These relationships will help Kari provide ongoing account management and will ensure effective communication and coordination of releases and upgrades. Kari is based in BPro's Pierre headquarters.

- **Solutions Architect** – Kevin Kumpf will lead all technical decisions regarding product design and infrastructure. As the Solutions Architect, Kevin will work directly with DOS to monitor the project to completion and oversee the implementation teams. As Solutions Architect, Kevin will lead all technical decisions regarding product design and infrastructure and will serve on the project team throughout the project. Kevin is based in BPro's Pierre headquarters.

- **Business Analyst Lead** - As BPro's elections systems expert, Dakota Bixler has been instrumental in most of BPro's recent successful system deployments, including Arizona, Hawaii, and New Mexico. Dakota will work directly with the BPro Project Manager to administer the project to a successful outcome. Her duties will also include business analysis, iteration and release planning and coordination of development activity. Prior to joining BPro in 2014, Dakota was the South Dakota Secretary of State's Election Coordinator and helped build and manage South Dakota's TotalVote VR/EMS system. Dakota works remotely in Marshall, MN and comes to BPro's Pierre headquarters on a regular basis.

- **Testing Lead** – Laura Heckmann was instrumental in the success of the VoteWA system deployment, her first system deployment as a BPro employee. Prior to joining BPro, Laura spent over five years at the Lincoln County (South Dakota) Auditor's Office, where her duties as an Election Specialist required daily use of the TotalVote system. Laura's familiarity with the TotalVote system makes her the ideal person to lead all system testing. Laura works remotely from Durham, NC.

- **Development Lead –** Joe Faddoul has worked for BPro since 2003 and has developed pieces of every TotalVote system deployed today. As the Development Lead, Joe will oversee BPro's development team and ensure all development is completed to meet Pennsylvania's requirements. Joe is based in BPro's Pierre headquarters.

- **Training Lead –** As the BPro Training Lead, Dakota Bixler will deliver training activities, draft a Training Plan, and ensure successful staging of training events. She will also coordinate organizational change management deliverables for the project.

- **Infrastructure and Security Lead** – Joshua Daws has 17 years of technical operations and project management experience in elections. As the CTO for the Nebraska Secretary of State's Office, he co-authored their RFP to implement their centralized voter registration system (NECVRS). From 2006 to 2012, Josh worked with contracted security vendors to test the internal and external controls of the NECVRS and to remediate their findings. In 2008, Josh created a security training curriculum and used social engineering to train end users. Josh also worked with BPro to implement a new election night reporting system for Nebraska in 2010. As graduate of the University of Nebraska-Lincoln in History, minoring in Political Science, he understands the technical and governmental sides of the election process.

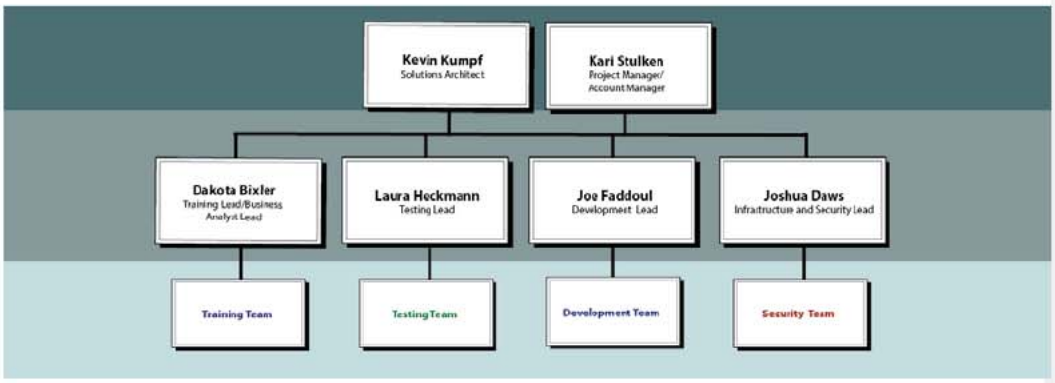
The list of Key Personnel does not represent all of the roles that BPro will staff for the Pennsylvania project. In addition to the above Key Personnel, the following disciplines are supported by senior level resources that will lead key support areas:

- **Database Analyst**: (DBA) to work with the DOS DBA to create processes for transfer of Pennsylvania VR data and images to TotalVote. Duties include: map fields, create extract, transmit and load procedures (ETL), coordinate with BA's and QA's for data integrity and quality standards.

- **System Analyst**: (SA) has extensive domain knowledge (i.e. elections) and prior experience of implementing similar systems, plus the technical design understanding and implications of implementing various features and functions in the system. BPro's SA understands how to design application functionally and technically and will be to work with the subject matter experts on how to best design the TotalVote application for Pennsylvania's needs.

- **Systems Engineers**: BPro's system engineers will lead activities for installation and implementation of system and network infrastructure components meeting security and configuration standards.

BPro Organizational Chart



J. Subcontractors. Provide a subcontracting plan for all subcontractors, including small diverse business and small business subcontractors, who will be assigned to the Project for each Lot. The selected Offeror is prohibited from subcontracting or outsourcing any part of this Project without the express written approval from the Commonwealth. Upon award of the contract resulting from this RFP, subcontractors included in the proposal submission are deemed approved. All subcontractors must also adhere to the general provisions outlined in **Section IV. Qualifications** of this RFP. The selected Offeror shall also supply applicable submissions for **Section IV. Qualifications** for each subcontractor associated with the proposal. Also, please describe your process for selection and management of subcontractors, including how subcontractors are evaluated on an ongoing basis for meeting security requirements. For each position included in your subcontracting plan provide:

1. name of subcontractor;
2. address of subcontractor;
3. number of years worked with the subcontractor;
4. number of employees by job category to work on this project;
5. description of services to be performed;
6. what percentage of time the staff will be dedicated to this project;
7. projected timeframe of involvement;
8. geographical location of staff; and
9. resumes (if appropriate and available).
10. Describe security training requirements for subcontractors. This would include descriptions for various types of personnel (i.e., developers, system administrators, etc).
11. Describe what information subcontractors will be allowed to access and how you will monitor their activities.
12. Describe whether the Offeror and proposed subcontractor(s) have previously worked together.

Offeror Response

BPro will not use subcontractors, unless Unique Source is used for Tier 1 Help Desk issues.

V. Financial Capability. The Offeror shall describe your company's financial stability and economic capability to perform the contract requirements. Provide your company's financial statements (audited, if available) for the past three fiscal years. Financial statements must include the company's Balance Sheet and Income Statement or Profit/Loss Statements. Also, include a Dun & Bradstreet comprehensive report, if available. If your company is a publicly traded company, please provide a link to your financial records on your company website in lieu of providing hardcopies. The Offeror shall also provide information regarding whether you foresee or are presently involved in any type of purchase, merger or being bought out by another company. The Offeror's financial capability information should include information on any foreign ownership or financing pertaining to the Offeror, any proposed subcontractor, or any employee, major partners, officers, stockholders, investors, or director of the organization. The Commonwealth reserves the right to request additional information to evaluate an Offeror's financial capability and the source(s) of any foreign ownership and investment. If the Offeror is unable to comply with any of the

financial capability requirements, please identify where you are unable to comply and provide a thorough explanation. At a minimum, the Offeror will provide:

- **A.** If available, audited financial statements, balance sheets and income statements or Profit/Loss Statements (including auditor's opinion and footnotes) for the most recent three fiscal years.
- **B.** Unaudited, interim financial statements, balance sheets and income statements or Profit/Loss Statements to bring financial information current within 12 months of submission of the bid.
- **C.** If available, please include a Dun & Bradstreet comprehensive report
- **D.** Please indicate whether your company is publicly traded or not
- **E.** Please provide information whether you foresee or are presently involved in any type of purchase, merger or being bought out by another company or entity.
- **F.** Please include any application information on any foreign ownership, financing or investors.

Offeror Response

BPro has included audited Profit and Loss Reports and Balance Sheets from 2016-2018. BPro is not publicly traded, has no foreign ownership and does not anticipate being bought out by another company or entity.

VI. Requirements. The following requirements and standards must be met. The Offeror shall acknowledge their understanding in their response and provide additional explanation where requested and whenever possible. Please refer to **Appendix C, Glossary of Terms** for additional clarification.

A. Incoming Transition. During the incoming transition period, the selected Offeror's project manager and project team will work closely with the DOS and the current Contractor. The project manager shall have oversight responsibility of all Offeror resources and its entire set of subcontractor resources. Responsibilities during the transition shall include, but are not limited to:

1. Review and become familiar with the current and active project and all pertinent system documentation.
2. Ensure the incoming key resources effectively learn the business processes and procedures used at DOS.
3. Capture, record, and manage and report incoming transition issues to the DOS.

B. Timeline. The selected Offeror shall implement the proposed solution with all 67 county election offices and DOS staff no later than December 31, 2021.

The Offeror shall submit with its proposal a draft project timeline based on the draft implementation plan. The draft timeline shall include, but not be limited to, all deliverables listed in **Section VIII.Tasks/Work Plan**, key dependencies, and transition to maintenance and support following the implementation period.

Offeror Response

Through our previous implementations, BPro has proven the ability to successfully work with both the customer and legacy vendors to provide a smooth transition process. BPro will implement the proposed solution no later than December 31, 2021 and has included a draft project timeline as part of our response to **Section VIII. Tasks/Work Plan**.

C. **Resources.** At present, the DOS has allocated 23 members in the existing project in the following roles. The Offeror shall recommend resource and roles necessary to support the proposed timeline and requirements of the RFP. The Offeror shall also provide an organizational chart in their submission.

1. 3 Application Support (including 1 Application Support Lead)
2. 1 Technical Writer
3. 5 Help Desk Agents
4. 3 Business Analysts
5. 3 Quality Assurance
6. 8 Developers (including 1 Development Lead)

Offeror Response

Current SURE resources will play a key role in the successful implementation of a new system. In all other previous deployments, BPro has utilized the experience of system support staff to provide a deeper understanding of the previous system and valuable leadership as the new system is developed and deployed.

BPro proposes to utilize:

- **Application Support & Business Analysts** – Work with BPro Business Analysts to support application with Pennsylvania's 67 county election offices, test releases.
- **Technical Writer** – Assist in documentation by providing knowledge of existing Pennsylvania election laws and procedures.
- **Help Desk Agents** – As part of this proposal, BPro proposes DOS continue to provide Tier-1 support. Many TotalVote Tier-1 questions center around election laws and procedures. BPro will provide all Tier-2 support.
- **Quality Assurance** – Perform automated and unit testing with each release
- **Developers** – Apps will still exist that need support and development that interface with TotalVote

D. **Solution Overview.** The Offeror shall provide an overview of the proposed solution and services offered to DOS. The overview must consider the Offeror's proposed approach to implementation and how the proposed solution will be provided to the DOS and county election officials (e.g., complete replacement of the existing application, maintaining the existing application while phasing in a new, parallel application, etc.). The Offeror shall present a concise high-level overview of the proposed solution, including:

1. System architecture diagrams;
2. If the proposed solution includes multiple deployment options (e.g., cloud, On-Premise, etc.), an overview of the differences should be submitted in the proposal;

3. Minimum application requirements for front-end and back-end modules;
4. Minimum requirements for the backend based on the stated requirements;
5. Interfaces and integration points;
6. Third party hardware and software;
7. Other key elements that will help the DOS better understand your proposed solution design; and
8. Completed functional matrix.

Offeror Response

BPro proposes for a complete replacement of Pennsylvania's SURE system with our TotalVote suite of products with features to cover every aspect of Voter Registration, Election Management, Campaign Finance Reporting and Lobbyist Tracking. BPro has fully completed the functional matrix, based on the TotalVote systems and features that are currently deployed around the United States. With our experience in providing election software, BPro has full comprehension of the significance of the effort to manage voter registrations, and how the daily maintenance of quality of voter records are an integral part of the overall success of every election. We integrate data across all BPro modules to provide seamless management of voter districts with Candidate Filing, Elections Management, Ballot Entitlement, Ballot Styles, Absentee Balloting, and Election Night Reporting. Online web information is provided for a wide range of public data such as sample ballots, polling place location, voter status, incumbent information, and election results.

The familiar, intuitive and consistent interface makes TotalVote easy to learn and easy to train new staff. Using a common web interface, point and click simplicity is provided along with the ability to use keyboard driven operations for the user who is doing "heads down" repetitive work.

TotalVote has fail-safe checks throughout the application to present the user with only what is currently active for an election and give instructive error messages when information is not sufficient to complete processing. Our web interface senses when a user is navigating away from a page and prompts the user when there is updated information that has not been saved to the displayed record.

One user login applies to the entire system and role-based security provides the ability to limit the areas accessible to any user to the area of work that is necessary for their job. Help text is available throughout the system and is fully searchable.

TotalVote has been designed and developed using state-of-the-art software language and an operating system that embraces the era of internet deployment and mobility support. Data sharing is a central feature of this architecture and will support Pennsylvania's future needs through the use of web services, data standards, and automation. Data flows through each TotalVote module minimize or even eliminate, data entry errors. Voter registration data populates candidate records, which makes up ballot data. The ballot data is used to setup election returns, results, and canvassing, all without any user input. Innovative features are documented throughout our proposal and we will continuously improve and create, even after TotalVote is in production.

TotalVote is built with configurable parameters so that if the business or administrative needs of the office change, in most cases the application can be adapted by your staff with minimal configuration changes that require reprogramming. For situations requiring program change, BPro can readily provide the necessary changes or assist your staff to accomplish needed changes.

Configurable parameters allow your management to alter list selections and code selections, and change operation options, without reprogramming. Most selection lists are driven by tables that are defined by your System Manager. Operating parameters are also configurable to adapt to Pennsylvania's current business needs, and to allow you to adjust to changing needs. With many combinations of options available, exceptions to the standard rules can be managed and built in. In addition, where necessary in the system, overrides with appropriate security level are available, and these overrides are audited to oversight reports.

Interfaces are built using a team approach with the team members from Pennsylvania and the BPro technical resources. BPro uses standard web services to communicate with other entities, which provides a secure, well known and flexible means of exchanging information.

BPro's TotalVote solution has been deployed in both on premise and cloud environments.

Figure 1 - Proposed TotalVote System Architecture

The simplicity of TotalVote only requires a current major browser (Chrome, Firefox, Edge, Safari) and MFA to access the system. For imaging, TotalVote users will need a PC and a scanner with a commonly used TWAIN driver installed. TotalVote is also integrated with Dymo printers but those are not required.

Below is a list of additional third-party software used in TotalVote:

- Iron Barcode
- Iron PDF
- iTextSharp
- Telerik
- SweetAlerts
- JQuery
- Hangire
- DYMO Framework
- Dynamsoft

E. Software Overview. The Offeror shall provide a detailed description of the proposed solution's software and product versions being proposed. The response to this section must detail the system features and capabilities and indicate if these are native to the software or if integration with a third-party software is required or recommended.

Offeror Response

The TotalVote system has been used in multiple states and is proven to improve the voter registration process, streamline entire election management process and provide greater transparency around the financing of campaigns. Each TotalVote system has been configured to the unique laws and requirements of each customer BPro works with. To begin every new project, BPro determines which current TotalVote system most closely matches the requirements of the new customer. The closest matching system's source code is used as the baseline code and is then configured to meet the exact requirements of the new system. Using this methodology, every TotalVote system is a unique version and each state's system independently receives version numbers.

Throughout the product description you will read about work queues. Work queues route work around the office, pairing data with associated images of documents to put them on the desktop of the right person for the most efficient processing. TotalVote allows election officials to configure the assignment of work queues to different users and define which parameters are used to push work from one work queue to another automatically. TotalVote creates workplace efficiencies by allowing multiple users to work from the top of the work queue (first in, first out), or work can

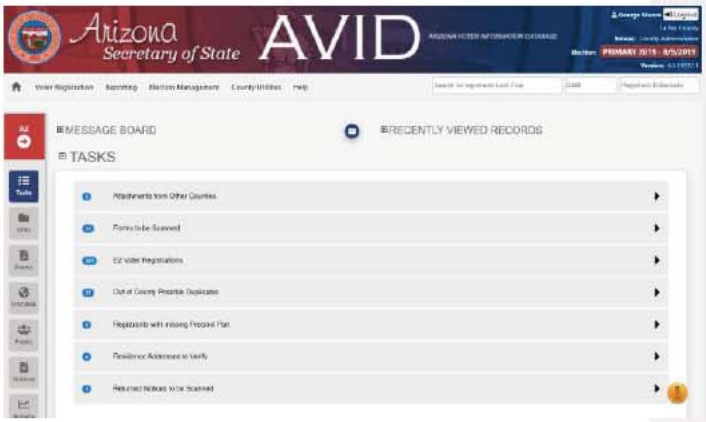


Figure 2 - TotalVote Work Queues

be specifically assigned to users. The system can monitor how long a record has been sitting in a queue and provide statistics for workload oversight.

In addition to deploying Voter Registration/Election Management systems in six states, BPro currently provides standalone Election Management systems for three additional states (Montana, Nebraska and Oregon). These systems help state and county users build elections using a common interface that can communicate with other election systems before, during and after an election. TotalVote's EMS module is an intuitive, user-friendly system that is used by states and counties around the country to set up every aspect of an election. Many jurisdictions have made the switch from using the EMS system provided by their tabulation vendor and now use TotalVote EMS as their primary system for setting up elections. Because TotalVote EMS is compatible with all the major tabulation systems, exports from TotalVote do not need to be manipulated before being exported to the tabulation vendor's system.

Figure 3 - Building Countywide Election Ballots

In TotalVote, the DOS can create a statewide election and define the election based on the type of election (primary, general, etc.), races on the ballot, districts, counties, and parties that are included in the election. Once the SOS has set up an election, authorized county users can further define local races that are part of a statewide election and manage the local portions of statewide elections. In addition, authorized county users can use TotalVote to create local-only elections and manage every aspect of them. TotalVote provides a comprehensive set of parameters to manage all details of any election. During the Analysis and Requirements phase of the project, we expect to identify additional specific parameters needed for Pennsylvania.

One of the primary components of the module of TotalVote is candidate management. Candidates can register in-person or online through TotalVote and as each candidate is certified, information is pulled from the candidate's voter registration record and linked to the appropriate contest. The Candidate Table contains all identifying information, including a unique Candidate ID Number. Candidates can also utilize the public portal to file their candidacy online.

Once the ballot definition information is entered into the system, TotalVote seamlessly creates every ballot style, automatically, in a single step. A ballot style is created for every precinct part and duplicate ballot styles are combined and connected to all applicable splits. The system includes multiple safeguards for quality assurance by allowing the County to error check throughout the process. After the necessary ballot styles are

determined, TotalVote presents sample ballots for review before releasing it to the ballot printing vendor. TotalVote also indicates the number of ballots necessary for each precinct. Once the accuracy of ballot styles is verified, the file is exported for printing. At that point, sample ballots can be released to the public through the Public Portal.

TotalVote also feeds the back-end data for all Public Portal functions. When on the Public Portal, a public user can search for and interact with registration and election data in the TotalVote system. The Public Portal is accessible, secure, easy to navigate, mobile-friendly, and can support multiple languages (currently TotalVote supports five languages – plus English). If a registered voter wants to specifically look up their own personal information, they would need to enter a few identifying factors, such as name, address, or date of birth to access their own record. When viewing their own record, voters can view the following information:

Voter Registration Information	UOCAVA Information & Ballot	Voting History
Important Election Dates	Accessible Information & Ballot	Provisional Ballot Status
Districts Where Eligible to Vote	County Elections Office Information	
Sample Ballot	Election and Voter Turnout Results	

Note: A voter that is protected under the Address Confidentiality Program will never appear on the Public Portal.

BPro currently works with six states (statewide) and individual counties in six states to provide fast, user-friendly Election Night Reporting websites, which have been well received by voters, election administrators, candidates, political parties, and members of the media. TotalVote's Election Night Reporting system is compatible with all major tabulation systems and results and turnout are updated automatically when a tabulation file is uploaded into TotalVote. By uploading Pennsylvania's GIS shapefiles, web visitors will be able to navigate a map of Pennsylvania and drill down to view election results and voter turnout by State, County, Congressional District, Legislative District, Senatorial District, School District, Tax District, and Precinct from any device. All public facing systems are built with responsive design and WCAG 2.0 compliant for full accessibility.

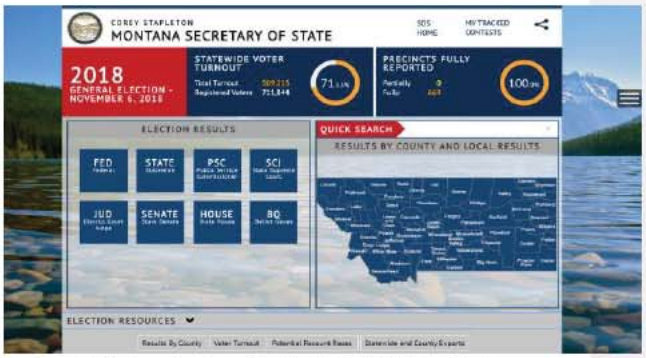


Figure 4 - Montana Secretary of State's Election Night Reporting homepage

TotalVote's Election Canvassing module is used to provide election canvassing for all statewide and local elections. After the completion of the Election Night Reporting, the TotalVote canvassing module is utilized in the canvassing process at the State and County levels. After provisional ballots are processed, TotalVote automatically provides a canvassing report for the County Canvassing Board. No extra data entry is required because the data is pulled from the previously imported or entered returns data. TotalVote's canvassing system would include creation and customization of all necessary reports.

At the request of customers, BPro built TotalVote's Campaign Finance module in 2013. The system has allowed North Dakota and South Dakota to provide greater transparency into campaign donations, has helped candidates and committees report donations and expenditures more efficiently through an online portal and has ensured that all campaign donations are available to be viewed by the public. After the Campaign Finance module was well received by key stakeholders, BPro also built a Lobbyist system for South Dakota to meet their requirements and provide lobbyists and lobbying firms an online option to register as lobbyists. The system also allows lobbyists to amend their affiliations, submit required documentation related to lobbying activities and pay fees associated with filing.

Figure 5 - South Dakota Campaign Finance Reporting System

In order to simplify federal reporting requirements, BPro worked closely with customers to automatically collect data required by the federal government. TotalVote simplifies the Election Assistance Commission's EAVS survey by collecting quantitative data pertaining to the National Voter Registration Act, the Uniformed and Overseas Citizens Absentee Voting Act, and other election administration issues, including the counting of provisional ballots and poll worker recruitment. The collection of this data is built into TotalVote to comply with the EAC EAVS Survey requirements and makes what was an arduous requirement simple to comply with. Data is presented in the EAC-required format and election administrators can submit the data to the EAC in a few simple steps.

F. Technical Capability. The Offeror shall describe their proposed solution in the following areas:

1. Describe your system's capability that allows "state of the art" services and your commitment to technological advances in the industry.;

Offeror Response

BPro has a track record of embracing technological advances in order to streamline the voter registration process, more accurately locate voters, and better ensure the security of sensitive personal data that is housed in a voter registration database. BPro designed and developed TotalVote using state-of-the-art software language and an operating system that embraces the era of internet deployment and mobility support. Data sharing is a central feature of this architecture and will support Pennsylvania's future needs through the use of web services, data standards, and automation. Data flows through each TotalVote module minimize or even eliminate, data entry errors. Voter registration data populates candidate records, which makes up ballot data. The ballot data is used to setup election returns, results, and canvassing, all with minimal user input. Innovative features and services are documented throughout our proposal and we will

continuously improve and create, even after TotalVote is in production. Most recently, BPro has integrated TotalVote with Help Desk systems such as DevOps and ServiceNow to provide a direct connection.

Since the first TotalVote Voter Registration system was deployed, BPro has continually added new features to secure Personally Identifiable Information (PII) inside the database. BPro's first system requiring Multifactor Authentication was launched in 2012 and ever since, BPro has continued to add additional factors to provide more login options while maintaining the highest level of security. More recently, BPro has introduced Yubikey and RSA integration as MFA options, as well as integrating with state and county Active Directories to provide a Single Sign On across all TotalVote modules. Additionally, BPro has integrated CloudFlare and other 3rd party security appliances to add additional layers of protection against DDOS.

BPro has also demonstrated its commitment to technological advances that improve election administration by developing the first commercially available GIS-based address point to support voter registration functionality. We've developed the solution as a standalone software product for managing point address data and sits between GIS software products and TotalVote. BPro's GIS software product provides the functions necessary to maintain point address data and accommodates changes over time from both GIS data and Voter Registration requirements. Our product provides interfaces to ingest GIS data and services, present the information to VR operators in an understandable user interface and supports address maintenance required for management of voter registration rolls over time. Through over a decade of developing election systems, BPro understands that VR operators are usually not skilled GIS operators and built a user-friendly system that only requires typical office-type computer user skills.

All BPro systems are built to help election workers process their responsibilities faster and more accurately. TotalVote provides them with the tools to spend more time doing their job and less time manipulating the system to access the data necessary to perform their job. BPro has also built TotalVote to accommodate advances in computer technology and all TotalVote administrative systems support dual screens to maximize efficiency.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. [redacted]:

Offeror Response

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Offeror Response

[redacted]

5. Describe in detail any security test(s) that your system has been submitted for and the results of the test(s). (e.g. who, what, when, etc.);
Offeror Response

TotalVote systems are regularly tested by a variety of security experts in the six states where BPro currently provides a centralized Voter Registration system. These security tests are conducted on either a weekly or monthly cadence by many sources, including the Department of Homeland Security, the National Guard, state IT departments and customer-procured third-party security experts. While all test results are strictly confidential, the variety of testing parties and the regular testing schedule demonstrate BPro's recognition of the importance of regular testing of each and every TotalVote system.

6. Describe how the proposed solution was independently audited from a third-party security researcher;
Offeror Response

TotalVote VR/EMS systems have been independently audited by third-party security researchers in every current system deployment. While the results of these audits cannot be included in a public document, we expect Pennsylvania will require similar audits and we will gladly comply.

As a result of the sensitivity of the data stored within TotalVote, BPro recommends SOC-2 Type 2 audits via independent auditors to report annually on the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the control description specifically relating to the TotalVote contract. If selected, BPro will conduct this audit of Pennsylvania's TotalVote system on an annual basis as required.

The auditor's report will conform to the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Reporting on Controls at a Service Organization published by the American Institute of Certified Public Accountants (AICPA). The auditors will conduct a Service Organization Controls (SOC) 2, Type 2 SSAE 18 audit. BPro will provide the auditor with access to all systems, facilities, information and people required perform the audit. The control objectives of the audit shall be at a minimum, equivalent to those required under the General Accounting Office Federal Information Systems Computer Audit Manual (FISCAM) for performing all work. FISCAM is also consistent with National Institute of Standards and Technology's (NIST) guidelines for complying with the Federal Information Security Modernization Act of 2014 (FISMA). This law requires federal agencies to develop, document, and implement agency-wide programs to ensure information security. NIST Special Publication 800-53 provides recommended security controls for federal information systems and organizations.

The procedures and report meet the FISCAM requirements and include application systems testing. Each review follows guidance provided by GAO's FISCAM Manual and includes a corrective action plan. BPro reviews the report, responds to each finding, and identifies its proposed corrective actions. The auditor's annual reports cover operations from effective date of full servicing capacity through the first year.

7. Describe in detail any non-security audit that your system has been submitted for and the results of the test(s). (e.g. who, what, when, etc.); and

Offeror Response

The TotalVote system has recently undergone several 3rd party audits designed to improve system performance. In order to audit how quickly TotalVote returns data, the VoteWA system speed is audited on a regular cadence. Load tests have been performed using Postman scripts and to audit the system development code, BPro has run numerous automated smoke tests and regression tests.

In Arizona, BPro has used automated load and stress tests to ensure system performance and uses Application Insights to ensure all APIs are performing properly. With over 75 interfaces between Maricopa County and Pima County's VR systems, it is imperative to identify the source of any API errors immediately. Additionally, Maricopa and Pima counties have built their own tests to validate connectivity and operations.

With every system in deployment, BPro reviews its internal business coding processes to ensure system performance meets contractual obligations.

8. Explain briefly any area of expertise that sets your company or organization apart from other providers as well as your company's resources and institutional stability.

Offeror Response

BPro is an independently owned, fiscally responsible company that has grown organically over the past 35 years. Because we don't have to answer to investors, we aren't required to gouge our customers to meet artificial margins. Instead, we focus on delivering the highest quality systems at a fair price and we continually reinvest in our people and our software. Many BPro employees have been with the company for 10+ years and several current employees have worked for BPro for over 20 years. As we have grown in the elections space, we have strategically sought out election experts from around the country and today our employees include CERA graduates and other former state and county election officials. These employees have added elections expertise and helped BPro continue to develop software and systems that best meet the everchanging needs of state and county election officials.

An area that is often overlooked in any election technology RFP process is the technical expertise of the variety of county election administrators that will use a new system. The RFP process often takes longer than anticipated and counties are often forced to learn a new system quickly and in the midst of the myriad of other election activities that take place leading up to an election.

BPro's systems are used by jurisdictions of all sizes, from Harding County, NM (population 655) to King County, WA (population 2.2 million). The ease of use of TotalVote allows election administrators to quickly learn the new system and incorporate it into their preset election routines. To help ease the transition process, BPro adapts each TotalVote system to incorporate a state's current workflows, forms and election processes whenever possible.

The first few TotalVote VR systems went live in some of the smallest states in our great country. South Dakota, North Dakota, Hawaii and New Mexico county election officials all helped prove that a new Voter Registration system could be incorporated by even the smallest, most remote jurisdictions that are not typically known for their technological prowess. Today, counties in major metropolitan areas (i.e. Seattle, WA, Austin, TX, Las

Vegas, NV, and Phoenix, AZ) are also realizing the advantages of TotalVote. BPro's proven ability build systems that are usable for the smallest jurisdictions while also powerful enough for large jurisdictions is one aspect that sets us apart from our competition.

The same is true for BPro's TotalAddress portion of our Voter Registration system. BPro has developed and successfully deployed a robust, near and long-term solution for managing point address data that has the capability of obsoleting the historical, error-prone street index file. BPro's GIS software product provides the functions necessary to maintain point address data and accommodates changes over time from both GIS data and Voter Registration requirements. TotalAddress will also provide a significant time savings after the next round of federal, state and local redistricting. Our product provides interfaces to ingest GIS data and services, present the information to VR operators in an understandable user interface and supports address maintenance required for management of voter registration rolls over time. VR operators are NOT required to be skilled GIS operators and only require typical office-type computer user skills. The ease of use has led to successful implementations of the system in Washington and Arizona, with South Dakota planning to implement the system in the near future.

TotalVote is an intuitive, user friendly system that can easily be adopted and accepted by small jurisdictions, while providing powerful tools and insights for large jurisdictions with a dedicated IT staff. BPro has built the TotalVote system by engaging our customers and building the features and tools that will best help election administrators perform their job. More than anything, what sets us apart from our competition is the relationships we have developed with every customer. The strengths of these relationships are demonstrated by the comprehensive system we are proposing in this response.

G. State of Manufacture. The selected Offeror must complete the chart provided in **Appendix E, State of Manufacture**. The Offeror is expected to list the name of the manufacturer and the state (or foreign country) of manufacture of all hardware required in the proposed solution. If the hardware component is domestically produced, the Offeror must indicate the state in the United States where the item was manufactured. This chart must be completed and submitted with the proposal.
Offeror Response

[redacted]

Other than a computer with a major browser, no hardware is required. Some optional hardware may be items currently owned by counties to support the SURE system. That includes:

- DYMO LabelWriter 450
- Handheld barcode scanners
- TWAIN-Compliant document scanners

H. Data Migration, Conversion, and Validation. The Offeror shall be responsible for migrating existing Department and county election official's data into the proposed solution. The Offeror shall also be

responsible for working with the Department and county election officials to develop a data plan to execute, convert, and validate data migration activities. The Offeror shall describe its experience and capabilities to perform this service. The proposal shall have individuals with experience in data analysis, migration, and reporting. The Offeror shall also describe their approach to data migration, including how mapping between systems will be documented and defined, cleaned/reformatted, and tested prior to migrated to the proposed solution. Also, please describe the level of desired support from the Department and county election officials to accomplish data migration, conversion, and/or validation.

Offeror Response

The Data Conversion effort is a key success factor for replacing Pennsylvania's SURE system. Bad data can overshadow everything else that is positive about a project. Further, quality testing a data conversion can be problematic because it is impractical to open and review every record and sampling is not very effective. BPro has developed a conversion process that ensures that all data is successfully mapped and accurately transferred into the TotalVote system. BPro ensures a quality delivery of data and images and will affirm the team's confidence in the new system implementation.

BPro is experienced with the data structure of voter registration data and data conversions through our successful delivery of election systems in six states. This includes building the South Dakota and Washington Voter Registration systems, which changed from "bottom-up" to "top-down" models with the implementation of TotalVote. In addition, BPro has built data exchanges for our customers to participate in both ERIC and Cross Check, in order to compare voter registration data with other states.

Our plan for Pennsylvania is to extract as much data as possible from the state repository and then fill in any missing pieces from each of your 67 county databases. Data that may only reside in county systems would include images, signatures, and transactional history. Every data element from the state repository and county databases that will be migrated to TotalVote will be mapped and documented, including values. Some values in legacy systems need to be converted for TotalVote. Also, any data corrections will be documented. Examples would be dates that occur in the future or invalid birthdates. Our conversion process includes a number of data validation techniques, both automated and manual, to ensure all data is transferred correctly.

DOS Resources Needed

BPro recommends that a Database Analyst (DBA) from the DOS Project Team will work directly with BPro's DBA to create processes to extract data and images from the SURE system. BPro proposes that the DOS DBA is added to the project team at Project Initiation in a 70% resourced role and remains with the project until 30 days after the last data or image conversion. Having members from the DOS Project Team is very important as your team knows your data.

Data Extraction and Preparation

Together the DBAs of both teams will create extract, transmit and load procedures (ETL) for moving the data and images to TotalVote. The DBAs will coordinate with the Business Analyst(s) and the Quality Analyst(s) to ensure the processes for conversion deliver a product with data integrity, meeting all quality standards, and created in TotalVote in a manner that is fully consumable into the business process and software logic of the BPro system. The entire process will be scripted and run end-to-end multiple times throughout development.

Data Mapping Rules

The DOS Team will provide a data dictionary of the SURE system data structure and full data extracts. The BPro DBA will work to fully analyze the data sets against the data structure of every field. BPro will document the mapping of data to the TotalVote system and present small trial conversions for verification. Legacy fields that do not have an "exact fit" will be reviewed with the DOS Team to determine the best course. For example: does the field contain data that needs to be used as input to logic on the TotalVote system, and if yes, how must the value in the field be stored in TotalVote?

BPro has special routines to evaluate all the unique code values for all fields that are coded, such as district, precincts, polling places, etc. These fields will usually be evaluated first and confirmed with DOS.

Resources for Data Scrubbing

The BPro DBA may identify outlying data that does not fit the definition of the field and requires "data scrubbing" or cleanup in preparation for conversion. Data scrubbing may be necessary on both the state and county level. These will be logged as conversion tasks. The DOS DBA will manage the tasks associated with data cleanup. These tasks may be handed off to be managed by various members of the DOS team depending on the nature of the problem and who owns the process that manages the data.

Strategies for Final Conversion

With final conversion, the legacy system should remain searchable to be used as a reference for the new TotalVote system conversion. BPro's process does not rely on data sampling to ensure quality data. BPro's conversion process will verify the converted content of all tables by comparing metrics supplied by backend queries against the legacy system.

- When a data set is harvested from Pennsylvania's legacy system for a conversion, the legacy data is retained as a query-able database.
- A series of counting queries are built to evaluate the content for each field. For an example – one query is built to count of the number of records that have the first name beginning with each level of the alphabet, returning an array of the 26 letters and a record count for each. (Another query would count the same for middle name, and another for last name, etc.) These queries are compiled in preparation for testing the conversion.
- BPro performs the conversion and applies the dataset to TotalVote tables.
- Testing the conversion: Inside the TotalVote application, the user searches on first name of "A*" (wildcard) and a count is returned. That count should match the query from the legacy system. This search is repeated for all letters of the alphabet and matched against the original SQL query results. There should be no exceptions that cannot be accounted for.
    - The example is repeated for all text fields. Tests can also be run for the last character in a text string.
    - The same example is used for numeric fields, testing for the first digit, and/or the last digit value, and retrieving value (0-9) counts for each field.
    - Date fields can be counted for months (how many birth dates in May), or counts of the day values, or counts of the year values.

Test Data Migration

Prior to the final data migration, the team will run multiple test migration to identify problems, bottlenecks and to capture metrics at key migration checkpoints. The resulting timing metrics will provide the input for scheduling of the final conversion. It also provides timing statistics necessary for scheduling the conversion. In

addition to being more efficient, BPro's conversion strategy has proven to be more effective in each implementation we have successfully completed.

I. **Voter Registration Model.** The DOS is interested in a top-down model for voter registration. A top-down model involves complete centralization of records and management in the office of the Secretary of State with online, real-time access to the records by each and all the Commonwealth's county election officials. The counties access the centralized system and all county processing is performed directly on the central data base. Department users will have access to all data within each county, but county election officials shall only have access to the data contained within their county and read-only access to data for all other counties depending on their roles and permissions. The proposed solution shall support transaction volume and capacity for Pennsylvania's election model. Please refer to https://www.dos.pa.gov/VotingElections/CandidatesCommittees/RunningforOffice/Documents/current votestats xls for current registration totals by county.

Offeror Response

BPro's TotalVote solution was designed as a centralized statewide top-down system. We believe TotalVote is a perfect fit to replace Pennsylvania's SURE system. In Hawaii, New Mexico, North Dakota, South Dakota and Washington, BPro's TotalVote system is a top-down solution using a centralized statewide database for all modules. All county users with appropriate permissions have access to the data from their county and read-only access to data from the other counties in the state. In Arizona, the TotalVote system is a hybrid solution with a centralized database that is accessed by 13 of Arizona's 15 counties. Arizona's two largest counties chose to retain their legacy voter registration systems and BPro built over 70 interfaces that allow these two counties to access read-only data from the statewide system in real time and provides the other 13 counties real-time, read-only access to data from Pima and Maricopa counties.

J. **General Requirements.** The proposed solution shall meet or exceed but are not limited to the general requirements listed below. The solution shall also meet or exceed requirements listed in **Appendix F, Detailed Requirements.**

The solution shall be nondiscriminatory, single, uniform, official, centralized, and interactive with the following requirements:

1. It shall be multijurisdictional in design and operation.
2. It shall support full integration with DOS business partners.
3. It shall provide operational and analysis reports as well as the ability to develop custom reports without extensive programming or intervention.
4. It shall contain the name and registration information of every legally registered voter, candidates, campaign finance registrants, or lobbying disclosure registrant in the state.
5. It shall serve as the single system for storing and managing the official list of registered voters, candidates, campaign finance filers, or lobbying disclosure filers throughout the state.
6. It shall contain other information deemed necessary by the DOS, and county election officials, for legally registered voters, candidates, campaign finance filers, or lobbying disclosure filers in the state.

7. A unique identifier shall be assigned to each registered voter, candidate, campaign finance filers, and lobbying disclosure filers.
8. It shall contain the full voting history of each registered voter.
9. It shall contain a full history of changes for each registered voter, candidate, campaign finance filers, and lobbying disclosure filers.
10. It shall enable any election official in the state, including county election officials, the ability to obtain immediate electronic access to the information contained in the solution.
11. It shall serve as the official voter registration list for the conduct of all elections.
12. The list shall be maintained so that it is technologically secure.
13. The solution shall include election management capabilities related to the administration of elections to include, but not limited to:
    a) Election setup;
    b) Poll workers;
    c) Ballots and ballot styles;
    d) Polling places;
    e) District management;
    f) Precinct management;
    g) Party management;
    h) Election returns at the statewide, county, or precinct levels;
    i) and related tasks at the state and county levels as applicable.
14. The solution shall support numerous methods of voting such as regular voting, regular absentee, UOCAVA voting, provisional voting, etc.
15. The solution shall be capable of interfacing with external services or databases.
16. The solution shall be capable of receiving electronic information obtained from other government or approved sources.
17. It shall enable the DOS and county election officials to generate reports or queries through the system, with minimal or no vendor assistance or intervention.
18. The solution shall maintain optimum transaction speed and availability regardless of the number of state and county election official users accessing the system.
19. It shall track all user activity within the system. All user activity for individual voters shall be viewable on that voter's record. All user activity throughout the state must be accessible, user-friendly, and exportable by the DOS.
20. It shall allow the DOS to set formatting standards for data fields and data criteria.
21. It shall be capable of incorporating a statewide or county GIS mapping system. It shall also have a GIS interface to allow the DOS or county election officials the ability to incorporate GIS software or data.
22. It shall be capable of generating correspondence letters in multiple formats, communications, information or registration cards, and notices to registrants, voters and election officials.
23. It shall validate and monitor data quality and standards set by the DOS.
24. It shall be capable of DOS configurable statuses and/or tags for application or record processing without Offeror assistance or intervention.
25. It shall be capable of merging records into one record to include the most updated information while maintaining all previous information and history.

26. It shall be capable of DOS configurable deadlines or dates for election, voter registration, campaign finance, or lobbying disclosure management.
27. It shall enable registration information to be electronically entered into the solution.
28. The solution shall support petition filing for candidate nomination with DOS configurable settings and workflow management.
29. The solution shall support workflow management and configuration for all business functions.
30. The solution shall support data exports and reporting capabilities with minimum or no vendor support or intervention.
31. The solution shall support application programming interfaces to support primary business functions.
32. The solution shall support various user roles and permissions to enable access to DOS and county election officials' users to complete respective business functions.

Offeror Response

BPro currently supports TotalVote systems around the country that meet all 32 general requirements listed above "out of the box." Additionally, BPro's TotalVote systems currently meet the vast majority of Detailed System Requirements "out of the box." Every state's election laws and processes are different and it would be nearly impossible to deliver a truly "COTS" election system. BPro has carefully reviewed Appendix F and any customizations have been clearly marked.

BPro's proposal and pricing cover all requirements and customizations that are presented in the RFP. We are committed to delivering this application with every requirement in the RFP as customized to be compliant with Pennsylvania election laws and HAVA, regardless of the effort or hours it will take to do so. While we have developed most of your requirements in one of our other state implementations, the requirements we've marked as customization will require further development to satisfy your needs that have not been implemented elsewhere. We have built customization time into our proposed project schedule.

While the actual amount of effort and hours needed for customization will be determined after the Analysis Phase. All current RFP requirements and their customized implementation as elaborated and documented in the Requirements specification during the analysis phase are covered within the proposed pricing and will be delivered as per the approved specifications at no extra cost.

To meet your desired schedule and to plan for scope changes as part of the Agile process, we have developed a phased implementation approach to deliver TotalVote in multiple phases. The first phase would be a Minimum Viable Product that would be used to successfully run your elections. The following phases would include features and requirements that are not considered necessary to run elections but could improve processing time and performance.

K. Voter Registration Application. The solution shall support and maintain a secure, online voter registration application, which shall be designed to meet Pennsylvania specifications and approval by the DOS. The Offeror shall work with the DOS to develop final acceptance criteria in the proposed solution. The current application can be found at register.votespa.com.

Offeror Response

BPro has recognized through its software sales and successful project implementations that a Commercial-Off-The-Shelf (COTS) voter registration and election management system is an impractical pathway to achieving a satisfied election customer, which is why our TotalVote solution has evolved into a hybrid model, consisting of existing software that supports customization. The majority of our TotalVote technologies have been previously developed and deployed as local and statewide solutions, yet TotalVote remains flexible to meet the needs of each individual jurisdiction's laws, statues, workflows and other best practices.

If selected, BPro will begin the project by determining which of our six current VR deployments best matches Pennsylvania's requirements. The closest system will be used as Pennsylvania's baseline code in order to minimize configurations and customizations. From there, BPro will work closely with DOS to develop a system that meets every requirement in Appendix F.

L. Voter Registration Application Programming Interface (API). The solution shall support and maintain the secure voter registration API developed by the DOS. The API was developed to provide an interface to the Department's online voter registration application in order to increase access to voter registration for third-party organizations or state agencies. The solution must support the current design and schema to support the API once the proposed solution goes live and the Offeror shall mitigate interruptions to third-party organizations in the proposed solution to continue service. The solution must support the ability for third-parties or state agencies to register online with a backend approval process. The solution must also support access management for third-parties or state agencies through multiple environments to develop, test, and implement an API. The Offeror shall work with the DOS to develop final acceptance criteria in the proposed solution. Offeror's may find existing documentation at www.dos.pa.gov/VotingElections/OtherServicesEvents/Pages/PA-Online-Voter-Registration-Web- API---RFC.aspx .

Offeror Response

Pennsylvania's Voter Registration Application Programming Interface is an innovative way to increase access to voter registration and reduce voter record processing times. If selected, BPro will support the Voter Registration API developed by the DOS. BPro built a similar API for Washington's Health Benefit Exchange (HBE). As a public assistance office similar to Pennsylvania's COMPASS, NVRA requires HBE to provide voter registration services. BPro's HBE interface redirects HBE users that want to register to vote to the VoteWA system and prepopulates information collected as part of the HBE process. From there, users can fill out any additional information and submit their voter registration form online. BPro recently deployed a similar process for Arizona's DOL.

M. Voter Registration Third-party Registration Tool (OVRDrive). The Department designed an online voter registration drive tool for organizations that could not financially support development for their own registration drive application. The proposed solution shall provide an online application tool for third party organizations to use for voter registration purposes, which shall be designed by Pennsylvania specifications and approved by the DOS. The online application shall provide the

Department with the ability to manage registrations to access to utilize the tool, data reporting, and the ability to provide a unique landing page for each approved organization. The current application can be found at www.ovrdrive.pa.gov.

Offeror Response

BPro has successfully built real time interfaces in every TotalVote system in deployment and currently supports a similar Voter Registration API in New Mexico, along with interfaces to various state and federal agencies in every state we work with. This includes Arizona, where BPro currently supports over 70 APIs that communicate in real time between the centralized AVID system (used by 13 of 15 Arizona counties) and "bottom-up" systems in Pima and Maricopa counties.

If selected, BPro will provide an online application tool for third party organizations to use for voter registration purposes and support the current online voter registration drive tool developed by the DOS. In our Washington deployment we developed a similar solution that allows organizations to utilize secure APIs to register voters.

N. List Maintenance. The Department's primary list maintenance vendor is the Electronic Registration Information Center (ERIC). Their mission is to help state and local election officials improve the accuracy of their voter rolls, register more eligible citizens to vote, reduce costs, and improve the voting process. Through its membership agreement, ERIC outlines the various reporting requirements of the member states, member states' responsibilities in using and processing ERIC reports/data for list maintenance activities. The Offeror shall adhere to all ERIC reporting requirements to share and process Pennsylvania data for list maintenance. When ERIC returns reports to PA, the proposed solution shall support primary list maintenance activities and deliverables to update voter records, queue and process to voters, and update voter statuses, as needed.

Offeror Response

TotalVote is fully integrated with ERIC to assist elections officials in identifying potential duplicate, interstate voter registrations and alerting those states when a voter registers in a new state. Currently, there are several organizations attempting to connect state voter databases to help eliminate duplicate voter registration records nationwide. Until there is one proven method for verifying voter registrations across all 50 states, TotalVote will continue to exchange data with ERIC or any other reputable organization that our customers request.

When Pennsylvania is ready to conduct list maintenance, TotalVote has the ability to run all registered voters through an automatic sorting process compliant with the NVRA list maintenance standards. It sorts qualified voters and allows counties to easily review and purge their old, inactive records. TotalVote also sorts qualified voters for the confirmation mailing process. TotalVote is integrated with USPS National Change of Address (NCOA) information, so clerks can check the current addresses for their voters receiving confirmation mailings.

Throughout the TotalVote system, correspondence templates are configured and maintained by DOS and county system managers. Correspondence triggers, like those necessary for NVRA, are integrated with the configuration of Voter Activities, including inactive/deleted voters. All TotalVote correspondence templates are fully configurable and allow DOS and county election officials to add Seals, logos and other branding materials. Although TotalVote generates all the notices to be sent, DOS and counties have full control and final approval over all correspondence that is mailed.

Figure 6 - Arizona's Notice Management Tool - County Level View

O. External Reporting and Exchanges. The proposed solution shall comply with the Department's business efforts to exchange data to improve transparency and strengthen business efficiency. Please see **Appendix A, Current State** for more information on some of the exchanges and reports listed below. At a minimum, the Offeror shall support and provide the following exchanges:

1. Election Assistance and Voting Survey. Every two years, the Department is required to provide voter registration, list maintenance, and elections data to the Elections Assistance Commission (EAC). However, the Department would like to implement this report each year for record retention and reporting. The Offeror shall develop an accessible and usable report, with Department approval, to easily export data to adhere to the EAC reporting requirements. This report shall be developed for the Department to generate with no intervention or support from the vendor. More information can be found https://www.eac.gov/research-and-data/datasets-codebooks-and-surveys/.
2. Campaign Finance Transmittal Service. As needed, the Department automatically sends files to a vendor on contract to data entry campaign finance reports that are filed on paper. The Department would like to continue this service and the proposed solution shall adhere to the transmission requirements.
3. Election Night Reporting. The Election Night Returns system provides the counties with a means to upload their returns for state-wide races to the Department. The information is then compiled and presented on the public-facing returns website for public consumption. The proposed solution shall support the Department's election night reporting obligations and provide a secure process for county files as well as a modern public-facing website for election night returns.

4. PA Manual Report. Every two years, the department is required to produce election returns to the PA Manual. The Department would like to develop an accessible and usable report, with Department approval, to easily export required data in the required format with no intervention or support from the vendor.

5. PennDOT Interface and Exchanges. The Department interfaces with the PA Department of Transportation to receive voter registrations via the MotorVoter process. The proposed solution shall support the requirements of the PennDOT exchanges and also support the Department's esignature service and HAVA validation.

6. Department of Health. Every two weeks, the Department of Health sends deceased data to the Department to transmit to county election officials. The Offeror and the proposed solution shall adhere to the reporting requirements to maintain voter records in PA.

7. Campaign Finance Export. The Department generates campaign finance files through a system request, which is then uploaded to a public facing SharePoint site. The Offeror and the proposed solution shall provide an accessible and usable report, with Department approval, to easily export data with no intervention or support from the vendor.

8. Voter Information Project (VIP). Each election, the Department provides data to the Voter Information Project to provide polling place information as an extract for public consumption. The proposed solution shall provide an accessible and usable report, with Department approval, that meets VIP specifications. The Department shall have the ability to generate the extract and send to VIP without vendor intervention or support. More information can be found here: https://www.votinginfoproject.org/about .

Offeror Response

BPro supports similar interfaces in each of the six TotalVote centralized deployments. Based on the unique nature of our hybrid system in Arizona, BPro currently supports over 70 real time interfaces between Maricopa and Pima counties local VR systems and the state's centralized AVID system. Included are specific responses to the individual interfaces referred above:

1. TotalVote simplifies the Election Assistance Commission's EAVS survey by collecting quantitative data pertaining to the National Voter Registration Act, the Uniformed and Overseas Citizens Absentee Voting Act, and other election administration issues, including the counting of provisional ballots and poll worker recruitment. The EAC EAVS Survey is generated from TotalVote in the EAC's specified format with a simple click of a button.
2. If selected, BPro will work with DOS and the third-party data entry vendor to successfully implement the new solution to support existing business practice.
3. BPro will provide valuable assistance streamlining Pennsylvania's Election Night Reporting system to ensure that statewide and multiple jurisdictional elections are reported accurately and efficiently. Similar to Pennsylvania, Oregon counties use multiple versions of multiple vendors tabulation systems. Prior to selecting BPro, state election officials spent unnecessary time on Election Night reformatting data from different sources to provide statewide election results. BPro was selected to standardize the election data from four different vendors and a combined six different election systems. By setting up their elections using BPro's Election Management system and then exporting their balloting data to their tabulation providers, all Oregon counties send results in a similar file format and Election Night Results are automatically reported accurately and quickly. Selecting BPro will streamline the reporting of Pennsylvania's statewide election results.

4. BPro proposes to work closely with DOS to develop the PA Manual Report. BPro has experience developing a variety of tools and reports that are usable and fully accessible, which would ensure the PA Manual Report is available to all Pennsylvanians of all abilities. While different in frequency, the PA Manual Report appears very similar to Washington's Reconciliation Report.
5. BPro currently supports interfaces with DMV/DOT agencies in each of the six TotalVote centralized deployments, including esignature service and HAVA validation. All data is automatically collected for inclusion in the EAVS Survey.
6. BPro currently supports interfaces with HHS agencies in each of the six TotalVote centralized deployments. These regularly scheduled interfaces automatically send potential deceased voter records to each county system, where they are automatically routed into the appropriate user's work queue for processing. Multiple users can work from the "top" of the work queue (first in, first out), or work can be specifically assigned to users. As with all items in the work queue, the system can monitor how long a record has been sitting in a queue and provide statistics for workload oversight.
7. BPro currently provides an identical interface and public facing site for the State of New Mexico.
8. As a longtime Microsoft partner, BPro has provided reports that meet the Voting Information Project specifications since the organization's inception as part of the Pew Charitable Trust. When the organization was founded, Microsoft and Google were its two biggest supporters (besides Pew). The VIP export is built-in to TotalVote and will be included in your solution.

P. Enterprise Licensing. In offering the best value to the DOS, Offerors are encouraged to leverage the Commonwealth's existing resources and license agreements when practical. The agreements may be viewed at: http://www.emarketplace.state.pa.us.

The Offeror shall describe how they are able to meet this requirement and the core requirements listed as follows;

1. Identify components or products that are needed for your solution that may not be available with the Commonwealth's existing license agreements. The Offeror shall clearly describe how any proposed solution components are licensed and explain the proposed licensing model.

Offeror Response

All necessary licensing for TotalVote is already included in our proposal costs and annual support and maintenance. All software licensed or provided by BPro to DOS, including: (a) all Contractor-proprietary software (including interfaces owned by Contractor); (b) all Extensions, interfaces and other software-based deliverables provided by Contractor to DOS; (c) all third party software, including all interfaces, Extensions and custom developments provided by DOS and owned by the applicable third party; (d) all beta, pre-release or pre-generally available release versions of software; and (e) all Enhancements to the software described in the foregoing.

2. The Offeror shall also describe any licensing requirements for both DOS and county election officials.

Offeror Response

TotalVote is licensed statewide to unlimited users for both DOS and counties.

3. The Offeror shall provide draft license in their proposal.

Offeror Response

Contractor will grant DOS and all Pennsylvania counties a non-exclusive, non-transferable, unlimited user, worldwide, multi-site license for the Solution (and sublicense with respect to third party software). No fees will be assessed for the Solution licenses over the duration of this Contract, or during any time period that DOS utilizes Contractor for maintenance and support of the Solution. If DOS discontinues maintenance and support of the Solution through Contractor, DOS and the Pennsylvania Counties will be entitled to maintain Solution licenses, subject to payment of licensing fees.

DOS and Pennsylvania counties, or other municipalities served by DOS, may use the Solution, and transfer and operate software onto different operating systems or different equipment. They may also make as many production and non-production copies of the Solution, software, and documentation as they deem necessary for production and non- production purposes, including testing, disaster recovery, backup, training and education, development, and archiving.

Contractor acknowledges that the intent of the scope of the Solution license is to make DOS' rights to use the Solution as broad as possible and, accordingly, the licensing language shall not be interpreted strictly or narrowly in favor of Contractor. In the event Contractor develops future limitations, qualifications and/or restrictions in how it licenses the Solution to its customers, such future limitations, qualifications and/or restrictions will have no effect on the scope of the license granted herein to DOS and the counties, and Contractor expressly disclaims the right to claim otherwise.

Other than the rights granted herein, no intellectual property rights to the Solution are transferred to DOS under this Contract. DOS will not disassemble, reverse compile, reverse engineer, or otherwise translate the Solution. Upon written request by DOS, Contractor will provide its best efforts to ensure interoperability between computer systems and/or programs.

DOS may provide services to Pennsylvania counties and other tax-supported entity users. DOS, Pennsylvania counties, and other tax-supported entity users may provide services to the public through Solution applications. The Solution may be used in the delivery of these services. Contractor acknowledges that such use of a Solution is permitted and acceptable.

DOS will be and remain the sole and exclusive owner of any non-software-based deliverables, such as designs, configuration outputs, test scripts, test data bases, workflow diagrams and schematics and reports developed by Contractor for or on behalf of DOS. Subject to the further terms of this section, all interfaces and Extensions paid for by DOS and developed by Contractor shall be and remain the sole and exclusive property of DOS.

Contractor acknowledges that DOS is working with a number of third parties to develop, maintain and support various systems and that it may be necessary to implement one or more interfaces between a Solution and such systems. Contractor will cooperate and work with DOS and such third parties to implement and use standard interfaces or develop and implement custom developed interfaces, in accordance with the terms of this, as necessary to allow information to pass from DOS' and/or other agencies' systems to Solution, and vice-versa. Such cooperation may include, among other things, Contractor's attendance at meetings with DOS

personnel and/or third party vendors and making available to DOS and third party vendors the Documentation for interfaces. Contractor will deliver the interfaces identified in the Contract. If Contractor must develop a custom interface, such interface development shall be considered a deliverable. Contractor will provide to DOS the documentation for all interfaces, including record layouts, design documentation, functional specifications, technical specifications, data transformations and data aggregations for each and every interface (both standard interfaces and custom developed interfaces). Contractor will provide documentation for all Enhancements to any interfaces at no additional charge to DOS. After project completion, Contractor will provide to DOS documentation for interface Enhancements as part of its maintenance and support service obligations.

Contractor will grant DOS a royalty-free license or provide access during the term of the Agreement to all Contractor-owned utilities and tools used by Contractor to provide services and/or in connection with the Solution, and, to the extent such licenses are sub-licensable by Contractor to DOS, a license to third party-owned utilities and tools used by Contractor to provide services and/or in connection with the Solution, including all tools and utilities used by Contractor to provide project management, implementation, evaluation and operational, maintenance and support services, and all tools and utilities used by Contractor to provide performance monitoring, testing, managing and support of the Solution (collectively, "Contractor Tools and Utilities"), which Contractor Tools and Utilities may be set forth in a project document. If Contractor has omitted any tools and utilities described above, such tools and utilities shall nonetheless be Contractor Tools and Utilities, the parties promptly shall update the appropriate documentation to reflect such omitted tools and utilities, and Contractor shall provide such tools and utilities to DOS in accordance with the above terms. If there are tools and utilities introduced in the future by Contractor then such tools and utilities shall be Contractor Tools and Utilities and Contractor shall make such tools and utilities available to DOS in accordance with and subject to the terms set forth in this section. During the pendency of a project, Contractor will provide training and education on the use of Contractor Tools and Utilities. For so long as the Agreement is not terminated and Contractor is providing maintenance and support services to DOS, Contractor will provide updated versions and/or all new Contractor Tools and Utilities as such updated versions are available, all at no additional cost to DOS.

4. Identify and explain any components that are missing from the Commonwealth's existing license agreements.
Offeror Response

At this time, BPro has not identified any missing components from the Commonwealth's existing license agreements.

5. If the Offeror can provide a more cost-effective licensing agreements, please explain in detail the agreement and how it would benefit the DOS and the Commonwealth.
Offeror Response

BPro always strives to provide the most cost-effective system, which includes all licensing agreements. Knowing that state and local election officials have limited budgets and a duty to provide ever expanding voter services, the entire TotalVote system, including all necessary licensing agreements, was built to be both effective and efficient.

6. Explain the ownership, transportability and transferability of the proposed license agreements. Any licenses or warranties purchased on behalf of the DOS for this project must be transferable at the time the Offeror is paid under contract for said component.
Offeror Response

Detailed above in #3

Q. Replacement of Personnel. The Offeror shall not divert or replace personnel without written approval of the Department and in accordance with the following procedures, after personnel have been assigned an approved.

1. The selected Offeror must provide notice of proposed diversion or replacement of key personnel to the Commonwealth Project Manager at least forty-five (45) calendar days in advance and provide the name, qualifications and background check of the person who will replace the diverted or removed staff. DOS will notify the selected Offeror within 10 calendar days of the diversion notice whether the proposed diversion is acceptable and if the replacement is approved. Replacement of all other personnel must be submitted 10 days prior to the replacement or substitution. DOS reserves the right to conduct a meeting with the proposed replacement prior to approval.
Offeror Response

BPro will provide notice of proposed replacement of non-key personnel to the DOS at least 45 calendar days in advance, along with the name, qualifications and background check of the person who will replace the diverted or removed staff.

2. The selected Offeror must provide notice of proposed diversion or replacement of non-key personnel to the DOS at least 14 calendar days in advance.
Offeror Response

BPro will provide notice of proposed replacement of non-key personnel to the DOS at least 14 calendar days in advance.

3. The selected Offeror may not replace its project managers for the duration of the Contract without DOS approval. If the project manager leaves the selected Offeror's employment, then the replacement must be approved by DOS.
Offeror Response

BPro will not replace its Project Manager without DOS approval.

4. The selected Offeror must provide a minimum of 45 calendar days overlap to the Commonwealth for replacement of key personnel.
Offeror Response

BPro will provide a minimum of 45 calendar days overlap to the Commonwealth for replacement of key personnel.

5. Advance notification and employee overlap is not required for changes in key personnel due to resignations, death, disability, dismissal for cause, dismissal as a result of termination of a subcontract, or any other cause that is beyond the control of the selected Offeror or its subcontractor. However, the replacement staff must meet Commonwealth approval and the same documentation as provided for the original staff must be provided. Replacement of key personnel whose availability changes for reasons beyond the control of the selected Offeror must occur 1) on a temporary basis within one week of the availability change and 2) on a permanent basis no longer than 30 calendar days from the availability change.
Offeror Response

BPro will ensure replacement staff receive Commonwealth approval and provide the same documentation as provided for the original staff.

6. In the event that the Offeror's personnel must be replaced, the newly proposed personnel must possess equal or greater experience and skills and must have a background check as described in **Appendix G, IT Contract Terms and Conditions**.
Offeror Response

Any replacement staff will have equal or greater experience and skills and will be submitted for a background check.

7. No more than five percent (5%) of the key personnel, and no more than twenty percent (20%) of the overall Offeror staff assigned to this project, may be substituted per year unless approved by DOS. The project must not incur any delays due to knowledge transfer related to replacement or substitution of Offeror personnel.
Offeror Response

Unless approved by DOS, no more than 5% of the key personnel, and no more than 20% of the overall BPro staff assigned to this project will be substituted per year.

8. DOS may request that the selected Offeror remove one or more of its staff persons from the project at any time. If a staff person is removed from the project, the selected Offeror will have 10 days to fill the vacancy with a staff person acceptable in terms of experience and skills, subject to DOS approval.
Offeror Response

If DOS requests that a team member is removed from the project, BPro will fill the vacancy in 10 days or less.

R. Staffing. The selected Offeror shall provide the necessary level of staff and skill to conduct all activities established in the RFP in order to meet all requirements and tasks. The Commonwealth reserves the right to accept or reject the proposed team. The Offeror shall staff adequately to ensure deliverables are delivered on-time and service level agreements are met as defined in **Appendix H, Service Level Agreements Vendor Hosted**. The selected Offeror shall ensure adequate levels of staffing throughout the life of the contract. The Commonwealth at its own discretion shall require the Offeror's staff to be on-site, particularly during times of testing and deployments. Space can be

provided for approximately 10 persons in the North Office Building located at 401 North Street, Harrisburg, PA**.** DOS shall provide workstation space, laptops, and telephony within its locations. The selected Offeror shall be responsible for annual background checks and badges and shall incur the cost of background checks and employee badges for access to Commonwealth facilities.

S. Background Checks and Facility Access.

1. **Annual Background Checks.** In accordance with Section 29, Background Checks, of the IT Contract Terms and Conditions, the selected Offeror, at its sole expense, arrange for an annual background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Commonwealth facilities, either through on-site access or through remote access. Also, please describe your organization's vetting process and process for background checks and security training of those who will be working on the contract. Individuals working under this contract must have the same, or at a minimum, equivalent background screening and IT security training as government employees.

Offeror Response

Every BPro employee assigned to this project will undergo an annual background check by Pennsylvania State Police. This will be in addition to the South Dakota Department of Safety background check that every BPro employee is required to undergo.

BPro employees receive security training using an internal training curriculum of videos, handouts and test materials. Security training topics include: Cybersecurity Awareness, Phishing, Spear Phishing, Malware, Business Email Compromise (BEC) and Insider Threats.

In addition to background checks and internal security training, BPro utilizes a variety of federal government security resources, including the following:

DHS – NICCS - NICE Cybersecurity Workforce Framework
https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

DHS - Cyber + Infrastructure - Insider Threat - Training & Awareness
https://www.dhs.gov/cisa/training-awareness

NIST - Computer Security Resource Center
https://csrc.nist.gov/publications/search?requestSeriesList=1&requestStatusList=1,3&requestDisplayOption=brief&requestPubNumber=800-&requestSortOrder=5&itemsPerPage=All

National Security Agency / Central Security Service - Cybersecurity Advisories & Technical Guidance
https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/smdpage11246/5/

2. **Facility Access.** Access to certain Capitol Complex buildings and other state office buildings is controlled by means of card readers and secured visitors' entrances. Commonwealth contracted personnel who have regular and routine business in Commonwealth worksites may be issued a photo identification or access badge subject to the requirements of the applicable Commonwealth Agency and the Department of General Services set forth in Enclosure 3 of Commonwealth Management Directive 625.10 Amended, Card Reader and Emergency Response Access to Certain Capitol Complex Buildings and Other State Office Buildings. The requirements, policy and procedures include a processing fee payable by the Licensor for contracted personnel photo identification or access badges.
Offeror Response

By proposing a cloud-hosted solution, BPro does not anticipate requiring regular access to worksites. If it is determined that any BPro employee does require an access badge, we will comply with the requirements of the applicable Commonwealth Agency and the Department of General Services set forth in Enclosure 3 of Commonwealth Management Directive 625.10 Amended.

3. Additionally, the Commonwealth reserves the right to conduct background checks or require security clearances over and above that described herein. See the IT Contract Terms and Conditions, at Section 29, Background Checks, and Section 55, Agency-Specific Sensitive and Confidential Commonwealth Data.
Offeror Response

BPro will submit employees to additional background checks and security clearances as requested by DOS.

T. Project Management. Project management involves planning, organizing and managing resources to bring about the successful completion of specific project goals and objectives. The selected Offeror shall provide project management services throughout the life of the project, which includes implementation and maintenance of the solution throughout its life cycle. These services include, but are not limited to, oversight of Offeror staff delivering and maintaining the work plan, communications plan, requirements management plan, risk management plan, change management plan, final report and lessons learned.

Offeror shall describe the project management methodologies and approach proposed for this project. Offeror shall submit a draft project management plan with its proposal, which must detail major milestones, critical paths, resources, and tentative dates for expected completion. The project management plan shall include, but not be limited to, the items listed in **Section VIII.Tasks/Work Plan.** The Offeror's proposal should also detail their approach to managing the effort to migrate the existing statewide systems and data to the proposed solution. The selected Offeror shall submit a final project management plan within 10 business days of receiving the notice to proceed. All plans are subject to Commonwealth approval.
Offeror Response

BPro has included a draft Project Management Plan as part of this response, which includes all aspects outlined above. If selected, BPro will provide a final project management plan for Commonwealth approval within 10 business days of receiving the notice to proceed.

U. **Public Applications/Sites.** The proposed solution shall support the ability for public users to interact with online services in an efficient, accessible and secure manner. The Offeror shall describe how the solution can support the DOS mission of providing online services to support election administration and disclosure services. The Offeror shall provide, at a minimum, the online applications provided below based on Department specifications. The Offeror shall also describe how the solution's configuration support's the ability to offer future services in addition to current Department offerings. The Offeror shall describe the proposed solutions ability to support language access and accessibility for online application/sites.

Finally, the Offeror and proposed solution shall adhere to **Appendix I, Customer Service Transformation; Design Principles and Requirements**. The current list of online services includes, but are not limited to:

Online applications/sites:

1. Online Voter Registration
2. Voter Registration API
3. Voter Registration 3rd party registration tool
4. Election Returns
5. Campaign Finance Reporting and Filing
6. Lobbying Registration and Filing
7. Voter lookups
8. Polling place lookups
9. Voter Hall of Fame
10. Election complaints
11. Full Voter Export with payment
12. Find application status
13. Provisional ballot searches
14. Online Regular Absentee Applications
15. Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) Ballot Retrieval
16. Petition Filing
17. Campaign Finance Reporting and Filing: Campaign Finance Data Export
18. Lobbying Registration and Filing: Integration with payment services

Offeror Response

BPro currently provides every online application/site listed above for at least one statewide customer, with the exception of a Voter Hall of Fame. BPro will work with DOS to ensure the Voter Hall of Fame is built to meet or exceed the current Voter HOF.

As detailed in Section VI-PP, BPro's policy is to ensure that every system, including those listed above, is fully compliant with WCAG 2.0 and available in multiple languages (where required by law).

When a login is required, BPro will interface with Keystone Login to provide a consistent and secure approach to account administration. To ensure security of public facing systems, BPro utilizes Google's reCAPTCHA to

protect your sites from spam and abuse. It uses advanced risk analysis techniques to tell humans and bots apart.

V. **Prefer Browser-Based Client.** The current system is used remotely via a Citrix client over a private network. The DOS would prefer a secure, browser-based client model which would minimize the complexity of the deployment across the Commonwealth yet accomplish the accessibility and security requirements stated.

Browser-based client shall be compatible with current version of the leading web browsers, such as Edge, Chrome, Firefox, Internet Explorer (legacy) and Safari in non-compatibility mode. Standard browser extensions or add-ons must be specified in the proposed solution.

If the solution relies on a browser plug-in, the Offeror shall state it in their proposal. The Offeror shall comply with all Commonwealth ITPs listed at https://www.oa.pa.gov/Policies/Pages/itp.aspx .

a) ITP-SFT002
b) ITP-SFT006
c) OPD-ACC001A
d) GEN-SEC013B

Offeror Response

TotalVote is a secure, robust, browser-based application that authorized users can access from any current version of leading web browsers (Chrome, Safari, Edge, Firefox, etc.). Because the system is browser-based, authorized users who may need access to the system outside of business hours can use Multifactor Authentication to authenticate themselves from any location. This will allow power-users to access the system remotely without compromising security.

BPro recommends accessing TotalVote through VPN, which is designed specifically providing users secure access to resource residing behind a firewall on a secure network. In addition to the security advantages, utilizing VPN can provide technological advantages, including allowing users to utilize the software natively on their devices. This allows users to utilize locally attached peripherals, such as dual screens, scanners, and printers. Typically, Citrix cannot support dual screen workstations and requires additional configuration to manage drivers for other devices.

W. **Modern, Standards-Based Technology.** The DOS requires the proposed solution to be based on modern and standards-based development and deployment environment. The Offeror shall describe how the proposed solution meets modern technology requirements and the goals of this RFP.

1. Core technology requirements are:
    1. The programing environment should use a widely used programming platform, along with the version numbers, framework and runtime environment.
    2. The preferred database management system is SQLServer.
    3. The application server environment can be deployed to commodity hardware using virtualization and scale out by adding server resources.

4. The database server environment can be deployed to commodity hardware and scale up by adding server resources.
5. The solution should minimize the use of proprietary third-party components within the vendor's product.

2. Third (3rd) Party Requirements:
   1. The Offeror shall identify and explain how the proposed solution and application(s) utilize any 3rd party software or technology. Please also explain how you will work with the 3rd party to resolve any problems.

Offeror Response

TotalVote is a modern, robust, browser-based application developed on the Microsoft .NET Framework platform using Microsoft SQL Server database. TotalVote is a top-down solution using a centralized statewide database for all modules. [redacted]

X. Imaging. The proposed solution shall support the ability to attach, upload, view, manage, interact, or export documentation for voter applications and voter records, campaign finance records, lobbying disclosure records, petition filing, or other business functions stated in the RFP. The DOS does not expect a full-fledged content management capability to maintain these documents, but it does expect a scalable solution that operates seamlessly within the overall system context.

Core imaging requirements include but are not limited to:

1. Capturing images
2. Attaching supporting documentation
3. Retrieving document images
4. Ability to use existing or commonly used scanners

Offeror Response

The document management and scanning utility within TotalVote is used to perform the following functions:

- Create digital images of paper-based correspondence, or other paper-based records;
- Associate the information with the correct records stored in the system.

Paper documents or forms are scanned by a Commercial -Off-The-Shelf (COTS) digital scanner that creates a computer-based digital image of the document for storage in TotalVote. Using information extracted from the image or through manually entered information by an operator, the images are "indexed," meaning the digital images are assigned numerical reference to associate it with a particular voter. Indexing allows the digital image to be stored and accessed from the voter record, which eliminates the need to store or manually retrieve the paper record for reference.

TotalVote's scanning utility is integrated into the voter registration application but accesses local hardware that is connected to the workstation PC. Users must log onto TotalVote and select the Imaging menu item to configure the local scanner that is maintained for future use as part of the user's account on that specific

workstation. TotalVote is a web-based product so the scanning utility is also part of the web-based system and the performance of the utility supports single operator scanning batches. If Pennsylvania has situations that involve larger scale scanning operations, additional licensing of the scanning engine may be required to deploy the scanning utility on a local PC to support higher rate of throughput.

The TotalVote scanning utility creates digital images of paper-based correspondence, or other paper-based records using the following functional modules that are provided by an industry leading Software

- Image capture and image optimization
- Barcode recognition and decoding
- Optical Character Recognition (OCR)

The minimum functionality performed for a paper record is image capture and image optimization where a digital image is created by a COTS digital scanner and passes an electronic rendering of the document in an industry standard file format to the scanning utility. In some cases, the reference data is used to "index" the image with meaningful information for storage and retrieval. In other instances, any documents received from a voter that is a response to a mailing by Pennsylvania will include the Voter Unique ID (VUID) in barcode format that provides the document index.

TotalVote Imaging Functions

BPro's recommended imaging solution starts at opening the mail and sorting the documents into structured and unstructured categories. The structured category contains all the known forms that are used as part of managing the voter registration rolls. This includes automatically recording the NVRA Source information, based off of form data or characteristics. The data and the image together are routed to a work queue where an Elections Staff member verifies the conversion and corrects any low confidence conversions. When the user selects a work item from the work queue list, the image of the document and associated converted data is presented to the user in one screen.

Viewing Attached Images

Registration documents are automatically attached to the voter record. Throughout the *TotalVote* system, an image icon displays with the voter records to indicate that an image is available for viewing. Viewing images attached to records is as simple as clicking on the icon. The image will be launched in a separate window and the user can launch as many image windows as desired. Images can be printed, faxed or emailed. By default, these images have any redaction applied to "white out" sensitive information when sent Internal prints are stored without redaction so all information is shown.

Signature storage

For registration forms, petitions and other signed documents, an image fragment is used for the signature to be excerpted and stored as a separate image that is prominently displayed. For structured forms, the signature area can be automatically framed for separate image storage.

Outgoing Communication

BPro TotalVote retains an image copy of the all outgoing communication as well. For example, an Incomplete registration notice sent to the voter is also stored to pdf, whether the notice was e-mailed or printed and mailed. The image is linked to the Correspondence activity and readily retrievable.

Maps, Electronic Records
Elections materials of all types are stored to image and linked to records throughout the system, including maps, candidate filings, and sample ballots. The objective is to eliminate all paper filing cabinets so that all information going forward is electronically searchable. As described above with records received electronically, these records can be stored as attached electronic documents or formatted images linked to the registration activity.

Y. Data Standards. The proposed solution shall allow the DOS to set formatting standards for each data criteria field to maintain uniformity in the information being entered and gathered by county election officials. Further, it shall be capable of recognizing "bad data" and be capable of disallowing that data from being saved into the system per the formatting standards with complete audit trail of the reason for the disallowed transaction. Additionally, the solution shall be capable of checking for and identifying duplicate information based on matching criteria set by the DOS. It shall also allow the DOS the ability to alter the matching criteria.
Offeror Response

Data flows through each TotalVote module minimize or even eliminate, data entry errors. Voter registration data populates candidate records, which makes up ballot data. The ballot data is used to setup election returns, results, and canvassing, all without any user input. Innovative features are documented throughout our proposal and we will continuously improve and create, even after TotalVote is in production.

TotalVote has been tested and proven to reduce the number of duplicate voter registration records by checking for existing voters when records are updated or added plus as part of a nightly process. The resulting possible duplicates from this nightly process are shown in the home queue to be administered. The simplicity of the TotalVote system allows users to spend more time eliminating duplicate records and less time setting up searches for possible duplicates.

Using TotalVote, incoming records do not need to be screened to determine whether the record is a new voter record or an existing voter record. If the record has been received electronically, then the data needed to search for a duplicate does not need to be manually entered by the user. Identifying information can be used to attempt a match of the records using combinations of fields. The matching rules applied are defined by your system management and can be changed over time. These fields can include:

- Name (parsed components)
- Date of Birth
- Social Security Number (or SSN4)
- Driver's license number
- Unique Voter Identifier

Matching on these information parameters constitute a "hard match", meaning there is a very low possibility that the new record is for somebody different. TotalVote also supports "soft matches", where only some of the parameters match, like partial name and date of birth. "Soft matches" are helpful in identifying voters who may have had a name change.

Z. Geographic Information. The selected Offeror shall provide a solution that can integrate and apply geographic information to business functions outlined in this RFP to support DOS and county election official's data sources. The solution shall be able to integrate with geographic information systems (GIS) to design, capture, store, manipulate, analyze, manage, and present spatial or geographic data. The solution shall also allow DOS and county election officials to analyze spatial information, edit maps or geo-enabled data, and present the results of spatial data. The proposed solution shall also be able to support external services or data exchanges, such as web services, to support spatially enabled data. The Offeror shall describe how the proposed solution can meet GIS requirements of the RFP, including but not limited to the following;

1. The solution shall integrate with GIS technologies and assist DOS and county election officials with election management and administration.
Offeror Response

REDACTED

2. The proposed solution shall manage voter addresses by requiring the entry of a physical residential address and validating whether: 1) the GIS-based address point is valid in the county process the application; 2) the GIS-based address point needs to be added to the county address database; 3) the GIS-based address point is valid in another Pennsylvania county; 4) the address is an out-of-state address; or 5) the address is invalid, incomplete, or cannot be recognized.
Offeror Response

REDACTED

1) the GIS-based address point is valid in the county process the application;

REDACTED

2) the GIS-based address point needs to be added to the county address database;

REDACTED

3) the GIS-based address point is valid in another Pennsylvania county;

REDACTED

4) the address is an out-of-state address; or

REDACTED

5) the address is invalid, incomplete, or cannot be recognized.

REDACTED

3. If the address is valid in the county processing the application, the solution must assign the registrant to the proper precinct and electoral districts based on the address point.
Offeror Response

REDACTED

4. The solution shall permit the user to enter an alternative address for the applicant's physical residential address and permit the user to enter an applicant's mailing address if the applicant indicates he does not receive mail at his residential address.
Offeror Response

REDACTED

5. The solution shall also integrate and assist with county redistricting procedures and the management of precincts and election districts. The selected Offeror shall detail how their solution meets this requirement, which technologies or software are in use to meet this requirements, and which technologies or software would be required to maintain this requirement in the proposed solution.
Offeror Response

REDACTED

6. If the proposed solution does not currently use GIS technologies, the Offeror shall detail how it does or does not currently meet this requirement and how it will achieve this requirement going forward.
Offeror Response

REDACTED

AA. Optional Services. The selected Offeror shall provide the following optional services at the sole discretion of DOS.

1. **Call Center Support.** Call center support shall consist of live agent support during core business hours Monday through Friday 8:00 AM to 5:00 PM EST to assist DOS, county election officials and public users with technical assistance. Offeror shall have a mechanism for call center support for non-core hours. In addition, some exception hours occur within some applications. The selected Offeror shall utilize the Commonwealth tools for incident tracking and reporting which is currently Service Now. The Offeror shall provide a toll-free phone number for the Commonwealth, county election officials, and public users to submit issues for technical assistance. The proposed Call Center solution should incorporate various request methods, including phone, chat, email and form submission at a minimum. Call Center Support should be staffed to resolve typical Tier 1 requests at levels of 80% resolution versus escalation. See **Appendix J, Support Hours and Activity**.

   If the Commonwealth elects for call center support and the Prime Contractor is not able to directly provide those services, the Prime Contractor must subcontract with UniqueSource. See **Appendix K, DGS UniqueSource Subcontract Language (FINAL)**

(Pilot).

The proposal must provide multiple tiers of support and must state whether the DOS is assumed to provide tier 1 support.

Offeror Response

BPro proposes the continued use of the toll-free phone number and Automated Call Distributor currently in place at the Department. Through BPro's experience supporting multiple statewide systems, BPro recommends DOS provide tier 1 support. BPro will provide adequate training to ensure DOS call center support staff can address all tier 1 issues independently. Most tier 1 questions are election related and best answered by DOS. Alternatively, tier 1 support could be provided by Unique Source if preferred by DOS. This would likely require training and support of call center staff by both BPro and DOS.

All tier 2 level support will be handled out of BPro's headquarters in South Dakota and performed by our in-house Technical Support Team. This team is co-located with our development and implementation teams. Technical support staff are technically minded individuals who are intimately familiar with TotalVote and elections. When you call, you WILL speak with someone who understands your issue. Our staff will make every effort to solve the reported issue as soon as possible.

Normal hours of operation for BPro's technical support team are Monday through Friday from 8:00 a.m. thru 5:00 p.m. Eastern Time. During election periods, BPro will support extended hours of operation. The exact hours during election times will be mutually agreed upon as part of the contract. During non-election times, additional support hours are also available after 5:00 p.m. or on holidays and weekends via phone/email at additional costs.

BPro currently interfaces with ServiceNow in Washington's VoteWA system deployment.

2. **Automated Testing.** The selected Offeror shall offer an automated testing tool that can streamline the process for the creation, management, execution, and maintenance of DOS test scripts. The automated testing tool must include functional, regression, integration and performance testing functionality. The Commonwealth, at its sole discretion, may leverage this option. Offeror shall describe its ability to perform automated testing.

Offeror Response

As BPro has matured and advanced its development approach, we realize the benefits of incorporating automated testing into the process. While not replacing manual testing, using tools, such as Selenium, greatly enhances our test coverage and execution. Our automated tests assist in preventing the promotion of code that does not pass basic functionality. This helps identify issues prior to user interaction with the software and reduces the need for emergency patches. These automated tests can also be used to stress and load test, simulating numerous transactions occurring in the system. This provides BPro the ability to address negative user interaction with the UI before the user experiences it directly.

To that end, BPro will use automated testing in its development toolkit for this project. As we gain expertise and experience with your processes, we will expand the use and increase the complexity of the tests. The test cases that may be candidates for automated testing include:

- Test cases that are executed repeatedly
- Test cases that are very tedious or difficult to perform manually
- Test cases which are time consuming
- Test cases that identify performance concerns
- Test cases that require staged data

We will consider the following areas when deciding which areas of the application would be suited for test automation:

- Critical features that have high value for the business
- Testing scenarios that run on a large amount of data
- Common functionalities across applications
- Technical feasibility
- Reusable components
- Complexity of test cases
- Ability to use the same test cases for cross browser testing
- Processes that would be used by multiple users at the same time

To start, we'll set a plan that includes all or some of the following components:

- Automation tools selected
- Framework design and its features
- In-Scope and Out-of-scope items of automation
- Automation test bed preparation
- Schedule and Timeline of scripting and execution
- Deliverables of automation testing

3. **Other Offerings of Services of interest to the Department.** The Offeror shall describe other offerings that may be of interest to the Department. Please detail the specifics of those offerings or services and how they meet the objective s of this RFP.

Offeror Response

TotalAddress' functionality can provide additional value to other state agencies.

BB. Solution Hosting. The selected Offeror shall propose a hosting solution that meet the needs of this RFP including those of the hosting requirements as described in **Appendix L, Non-Commonwealth Hosted Requirements**. The Offeror shall detail the network configurations required for a vendor hosted solution. This shall also include recommended bandwidth requirements to support DOS and public use of the solution.

Offeror Response

[redacted]

1. The Offeror shall provide the Department with multiple environments at the primary hosting data center to facilitate testing, training, and production activities.

2. The modification or expansion of the hardware and infrastructure supporting the Department solution shall be the sole responsibility of the Offeror as part of this RFP.

3. The technical architecture shall be designed for resiliency.

4. The Offeror shall perform a performance test of the staging and production environments and shall tune the network and server infrastructure and the connectivity solution to ensure that application performance is compliant with agreed-upon service levels before each rollouts go-live decision point.

5. Additionally, to the extent the Purchase Order or other procurement document's term expires or terminates, and a new Purchase Order or other procurement document has not been issued by the Department, the Offeror shall, upon request by the Department, promptly return all Commonwealth data and comply with the reaming terms of this section as described above.

6. If the Offeror proposes a Cloud-based solution, the solution shall undergo a Commonwealth Cloud use case review. In order to be implemented, the cloud case proposal needs to be approved by the Commonwealth.

Offeror Response

BPro will provide the environments necessary for the Department to facilitate testing, training and production activities for the implementation of the TotalVote solution. BPro will monitor the system and be solely responsible for the modification or expansion of the infrastructure to support DOS. The BPro TotalVote

solution's technical architecture is designed for resiliency. Primary and Secondary locations can be located in different regions (e.g. North Central US and Eastern US). BPro will work with the Department to implement a solution that is in keeping with the Commonwealth's needs. BPro is well versed in performance testing of the TotalVote product. We have performed this testing in multiple state and local jurisdictions. Testing of the UI/UX of the TotalVote website and the database scalability is crucial to a successful implementation. Upon the expiration or termination of the Purchase Order and non-issuance of a new Purchase Order, BPro will return all data belonging to the Commonwealth in the agreed upon format by all parties. [redacted]

CC. Data Hosting. The Offeror must provide information on all data hosting options. All data storage, repositories, transit, processing and hosting must be within continental U.S. borders.

Offeror Response

[redacted]

[redacted]

[redacted] will be set up for emergency purposes.

3. Offeror shall state how the proposed solution supports retention requirements as required by election laws and policies. Please see **Section VI. MM Policies and Standards**.

TotalVote can support any retention requirements as required by election laws and policies. As part of the VoteWA deployment, the WA Data Governance Committee determined the length every record (cancelled registrations, signatures, images, etc.) should be saved and BPro built the retention requirements into the TotalVote software. BPro recommends DOS take a similar approach.

4. Offer shall describe how the proposed solution can support multiple data interfaces and exchanges with state agencies and key stakeholders.
What interface methods are available and documented?
Offeror shall supply this type of documentation with the proposal.

BPro has helped Arizona, Hawaii, New Mexico, North Dakota, South Dakota, and Washington increase the efficiency of their voter registration process by developing interfaces to other federal and state agencies that generate important data for maintaining accurate voter registration rolls. As technologies have advanced and government agencies have replaced their legacy systems with more modern Information Technology architecture, BPro has developed more and more efficient data sharing protocols that enable greater

efficiency for the management of external data. Through our proven experience, BPro has the expertise necessary to take advantage of new state and federal interfaces as new systems continue to become available.

Interfaces are built using a team approach with the team members from Commonwealth of Pennsylvania's DOS and BPro technical resources. BPro uses standard web services to communicate with other entities. This approach provides a secure, well-known, and flexible means of exchanging information. BPro has built interfaces with a wide variety of federal and state-based systems that help verify voter information, create and print ballots, and record and report election results. Listed below are some of the interfaces implemented in TotalVote in various jurisdictions. This list continues to grow as new systems become available.

On the federal/national level, TotalVote currently integrates with:

- USPS and National Change of Address (NCOA) information through Melissa Data
- American Association of Motor Vehicle Administrators (AAMVA) and Social Security Administration (SSA)
- Electronic Registration Information Center (ERIC)
- Cross Check
- VIP 5.1 Specification

On the state and county level, TotalVote integrates with:

- Point addressing and district data
- Department of Health/Vital Records (Deaths)
- Department of Corrections
- Department of Motor Vehicles
- Statewide Voter Records
- Online Voter Registration
- Ballot Printers and Tabulators

All current TotalVote interfaces are property of BPro's customers and are considered proprietary and confidential. As such, BPro cannot provide interface documentation. If selected and a contract is signed, BPro will provide DOS documentation for all interfaces, including record layouts, design documentation, functional specifications, technical specifications, data transformations and data aggregations for every interface (both standard interfaces and custom developed interfaces).

5. Offeror shall describe how the proposed data hosting solution can demonstrate compliance to policies and procedures for protecting commonwealth electronic data, specifically as identified in Commonwealth IT policies ITP- SEC019, SEC020, SEC031 and any related IT policies.

The TotalVote Voter Registration module is not only a statewide voter registration list, but a full voter administration package. The system includes several confidential fields, including driver license numbers, dates of birth, partial social security numbers, along with information about confidential voters. Providing functionality and security for the system is a high priority. The data stored in the TotalVote Voter Registration module is private and BPro takes multiple precautionary security measures to ensure data safety.

Data encryption will be employed to ensure that voter registration data is secure while being stored in the database, manipulated as a part of a function, or in transit from one function to another to ensure that only authorized functions, procedures, or users can gain access to that data. Input checks and validations will be performed at all ingress points into the application whether through direct input received from the web front-end interface or through transfers from function to function or component to component to ensure that no malicious code can infiltrate the system in any way through application ingress points.

These coding practices, coupled with the following five-part approach to implementing and managing the information security architecture for the system, will provide the most effective and efficient level of protection and the highest level of risk mitigation.

This five-part approach is comprised of the following:

1. Vulnerability Management and Remediation
2. Event Monitoring
3. Privilege Management & Auditing
4. Computer Incident Handling
5. Security Architecture Design & Implementation

If selected, BPro will ensure compliance with Commonwealth IT policies ITP- SEC019, SEC020, SEC031 and any related IT policies. BPro complies with similar policies in every other state that uses the TotalVote system.

6. The Department may request at any time a complete copy of the Commonwealth data associated to the solution in a format acceptable to the Commonwealth.

BPro will provide a complete copy of the Commonwealth data associated to the solution at the request of the Commonwealth.

7. The Offeror shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Storage of backup media offsite is required. The data retention period for data storage will be 12 months. Stored media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

[redacted]

8. The Offeror shall provide backups to include, but not limited to, device configurations, system configurations, applications configurations, user accounts, user permissions, application data, CRM records, images, and documents within the application. This shall

include a full backup once per week, incremental backups every night and hourly transaction log backups.

[redacted]

Point in Time Restore is designed to recover a database to a specific point in time within the backup retention period supported by the service tier of the database. Restoring creates a new database with the same service tier that was in use at the chosen restore point and the lowest performance level supported by that tier.

[redacted]

9. The Offeror shall provide an off-site archival solution in accordance with the following schedule:
   Weekly full back ups for the last 6 months; and
   Monthly full back ups for the last 12 months; and
   Annual full back ups for the last 3 years

[redacted]

10. All backup data and media shall also be tested on a regular basis. The backup test results shall also be provided to the Commonwealth after each test. A mutually agreed upon process and reporting approach will be decided between the Commonwealth and the Offeror. Periodic restoration processes should be also documented and verified via testing with the Department.

A backup is only as good as its restorability. BPro provides regular restores for testing backups of all TotalVote system data. BPro's process to validate backups is to create a full set of backup data from the Production environment and restore the data to the Test environment. In addition to testing the restorability of your data, this ensures that data in the Test environment is up to date, which can benefit other testing procedures that occur in the Test environment. If selected, BPro will work with Pennsylvania to determine how often backups are created and tested.

11. All archival and restoration processes, tools and resources must support and perform to the associated Service Level Agreements as stated in this RFP.

If selected, BPro will work with Pennsylvania to create mutually agreed upon Service Level Agreements.

12. All Commonwealth data must be stored within continental United States.

All data will be hosted within the continental United States.

Offeror Response

Please see above for individual responses to questions 1-12 above.

DD. Solution Requirements. It is the DOS's goal for the entire solution to work seamlessly for every user as well as achieve requirements with minimal customizations for business needs outlined in this RFP and in **Appendix F, Detailed Requirements**. Any proposed customizations or modifications shall not limit the Commonwealth's ability to utilize core product upgrades. As much as possible, the use of product interfaces and/or extensions should be used to address requirements not met by the core product. The selected Offeror shall review the requirements documents and identify where the proposed solution aligns with the requirements. The DOS reserves the right to change any of the responses provided by the Offeror if they determine the Bidder selected an incorrect response code.

1. The proposed solution shall meet or exceed the requirements as defined in **Appendix F, Detailed Requirements**. A functional requirements matrix must be submitted with this RFP in Microsoft excel. For each requirement, please list a response code of F/P/N. The response codes and definitions are listed below.

For each requirement listed in **Appendix F, Detailed Requirements**, the Offeror will indicate "whether" the proposed solution aligns with the requirement.

Response Code: "Whether"	Definition:
F – Fully met	Requirement will be fully and completely met
P – Partially met	Requirement will be partially met
N – Not met	Requirement will not be met

For each requirement with a response code of F/P/N (above), the Offeror will select one of the following response codes which specifies "How" the requirement will be satisfied.

Response Code: "How"	Definition:
O – Out of the box	Requirement can be met out-of-the-box without additional development in Offeror's proposed solution. Functionality is available via configuration or preferences or settings available in Offeror's proposed solution is considered out-of-the-box.
I - Integrated	Requirement met with a partner/subcontractor product which has been fully and seamlessly integrated with Offeror's proposed solution.
T – Third Party	Requirement met through integration with 3rd party software product, defined here as an open source or publicly available product over which

	Offeror has limited or no control. For example, Melissa data would qualify as a third party in this example.
E – Extension	Requirement met through additional coding that extends functionality without altering the base code.
C – Customization	Requirement will be met via customization, development, or enhancement of base/source code and/or components.

The Offeror shall review and complete the Detailed Requirements document in its entirety.

Offeror Response

BPro has completed ***Appendix F - Detailed Requirements*** in its entirety. Any response marked "Out of the box" has been successfully deployed in at least one of BPro's statewide TotalVote systems. All requirements will be configured to meet Pennsylvania's exact requirements.

2. The Offeror shall describe any additional features, products, or services that may be available to the DOS and county election offices at no additional cost.

Offeror Response

At the request of customers, TotalVote now includes a calendar on the home screen, directly below the Work Queue. Important election events (from multiple elections when applicable) automatically populate on the calendar as elections are created. A fully incorporated calendar allows DOS and county users to visualize upcoming events as they are performing their assigned tasks to support one or more elections, which may overlap.

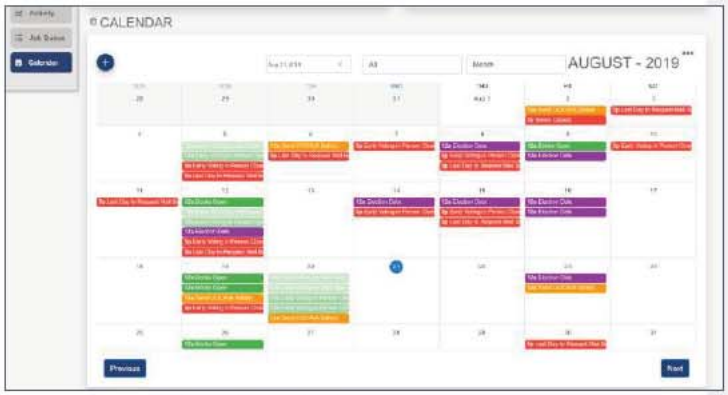


Figure 7 - TotalVote Election Calendar

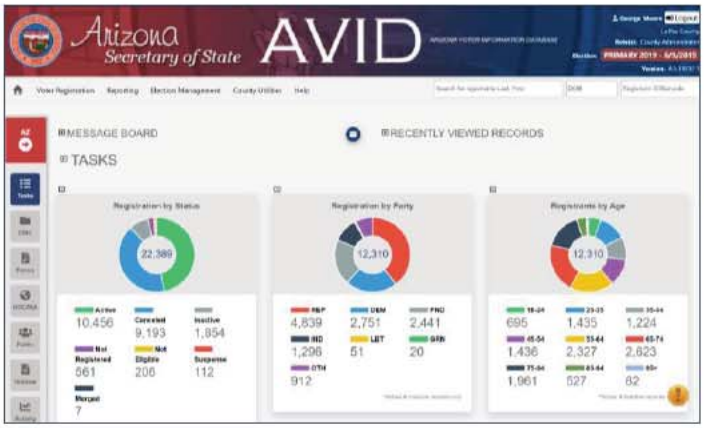


Figure 8 - Realtime Voter Registration Statistics

TotalVote also includes realtime Voter Registration statistics as an option on the homepage. This configurable screen can include statistics by status of registration, registration by party, and registration by age. Quick access to this information can be a valuable asset to DOS and county election officials.

3. The Offeror shall also describe where they do not meet the requirements as defined in **Appendix F, Detailed Requirements**.

Offeror Response

BPro does not meet every requirement out of the box. Many of the requirements marked customization are unique to Pennsylvania and, although we have deployed similar features in other states, will require customization in order to meet Pennsylvania's exact requirements. BPro's decade of experience and successful track record demonstrate our ability to deliver your requirements on time and on budget.

4. The Offeror shall outline all settings for administrative users, including super admin users, that are configurable, and which are not, as well as the default status of those settings.

Offeror Response

TotalVote can accommodate both user-based and role-based authorization. Role-based authorization is the preferred approach because of the difficulty of maintaining user-based authorization. This capability will exist in the event that the DOS needs it. A role can have many assigned permissions and permissions can be assigned to one or more roles.

A user may be assigned more than one role. Roles are cumulative, granting a user the sum of permissions assigned to their roles. We will use least-privilege access principles in defining the access associated with each role, which will keep users from seeing data for which they have no functional need.

Our application has multiple user levels that are assigned different levels to access TotalVote functions and data. These levels and capabilities are defined through the use of user permissions and roles. Granted permissions allow, or prohibit, users from viewing, entering and editing data as well as other actions available in TotalVote. Roles are grouping of functions that users are given permission to access. This construct allows the user community to be tailored and modified as appropriate.

Figure 9 - Configuring County User Permissions

The access a user is granted consists of a union of the permissions granted to all the roles to which they have been assigned. Therefore, a user has access to the application features relevant to the permissions associated with the roles assigned to the user. Each role can have many assigned permissions and each permission can be assigned to one or more roles. Further, each user may be assigned one or more roles and each role may be assigned to many users.

Roles range from Global System Administration to temporary workers in a county elections office. The Global System Administrator has access to all functions and actions within the system and such permission would only be granted, for example, to the IT department entrusted with system operation and maintenance. A temporary worker can be limited to data entry by being granted access to only the data fields in the voter record.

Role-based authorization is ideal for states with large, urban counties and small, rural counties. In county election offices that serve large populations, users will likely have fewer roles and will handle large volumes of few tasks. For example, Allegheny County likely has one (or more) employee that focuses solely on absentee ballot requests and will be assigned few (if any) other roles. Alternatively, small county election workers handle a variety of tasks throughout their day and will be assigned more roles to reflect the many hats they wear. In Susquehanna County, an election worker likely processes a few absentee requests as one of many tasks they perform on a daily basis.

Below is a list of permissions that can be assigned to a role (from Arizona). All available permissions will be configured to meet DOS requirements and permissions not applicable to Pennsylvania will be removed:

Permission	Description
Add To Race	Allows the user to add a candidate to a race from a voter record.
Advanced Search	Allows access to the Advanced Search menu item.

Advanced Search Log	Allows access to the Advanced Search Log menu item.
Allow Commercial Address	Allows a user to add a voter at an address point marked as "Commercial" in Total Address."
Allow NULL Address	Allows a user to add a voter at an address point marked as "NULL" in TotalAddress.
Allow PMB	Allows a user to add a voter at an address point marked as "PMB" in TotalAddress.
Allow Removal of OLVR	Allows the user to remove an OLVR Registration from the Home Queue. A "Remove" button will appear next to the individual records in this queue.
Ballot Import/Export Options	Allows the menu item "Ballot Import/Export Options" under "Election Management," where the user can specify content for their ballot sorter files.
Ballot Proofing	Allows the menu item "Ballot Proofing" under "Election Management" (shortcuts to ballot-related reports).
Ballot Return	Allows the menu item "Ballot Return" under "Election Management," where the use can mark sent ballots as returned.
Ballot Set Up	Allows the menu item "Ballot Set Up" under "Election Management," where the user has access to adding races, candidates, ballot measures, creating ballot styles, and importing and publishing ballots to the Public Portal.
Ballot Tracking	Allows the menu item "Ballot Tracking" under "Election Management," where the user can access a page to upload a file from their mail house and track ballots.
Candidate Lot Draw Ordering	Allows the menu item "Candidate Lot Draw Ordering," where the user can assign a candidate lot draw order.
Change Election	Allows the menu item "Elections" under "Election Management," where the user can select their election from a list of existing elections.
County Office Information	Allows the menu item "County Office Information" under "County Utilities," where the user can edit contact information for their county.
County Office Information - Edit	This will be removed.
County Options	Allows the menu item "County Options" under "County Utilities," where the user can control content such as the use of italics and bold, county home screen message, and languages supported by your county.
County Order Preference	Allows the menu item "County Order Preference" under "County Utilities," where the user can set their order for how notices appear on their unsent notices home queue, and the order their districts will appear on reports. This is within the "County Settings" permission (below).
County Settings	Allows the menu item "County Settings," with brings up menus for "Order Preferences" (referenced above) and "Tabulation Vendor Select," where the user can designate their tabulation vendor.
Create New Precinct	Allows the button "Create New Precinct" on the "Precinct Splits" page under "County Utilities."
Create New Precinct Split/Combine/Delete/Edit	Allows the button "Create New Precinct Split" on the "Precinct Splits" page under "County Utilities."

Create New Role/Delete Role	Allows "Create New Role" button under "User Roles/Permissions," found under the "County Utilities Menu.
Deceased Records - Insert	Allows "Insert New Deceased Record" button within "Deceased Records Search."
Deceased Records Search	Allows "Deceased Records Search" menu item under "Voter Registration."
Delete Voter Record	Allows a delete button on the voter activity tab of a voter record.
District Assignment	Allows "District Assignment" menu item under "County Utilities."
Districts	Allows "Districts" menu item under "County Utilities."
Early Voting	Not applicable.
Edit Previous State Registration Info	Allows the user to see the "Previous Registration Info" section on a voter record (adding or updating).
Edit Roles for User accounts (County)	Allows the user to edit roles and user accounts from the "User Roles/Permissions" page under "County Utilities."
Election Canvassing	Allows access to the "Election Canvassing" menu item under "Reporting."
Elections	Allows access to the "Elections" menu item under "Election Management."
Export Ballot Styles	Not applicable (done from Ballot Set Up page).
Export EAC Data	Allows access to the menu item "Export EAC Data" under "Reporting" menu.
Export ERIC Data	Not applicable (State permission).
Felony Records - Insert	Allows "Insert New Felony Record" button within "Felony Records Search."
Felony Records Search	Allows "Felony Records Search" menu item under "Voter Registration."
Flag Records	Allows a checkbox for "Flag Record" with a notes field on a voter record. Saving this "Flag" will cause the registration to appear in the home queue under "Flagged Records."
Header Menu	Makes the header menu visible (Home button, various menu drop-downs).
Home Queue	Allows access to the Home Queue.
Impersonate User Role	Allows access to the menu item "Impersonate User Role" under "County Utilities."
Import Deceased File	Allows access to "Deceased File" menu item under "County Utilities"➔"Import File."
Import NCOA File	Allows access to "NCOA File" menu item under "County Utilities"➔"Import File."
Mail-Only Precinct Notice	Not applicable.
Manage precinct splits	Allows user to edit, delete, and combine within the precinct splits page.
Manually Export BOD Files	Not applicable.
Manually Import BOD Files	Not applicable.
Mentally Incapacitated Records - Insert	Allows "Insert New Mentally Incapacitated Record" button within "Mentally Incapacitated Records."

Mentally Incompetent Records Search	Allows "Mentally Incompetent Records Search" menu item under "Voter Registration."
Messages	Allows access to the "Messages" menu item under "County Utilities" where users can see queued email and text messages.
Notice Management	Allows access to "Notice Management" menu item "County Utilities," which allows the user access to the Notice Management tool.
Office/Incumbent Management	Allows access to the "Office/Incumbent Management" menu item under "Election Management."
Online Voter Application	Allows online voter registrations to appear in your home queue.
OPEX Import	Not applicable.
Outbound Ballot Processing	Allows access to "Outbound Ballot Processing" menu item under "Election Management."
Petitions	Allows access to the menu item "Petitions" page within VoteWA (NOT Runbeck Petitions Portal).
Poll Woker Positions - Edit	Not applicable.
Poll Workers	Not applicable.
Polling Place Precincts	Not applicable.
Possible Duplicate Registrants	Allows access to the menu item "Possible Duplicate Registrants" menu item under "Voter Registration."
Post Voting History	Not applicable.
Precinct Splits	Allows access to the menu item "Precinct Splits" under "County Utilities."
Private Data in Advanced Search	Allows user to check or uncheck "Restrict Private Data" button on Advanced Search page.
Process Registrant Registrations - Add/Update	Allows access to "Add Registrant" menu item under "Voter Registration."
Process Returned Notices	Allows access to "Process Returned Notices" menu item under "Voter Registration."
Provisional Ballots - Add/Update	Activates "New Provisional Ballot" button on the Provisional Tab of a voter record.
Provisional Ballots - Delete	Allows the user to delete a provisional record that has been entered on the Provisional Tab of a voter record.
Public Records Requests	Shows "Public Records Requests" home queue item.
Public User - Default Status	On advanced search, a voter can only view active and inactive voters, this status allows all statuses to be viewed.
Public User - Registrant Record View	Restricts Registrant Record view to only public information.
Public User - Search Options	Restricts search options for a public user.
Purge Inactive Voters	Allows access to "Purge Registrants" menu item under "Voter Registration."

Queue item - Absentee Records	Adds a queue item under "Activity" for ballot records that have been created for a specific election.
Queue Item - Attachments Flagged for Removal	Adds a queue item of Attachments Flagged for Removal.
Queue item - Attachments from Other Counties	Adds a queue item for Attachments from Other Counties.
Queue Item - Deceased	Adds a queue item for Deceased (voter records that match with the deceased database).
Queue item - Deceased - Automatic Resolution	Not applicable.
Queue Item - DOL Registrations	Adds a queue item for DOL Registrations.
Queue Item - Failed ID Check	Adds a queue item for Failed ID Check (records that have a "Failed ID" flag on the record).
Queue item - Failed ID Check for Two Federal General Elections	Adds a queue item for Failed ID Check for Two Federal Elections.
Queue item - Felon - Automatic Resolution	Adds a queue item for Felon-Automatic Resolution (pending potential felons unresolved after 30 days).
Queue item - Flagged Records	Adds a queue item for Flagged Records.
Queue item - Forms to be Scanned	Adds a queue item for Forms to be Scanned.
Queue item - In County Possible Duplicates	Adds a queue item for In County Possible Duplicates.
Queue Item - Inactive Two Federal General Elections	Adds a queue item for Inactive Two Federal General Elections.
Queue Item - Mentally Incapacitated Match	Not applicable.
Queue item - Mentally Incompetent - Automatic Resolution	Adds a queue item for Mentally Incompetent Matches.
Queue item - Merges from Other Counties	Adds a queue item for Merges from Other Counties.
Queue item - NCOA	Adds a queue item for NCOA matches.
Queue item - Online EZ Voter Registrations	Not Applicable.
Queue item - Out of County Possible Duplicates	Adds a queue item for Out of County Possible Duplicates.
Queue item - Provisional Ballot Logged by Outside County	Adds a queue item for Provisional Ballot Logged by Outside County.
Queue item - Recently Added Registrants	Adds a queue item for Recently Added Registrants.

Queue item - Recently Updated Registrants	Adds a queue item for Recently Updated Registrants.
Queue item - Registered Voters with no DOB	Adds a queue item for Registered Voters with no DOB.
Queue item - Registered Voters with no Precinct Split	Adds a queue item for Registered Voters with no Precinct Split.
Queue item - Registrants with recently added Attachments	Adds a queue item for Registrants with recently added Attachments.
Queue item - Residence Addresses to Verify	Adds a queue item for Residence Addresses to Verify.
Queue item - Returned Notices to be Scanned	Adds a queue item for Returned Notices to be Scanned.
Queue Item - Review - DL	Not applicable.
Queue Item - Review - SSN	Not applicable.
Queue item - Suspense - Registrant Too Young	Adds queue item for Future Voter – Under 18.
Queue item - Voters Transferred Out of County	Adds a queue item for Voters Transferred Out of County.
Queue item - Voting History from Other Counties	Adds a queue item for Voting History from Other Counties.
Quick Search	Adds the quick search.
Registrant Activity tab	Adds the Registrant Activity tab on voter records.
Registrant Attachments - Delete	Allows the user to delete attachments.
Registrant Record - View	Allows a user to view a record.
Registrant Record Views	Shows registrant record views on voter activity tab.
Registrant Record Views	Duplicate of above.
Registration Date - Edit	Allows the user to edit the original registration date.
Reports	Allows access to the "Report" menu item under Reporting.
Returns Administration (County)	Allows access to the "Returns Administration" menu item under "Election Management."
Returns	Allows access to the "Returns" menu item under "Election Management."
Rosters	Not applicable.
Scan Forms	Allows access to the "Scan Forms" menu item under "Voter Registration."
Schedule Races	Allows access to the "Schedule Races" menu item under "Election Management."
Search for a Registrant Record	Allows access to advanced search.
Signature Update Notice	Not applicable.

Tabulators	Allows access to the "Tabulators" menu item under "Election Management," where the user can export their tabulator vendor file.
TotalAddress	Allows access to the "TotalAddress" menu item.
Transfer Voter	Allows the "Transfer Voter" button on a voter record, including the ability to transfer a voter with an accepted ballot.
Undeliverable Notice Return	Not applicable.
UOCAVA Ballots - Precinct Board Determination	Not applicable.
UOCAVA Voters	Allows access to "UOCVA Voters" menu item under "Voter Registration."
User Roles/Permissions (County)	Allows access to the "User Roles/Permissions" menu item under "County Utilities."
Users	Allows access to the "Users" menu item under "County Utilities."
View Audit Tables	Allows access to the "Audit Tables" menu item under "Reporting."
View State Saved Searches from advanced search	Allows a user to view state saved searched from the Advanced Search page.
Voting History - Delete	Allows a user to delete voter history.
Voting History Export	Not applicable.
Voting Locations	Allows access to the "Voting Locations" menu item under "Election Management."
Voting Locations to Election	Allows access to the "Voting Locations to Election" menu item under "Election Management."

5. The Offeror shall detail the proposed solution's scalability, capacity and performance. Please describe your approach to load balancing and/or clustering for extended scalability, performance, transaction processing and solution architecture to support scalability and performance. The solution must have the capacity to meet usage demands with the flexibility to handle high-volume timeframes and demand.

Offeror Response

[redacted]

6. The Offeror shall describe the programming platform, framework, and environment(s), and how they meet the requirements and objectives of the RFP.

Offeror Response

TotalVote is a modern, robust, browser-based application developed on the Microsoft .NET Framework platform using Microsoft SQL Server database.

7. The Offeror shall describe and explain how their solution is interoperable and meets the requirements and objectives of this RFP.

Offeror Response

Since 2007, BPro has helped Arizona, Hawaii, New Mexico, North Dakota, South Dakota, and Washington increase the efficiency of their TotalVote systems by developing data exchanges to other federal and state agencies. TotalVote has been designed and developed using state-of-the-art software language and an operating system that embraces the era of internet deployment and mobility support. Data sharing is a central feature of this architecture and will

support Pennsylvania's future needs through the use of web services, data standards, and automation. Data flows through each TotalVote module minimize or even eliminate, data entry errors. Voter registration data populates candidate records, which makes up ballot data. The ballot data is used to setup election returns, results, and canvassing, all without any user input. Innovative features are documented throughout our proposal and we will continuously improve and create, even after TotalVote is in production.

TotalVote's Election Management module is used by jurisdictions around the country to setup elections and build ballots before every election. TotalVote customers around the country currently use every Voting System certified in Pennsylvania after January 1, 2018. The simplicity of the TotalVote system allows our customers to easily build their election in the TotalVote Election Management system and seamlessly export ballot data to their tabulation vendor. By avoiding building their ballots twice in two separate systems, TotalVote county users are able to save time and improve the accuracy of their elections. In addition to saving counties time setting up their election, using TotalVote EMS will simplify multijurisdictional election results reporting that may require results from multiple tabulation systems to be added together. By receiving the results in TotalVote, data from multijurisdictional races can be combined automatically and results can be available to the public sooner.

As technologies have advanced and government agencies have replaced their legacy systems with modern Information Technology architecture, BPro has developed more and more efficient data sharing protocols that enable greater efficiency for the management of external data. Through our proven experience, BPro has the expertise necessary to help Pennsylvania support and maintain existing interfaces and to take advantage of new state and federal interfaces as new systems continue to become available.

8. The Offeror shall describe in detail how the proposed solution supports the needs of this RFP and will be reliable and available through the proposed solution's life cycle.

Offeror Response

BPro's track record demonstrates the reliability, availability, and flexibility to meet every customer's requirements throughout the life cycle of the system and beyond. Currently, Hawaii, Nebraska, New Mexico, North Dakota, South Dakota all have statewide TotalVote systems that have extended beyond the initial scope and life cycle of the contract. BPro's ability to enhance systems has provided added benefits and BPro's customers have acknowledged these ongoing benefits by extending BPro's contracts around the country.

9. The Offeror shall describe the usability of the proposed solution of the various user groups that supports the needs of this RFP and election administrators, which includes the Department, county election officials and external users such as the public.

Offeror Response

As a web-based system, TotalVote offers usability improvements before the system is even implemented. Users no longer need a specific thin-client and can login from any device using multifactor authentication. By utilizing a browser-based system, BPro eliminates the need for software and drivers to be loaded on specific devices and constantly monitored for updates.

The familiar, intuitive and consistent interface makes TotalVote easy to learn and easy to train new staff. Using a common web interface, point and click simplicity is provided along with the ability to use keyboard driven operations for the user who is doing “heads down” repetitive work.

TotalVote has fail-safe checks throughout the application to present the user with only what is currently active for an election and give instructive error messages when information is not sufficient to complete processing. Our web interface senses when a user is navigating away from a page and prompts the user when there is updated information that has not been saved to the displayed record.

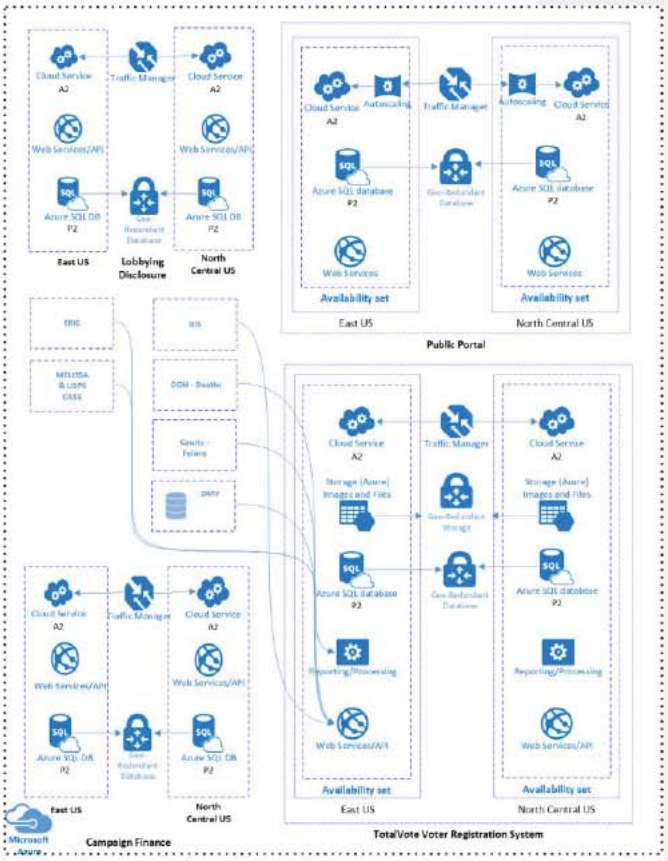
User manuals are available online for quick answers to questions. Help text is available throughout the system and is fully searchable.

All public facing portions of the system are fully accessible (WCAG 2.0) and provide any citizen of any ability with important election information. Additionally, all public facing systems are built with responsive design to allow users to access the system from any web-enabled computer, tablet or phone.

10. The Offeror shall provide an architectural diagram of the solution with descriptions of the solutions scalability. This should include the entire solution, including all proposed interfaces and endpoints.

Offeror Response

[redacted]



11. The Offeror shall describe whether the solution software or supported technology can be installed and configured by only the respondent. The response should clearly state the reasons why that is the case.

Offeror Response

TotalVote is a proprietary system, built and owned by BPro, Inc. Only BPro has ability to install and configure the system to meet the unique needs of state and county election officials around the country. For over 10 years, BPro has successfully proven our ability to configure the TotalVote system to comply with federal and state election laws and meet the requirements of our customers.

12. The proposed solution shall provide a module for defining and assigning roles and permissions to users based on tasks to be performed in functional areas.

Offeror Response

The proposed application has multiple user levels that are assigned different levels to access TotalVote functions and data. These levels and capabilities are defined through the use of user permissions and roles. Granted permissions allow, or prohibit, users from viewing, entering and editing data as well as other actions available in TotalVote. Roles are grouping of functions that users are given permission to access. This construct allows the user community to be tailored and modified as appropriate.

The access a user is granted consists of a union of the permissions granted to all the roles to which they have been assigned. Therefore, a user has access to the application features relevant to the permissions associated with the roles assigned to the user. Each role can have many assigned permissions and each permission can be assigned to one or more roles. Further, each user may be assigned one or more roles and each role may be assigned to many users.

Permissions range from Global System Administration to temporary data entry clerks in county offices. The Global System Administrator access to all functions and actions within the system and such permission would only be granted, for example, to the IT department entrusted with system operation and maintenance. A temporary data entry clerk in a particular county can be limited to data entry by be granted access to only the data fields in the voter record.

13. The proposed solution shall employ a robust audit logging strategy and must include logs to aid in performance and compliance monitoring and evaluation of security incidents. The solution shall have data audit trails that permits reconstruction of the original activity. Offeror shall describe the proposed solutions audit logging capability and demonstrate how the audit logging compiles to NIST Special Publication (SP) 800-53.

Offeror Response

[redacted]

In addition, Microsoft has developed an extensible compliance framework that enables it to design and build services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape. This compliance includes the Federal Information Security Management Act (FISMA)

[redacted]

[redacted]

EE. Licensing Requirements. Any click-through terms presented to an individual upon use of any component of the solution must be pre-approved in writing by the Commonwealth Contracting Officer. Such terms may not be inconsistent with the final negotiated contract terms and conditions resulting from this RFP. See **II. Objections and Additions to Standard Contract Terms and Conditions.**

Offeror Response

No click-through pricing is included in this proposal. If DOS ever wanted to send push notifications from the system, outgoing text messages are available. Any click-through pricing would require DOS approval.

FF. Election Administration. The proposed solution shall be capable of providing services for each area listed below as well as requirements listed in **Appendix F, Detailed Requirements**, but these shall not be understood as fully inclusive or final requirements. The selected Offeror shall work with the DOS and county election officials to fully define requirements to meet the needs of the RFP. Offeror shall describe its solutions capabilities for the following:

1. Voter Registration; The proposed solution should provide an efficient product for the management of a statewide, uniform voter registration database and functionality related to such in accordance with state and federal law.

Offeror Response

BPro's TotalVote Voter Registration system is proven to improve the accuracy of voter rolls, eliminate duplicate voter records (both in state and around the country), increase transparency, and help state and county election officials save time. BPro currently provides Voter Registration systems in Arizona, Hawaii, New Mexico, North Dakota, South Dakota, and Washington. Each project is very different, because of unique customer requirements and state laws. BPro is very proud of the systems and relationships we have developed, and we plan to continue our partnerships as each state's needs evolve. We expect to develop a similar relationship with the Pennsylvania Department of State and county election officials and will work with you to tailor the steps to a successful implementation that's the best fit for your needs and requirements.

Through our successful Voter Registration system deployments in six states, BPro meets the vast majority of the requirements out of the box and has deployed most features in multiple election cycles. Our experience will allow BPro to provide valuable input throughout the development and deployment process. BPro's expertise has come from constantly looking at ways to improve its business value delivery, adopting new technology or processes as are relevant, and embracing the opportunity with each new project to learn from our customers as well. We envision a similar relationship in Pennsylvania that extends well beyond the initial scope of the project.

2. Elections Management; The proposed solution should provide for efficient and transparent end-to-end management of election functions, including candidate filing, candidate list certification, absentee balloting, polling place and poll worker management, election equipment inventory, and official and unofficial election returns.
Offeror Response

TotalVote's EMS module is an intuitive, user-friendly system that is used by states and counties around the country to set up every aspect of an election. The Election Management module is currently used in nine statewide deployments (BPro's six VR deployments, plus Montana, Nebraska and Oregon). Many jurisdictions have made the switch from using the EMS system provided by their tabulation vendor and now use TotalVote EMS as their primary system for setting up elections. This is possible because TotalVote EMS is compatible with all major tabulation systems (including all systems currently certified in Pennsylvania) and exports from TotalVote do not need to be manipulated before being exported to the tabulation vendor's system.

In TotalVote, DOS can create a statewide election and define the election based on the type of election (primary, general, etc.), races on the ballot, districts, counties, and parties that are included in the election. Once DOS has set up an election, authorized county users can further define local races that are part of a statewide election and manage the local portions of statewide elections. In addition, authorized county users can use TotalVote to create local-only elections and manage every aspect of them.

One of the primary components of the election management module of TotalVote is candidate management. Candidates can register in person or through TotalVote's Voter Information Portal, and as each candidate is certified, information is pulled from the voter registration record and linked to the appropriate contest. The Candidate Table contains all identifying information, including a unique Candidate ID Number.

Once the ballot definition information is entered into the system, TotalVote seamlessly creates every ballot style, automatically, in a single step. A ballot style is created for every precinct part and duplicate ballot styles are combined and connected to all applicable splits. The system includes multiple safeguards for quality assurance by allowing the County to error check

throughout the process. After the necessary ballot styles are determined, TotalVote presents sample ballots for review before releasing it to the printing vendor. TotalVote also indicates the number of ballots necessary for each precinct. Once the accuracy of ballot styles is verified, the file is exported for printing. At that point, sample ballots can be released to the public through the Public Portal.

TotalVote feeds the back-end data for all Public Portal functions. When on the Public Portal, a public user can search for and interact with registration and election data in the TotalVote database. The Public Portal is accessible, easy to navigate, mobile-friendly, and can support multiple languages (currently TotalVote supports five languages, not including English). If a registered voter wants to specifically look up their own personal information, they would need to enter a few identifying factors, such as name, address, or date of birth to access their own record.

TotalVote also includes many processes to track the different types of Absentee voters (including UOCAVA voters) and the different stages of the Absentee process. In preparation for an election, TotalVote will parse out all voter records that are scheduled to be Absentees for the election, which can include both permanent and temporary absentee voters. TotalVote also tracks the type of UOCAVA voters and includes that information on the EAVS report.

TotalVote is also used to manage Polling Places, Poll Workers and Inventory of Equipment for every polling place. Features of TotalVote's Poll Worker management module include recruitment, Election Day assignments and payroll. Inventory can manage election equipment on a countywide basis or to assign equipment to individual polling places.

TotalVote's Election Night Reporting system is compatible with all major tabulation systems and results are updated automatically when a vote tabulator file is uploaded into TotalVote. Web visitors will be able to navigate a map of Pennsylvania and drill down to view results and voter turnout by State, County, Congressional District, Legislative District, Senatorial District, School District, Tax District, and Precinct (if available) from any device. TotalVote also flags possible recounts for any of the reported contests, based on Pennsylvania statutes.

TotalVote's Election Canvassing module is used to provide election canvassing for all statewide and local elections. After the completion of the Election Night Reporting, the TotalVote canvassing module is utilized in the canvassing process at the State and County levels. After provisional ballots are processed, TotalVote automatically provides a canvassing report for the County Canvassing Board. No extra data entry is required because the data is pulled from the previously imported or entered returns data. EMP's canvassing system would include creation and customization of all necessary reports.

TotalVote currently includes several other important Election Management features, including:

- Fully developed interfaces with every major Electronic Poll Book vendor
- Poll worker assignments (including location and responsibilities) and the ability to process poll worker payments.

- Polling place and election technology asset management

TotalVote provides a comprehensive set of parameters to manage all details of any election. During the Analysis and Requirements phase of the project, we expect to identify additional specific parameters needed for Pennsylvania.

3. Campaign Finance; The proposed solution shall increase transparency and accuracy with campaign finance. We are seeking a new solution that streamlines the online entry of data from our customers, receives and posts campaign finance reports online filed by candidates for statewide, legislative and judicial offices, as well as political committees and contributing lobbyists registered in Pennsylvania. Furthermore, a system that approves, rejects, and can amend campaign finance reports. The solution shall also provide an online website to allow users to submit and search reports electronically. The proposed solution should also provide the flexibility and scalability to extend campaign finance processes to county election officials as requested by DOS. Additionally, the proposed solution shall support reconciliation and auditing of campaign finance data. And;

Offeror Response

In North Dakota and South Dakota, TotalVote's Campaign Finance Reporting systems have increased transparency and made it easier for campaigns, political committees and lobbyists to comply with the campaign finance reporting laws in each state. All reports are filed online and can be reviewed and either approved or rejected by state and county users. Once reports are filed, they are searchable by any citizen, ensuring this important information is available.

County elected positions that require campaign finance reporting can be added to the system as enhancements. This feature is currently built but not deployed in either North Dakota or South Dakota.

4. Lobbying Disclosure. The proposed solution shall increase transparency and accuracy with Lobbying Disclosure. We are seeking a new solution that streamlines the online entry of data from our customers, receives and posts online reports filed by registered lobbyists and lobbying organizations in Pennsylvania. Furthermore, able to keep historical data related addresses and information from each filer. The solution shall also provide an online website to allow users to submit and search reports electronically.

Offeror Response

Similarly to BPro's Campaign Finance Reporting systems, TotalVote's Lobbying Disclosure system has increased transparency in South Dakota. Although this system has not been used as widely as other BPro systems, our referrals will provide detailed evidence about how BPro's

Lobbyist Disclosure system has increased transparency of the funding of elections in South Dakota. Users can file online, and these filings can be searched by any member of the public.

GG.Solution Support.

1. **Hours of Support.** The selected Offeror shall provide support for the DOS, county election officials, and key business partners during core business hours Monday through Friday 8:00 AM to 5:00 PM Eastern Time (EDT or EST as applicable) and evenings and weekends as requested. Support shall include, but not be limited to, assistance and ongoing support regarding problems/issues, release support, and identification and correction of possible data or system errors. The selected Offeror shall also provide elevated levels of support as requested by the DOS to support critical deadlines and election duties. The selected Offeror shall describe how it will support the operations during core business hours and during critical election periods listed in **Appendix J, Support Hours and Activity.**

Offeror Response

Normal hours of operation for BPro's technical support team are Monday through Friday from 8:00 a.m. thru 5:00 p.m. Eastern Time. During election periods, BPro will support extended hours of operation. The exact hours during election times will be mutually agreed upon as part of the contract. During non-election times, additional support hours are also available after 5:00 p.m. or on holidays and weekends via phone/email at additional costs.

2. **Types of Support.** The Offeror shall describe all types and levels of support available (i.e. telephone, web chat, email) to the Department and county election officials. Responses should discuss technical services and help desk services available to the state and counties during the implementation phase of the project as well as services available during the maintenance and support of the solution. At a minimum, email and phone support shall be provided. If selected by DOS, the selected Offeror shall support services for application assistance, technical support, application maintenance, application research, incident management, testing and development for bug fixes and/or enhancements. The selected Offeror shall also maintain support statistics on help request volume, resolution, and response time, and provide reports to the DOS upon request. The format and design of the report will be mutually agreed upon between the Offeror and the DOS. The Help Desk will contact and inform the DOS of any system changes requested from non-DOS users. All system changes must be reviewed and approved by DOS following the agreed upon procedures in this RFP. The Offeror shall provide support to

the DOS, county election officials, and key business stakeholders. Please reference **Appendix J, Support Hours and Activity**.

Offeror Response

As discussed in AA. above, all tier 2 level support will be handled out of BPro's headquarters in South Dakota and performed by our in-house Technical Support Team. This team is co-located with our development and implementation teams and is able to provide application assistance, technical support, application maintenance, application research, and incident management, along with testing and development for bug fixes. When you call, our staff will make every effort to solve the reported issue as soon as possible.

TotalVote currently collects statistics on help request volume, resolution, and response time. If selected, BPro will work with DOS to develop an interface between ServiceNow and BPro's TFS. BPro has built a similar interface for the VoteWA system.

3. **Incident Management.** The selected Offeror shall provide and manage a process to track, monitor, and resolve problems/issues. Offeror shall describe its methodology to classify incidents as problems as to their criticality and impact, including resolution procedures and escalation process for each classification of problems/issues. Offeror shall describe what incident management tools it has in place to facilitate its solution support. The Commonwealth currently uses Service Now as its incident management solution (ITSM). Offeror shall describe how its incident management tools will integrate with Service Now or the Commonwealth's standard ITSM tool to meet the needs of this RFP.

Offeror Response

In Washington's VoteWA system, BPro currently accommodates Service Now and follows the Issue Escalation Diagram (pictured) in resolving and escalating issues and will respond to issues based on the criticality of the issue. When a problem is reported, a BPro support engineer will work closely with DOS staff to ensure the issue is prioritized correctly according to the following criticality scale:

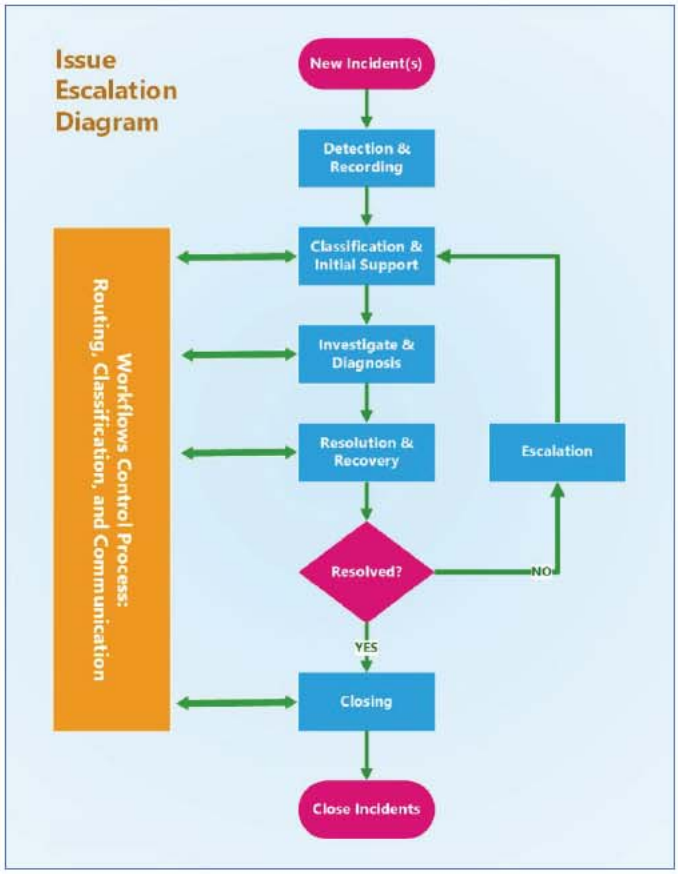


Figure 10 - Issue Escalation Diagram

Criticality 1: The production environment is seriously impacted by some issue or is out of service. There is no work-around available for this criticality status. Team BPro support engineers will use their best judgement to escalate the issue and work on a resolution.

Criticality 2: Production is operable, but a serious issue has occurred. Production is functioning at a sub-standard level. Team BPro support engineers will use their best judgement to escalate the issue and work to find resolution.

Criticality 3: Minor problem or small enhancement request. These issues will be resolved according to the routine build schedule.

The following tables describes BPro's response time goals in responding to issues reported by TotalVote users:

Criticality	Initial Phone Response	Begin Resolution	Expected Status Response Times
Criticality 1	Within the hour	Within the hour	Every hour
Criticality 2	Within 4 hours	Within 8 hours	Once a Day
Criticality 3	Within 8 hours	As prioritized	Once a Week

4. **Notifications.** Offeror shall describe its notification policies and procedures. Offeror shall include policies and procedures of notifications to service subscribers and users in the event of scheduled maintenance, unscheduled maintenance, emergency maintenance, downtime, system errors, degraded performance, or incident management. Offeror shall notify the Commonwealth, and county election officials where applicable, of any solution, data or information breach that occurs immediately upon discovery.

Offeror Response

BPro will notify DOS without unreasonable delay if a data breach is confirmed. In the event the breach affects any DOS data, the notification will include the nature of the breach, the number of records potentially affected, and the specific data potentially affected.

Major and minor upgrades are conducted after-hours and usually require less than one hour of downtime. Any emergency upgrade that requires system downtime during regular business hours is only conducted upon request from designated personnel at DOS and upon communication to the User Group.

HH. Release Management. Release management delivers changes to an organization at optimal cost and minimized risk. It improves consistency in implementation across projects, products, and services within an agency and ensures they meet audit requirements for traceability throughout service transition. Release management focuses on the following objectives:

1. Ensures all releases can be tracked, installed, tested, verified, and backed out if appropriate.
2. Ensures service design packages are completed and updated with release plans throughout the process.
3. Deploys releases following the release plans and agreed upon schedule.
4. Records and manages deviations, risks, and issues related to the changes and takes necessary action.

The selected Offeror shall work with the DOS project manager or designee to provide support and management for releases in accordance with the process defined in **Appendix M, Release Management Process Plan.**

The selected Offeror shall provide functional software upgrades/releases during the life of the contract at no additional cost to the Commonwealth. The solution shall not exceed six (6) schedule releases per year and six (6) additional patches per release. Changes due to legislation shall be included in a standard release without additional cost to the Commonwealth, unless those changes are in size similar or exceed a standard release and are limited by legislative time constraints to deploy. See **Appendix N, Historic Release Information**.

The selected Offeror shall utilize DOS release management process to deploy all changes to the solution in the DOS environments. The selected Offeror shall work with DOS to determine priorities of changes in the next release and which items will move to the backlog for the next scheduled release. The Commonwealth currently uses Microsoft Team Foundation Server (MTFS) as its release management solution. Offeror shall describe how its release management tools will integrate with MTFS or the Commonwealth's standard release management tool. The selected Offeror shall adhere to the deployment methodologies used by DOS as stated in **Appendix O, Current Deployment Methodologies**.

Offeror shall describe its approach to the following;

1. Methodology and processes for updating the solution for all types of releases, including but not limited to, software releases, commonwealth requested enhancements, security updates, system maintenance, patches, and system enhancements;
Offeror Response

All of the situations presented in Question 1 qualify as standard releases. Each standard release and patch is tested and all necessary training and documentation is included.

Types of releases are categorized as follows:

- **Major Release:** Introduces new functionality to the TotalVote software. These are usually numbered before the decimal point. For example, a major release will be numbered 1.0.
- **Minor Release:** A significant improvement to an existing system, many times packaging together several fixes. These are usually numbered after the decimal point of the major release. For example, a minor release to version 2 will be numbered 2.1.
- **Emergency Release:** As the name implies, this is an unplanned fix to a certain function which simply solves a symptom by allowing the developers to fix the problem. These are usually numbered using the standard for minor releases.

Release Numbering Standard

For release management, BPro will use the following numbering system:

- [Major Version].[Minor Version].[Last 2 Digits of Year + Day of Year]. [Build number for that day]
    - Example: 1.3.19098.1

Release Management Planning

Prior to releases of software for unscheduled full releases, upgrades, or hot fixes, a change order form will be submitted by BPro to PA DOS. The change order form is used whenever a

function is changed or new functionality is planned to be introduced. This form is approved by those named to the Change Control Board or the PA DOS Product Owner prior to the release.

The change order form created in TFS will be used to submit the request.

2. Software Development Life Cycle (SDLC) used to implement releases;

The standard software development process at BPro is Agile.

3. how new functions and features are released to clients and a client's ability to control which new features are implemented;

New functions and features are added to the backlog and included as a part of the planning and grooming.

4. whether and how test or staging environments are available to the client;
Offeror Response

A testing or QA environment is available to the client to verify all code prior to implementation in Production.

5. how testing will occur using client data and appropriate configurations;
Offeror Response

Regular backups will be made of production data and provided in the QA environment to provide real-world scenerios for testers. Additionally, scripts may be generate by BPro to 'stage' data (ie Mass Notices, Absentee Requests, etc).

6. processes to support continuation of operational data exchanges (such as list maintenance supporting processes) with other Commonwealth agencies and 3rd parties identified as vetted partners;
Offeror Response

BPro will work with DOS to provide exports via the application interface or through REST APIs.

7. compliance with industry standards and frameworks, such as Information Technology Infrastructure Library (ITIL), the Association for Equipment Management Professional (AEMP) and the Institute of Electrical Electronics Engineers (IEEE), Control Objectives for Information and related Technologies (COBIT); and
Offeror Response

BPro regularly reviews new and updated standards to guide both functional and security development. The items are recorded as a part of BPro's log of future development. Before implementation items are discussed with the client to determine scope and impact of work.

8. describe any duties or involvement of commonwealth and/or county election staff in releases.

Offeror Response

While releases go through automated and staff testing by BPro, DOS should provide staff that can test new functionality and bug fixes in the Sandbox/QA environment to verify they meet acceptance criteria.

II. Reporting. DOS requires a solution with an easy to use and intuitive reporting functionality. The selected Offeror shall meet the reporting requirements defined in **Appendix F, Detailed Requirements**.

1. Offeror shall provide a description of all standard reports available with the proposed solution. It shall also describe whether reports will be static or dynamic in nature.

Offeror Response

TotalVote has developed an extensive collection of preformatted, static reports built into the main product because reporting, especially statistical reporting and voter listings, are essential to the many facets of management of elections. Reports can be exported to Word (rtf), Excel, CSV or printed to PDF format.

TotalVote also includes a variety of "canned" reports including (but are not limited to):

- Voter lists for any combination of status (active, inactive, cancelled) and Election Districts, Precincts.
- Listings and Statistical Reports of Absentee Reports of applications received, and ballots issued and returned
- Statistical Reports of Voters Registered, and Voted, with breakdown of how voted, for any election. This can also be broken down by Precinct or Election Districts.
- Statistical reports and Voter Listings of Voters with specific Activity within a selected date range.
- Summary statistics and detail statistics on work throughput for users and work queues for any date range.
- Summary and detail statistics on Elections measures for a single election by selections of:
    - Elections District
    - Polling Place
    - Precinct
    - Ballot style
    - How voted
    - User

While many of these reports are static in nature, they allow for input parameters, like dates, which make the reports dynamic because the data changes based on the parameters in the search.

2. Offeror shall describe the proposed solution's ability to support the development or assembly of custom reports. Offeror shall describe the level of knowledge, skills, or training required for the user to develop custom reports.

Offeror Response

TotalVote was built to allow users with basic office computer skills to generate custom reports that fit their unique needs for the roles they serve in their office. BPro will provide training on generating reports so DOS and county users can create and save ad hoc reports independently. Users in small and large counties alike will be trained to create, save and recall reports that will save time and allow them to do their job more efficiently.

3. Offeror shall describe the solution's ability to support ad hoc reporting by DOS and county election officials. Offeror shall also describe what level of access and capabilities users will have for ad hoc reporting. The Offeror shall also describe the formats of reports or the reporting functionality.

Offeror Response

TotalVote's Data Generator, or Advanced Search, is used to create searches using one or more fields in the database (name, date of birth, driver's license, SSN, voter unique identifier (VUID), and/or address are some examples) to narrow down Search Results. Searches can also be saved and recalled to run again. In addition, within the application, many of the Search Results grids are exportable to CSV. When the data is exported to CSV, the first sheet of the Excel file created will contain a data dictionary. Parent and child tables can be exported to separate sheets of the Excel file. In this manner, the user can employ a familiar tool to manipulate data and create reports.

4. Sample reports. The Offeror must provide a list of the various reports available from your proposed solution, as well as examples of those reports. At a minimum, provide the first and last page of each report.

Offeror Response

Sample reports from TotalVote systems contain real voter data from other states. This data cannot be included in BPro's RFP response. If selected for an oral presentation, BPro will demonstrate reports and show examples.

5. Exportability. Offeror shall describe the solution's ability to export reports or to export data by DOS and county election officials. The Offeror shall also describe the solution's capability to support standard export formats such as CSV, TXT, XML, etc.

Offeror Response

TotalVote's preformatted, "canned" reports can be saved as CSV, Excel, PDF, RTF and Word files. Ad hoc reports are configured to produce data in CSV format, which provides the greatest flexibility to sort data generated in the report.

6. Standard Reporting. The Offeror shall provide a proposed solution that can integrate with Commonwealth reporting tools. The Commonwealth uses Microsoft Power BI as a common reporting tool. The solution must be able to integrate with Microsoft Power BI and supported reporting services.

Offeror Response

Current BPro customers use Power BI to allow for the collection, integration, analysis, and presentation of voter registration and elections related data. Detailed analysis of this information can be used to support better business decision making and ultimately improve the voter registration and elections processes.

JJ. Solution Maintenance. All standard solution and hardware maintenance shall be completed outside of core business hours, which are defined as 8:00 A.M. to 5:00 P.M. (EST – Eastern Standard Time) Monday through Friday. During primary, general or other election days classified as critical cycle times, the core business hours are 6:00 A.M. to 2:00 A.M. EST or as otherwise requested by the DOS, which may also include weekend hours. The DOS requires the selected Offeror to provide the following in the way of maintenance coverage for the proposed solution regardless of the hosting option:

1. The DOS requires the solution to be capable of integrating with existing Commonwealth systems or systems that may be implemented in the future. The Offeror shall describe the proposed solution's integration capabilities with other disparate systems.

Offeror Response

Data sharing is a central feature of the TotalVote architecture and will support Pennsylvania's future needs through the use of web services, data standards, and automation. BPro utilizes secure REST APIs that are easily integrated by third parties who have been given the necessary access to interact with them. Through our previous deployments, BPro has a deep understanding of the level of effort it takes to interface with other state agency systems, along with an appreciation for the importance of the data these systems can contribute in order to improve voter and election data. part of this effort, below is a partial list of systems BPro will provide interfaces to:

- Pennsylvania Vital Records system
- Pennsylvania Felon Records system
- Pennsylvania Department of Motor Vehicles system
- ES&S, HART, Clear Ballot, and Dominion election systems
- Pennsylvania approved electronic pollbook solutions

- Statewide GIS data
- Third party address verification
    - ERIC, USPS-CASS, Melissa Data, etc.

2. Ongoing software updates for the proposed solution, as they become available and are thoroughly tested; such updates may include, but are not limited to, bug fixes, patches, and other improvements. Offeror shall describe how the updates will be tested prior to updating any DOS environment. When appropriate, testing must also be coordinated and approved with county election officials.

Offeror Response

When an issue is reported, BPro will work with the Product Owner to prioritize and review bugs so that they can be resolved appropriately. BPro will then fix any issues in the development environment and test the fix. Once the fix has been tested BPro will schedule a release with DOS that that it may be released to a Sandbox environment for DOS testing. With approval, the change will be ready for the next scheduled release to the Production Environment. Each software release will be recorded by BPro and provided to the Product Owner as release notes. This will include a release number and an itemized list of fixes included in the update.

System enhancements are included in scheduled releases. Enhancements must be fully specified by DOS and submitted to BPro through the DOS Project Manager before BPro begins development. The development effort will take place in a development environment and, when BPro has completed the enhancements, the enhancements will be posted to the Sandbox environment for QA testing by the BPro QA manager and DOS staff. If necessary, BPro may offer webinar demonstrations of the enhancements to DOS and county elections staff. When the Sandbox code is approved as complete and ready for rollout to production. Each software release will be recorded by BPro and provided to the Product Owner as release notes. This will include a release number and be documented with enhancements included in the update.

3. The selected Offeror must receive DOS approval prior to implementing any hardware or software upgrades/updates in any environment used by the DOS.

Offeror Response

If selected, BPro will receive DOS approval prior to implementing any hardware or software upgrades or updates in any environment used by the DOS.

4. Software updates that modify features and functions shall include an update to online help, training tutorials, reference guides and user manuals.

Offeror Response

BPro provides documentation for system administrators as well as support for end users. End user support, including user manuals and guides, is available within the TotalVote application and accessible through any browser. During M&O, if newly defined requirements result in a brand-new feature or a change to user experience, BPro will update the user manuals and guides to reflect the changes to the system.

KK. Enhancements. DOS may request work to be completed due to legislative or other program changes that may exceed the standard release or time frame. The selected Offeror shall provide enhancements as requested by DOS. The selected Offeror shall create a statement of work for each enhancement to be reviewed and approved by DOS. The selected Offeror shall be responsible for the project management, development, and implementation of system enhancements upon the request of DOS. System enhancements will include the addition of any new feature(s) or function(s) requested by DOS, to the solution after final acceptance. Configuration changes that do not require source code changes will be considered maintenance and support and not an enhancement. Any enhancements that exceed the allotted hours in a year shall be based on the hourly rate as stated in **Appendix P, Cost Submittal**. Legislative changes and mandates shall not be considered enhancements if they are minor in scope (no more than ten (10) percent of the full standard release) and will be considered normal maintenance and support. Enhancement work shall be completed in addition to standard release and operational support without causing disruption to daily activities.

Offeror Response

BPro agrees to provide any additional enhancements at the request of DOS. BPro has similar agreements in place with other TotalVote customers, including those listed as references.

LL. Quality Assurance ("QA") Strategy. The Offeror shall provide a detailed description of the proposed QA methodology adhering to best practices and clearly identifying control tasks and testing required to transition functionality from one environment to the next (e.g. QA to staging and production). The Offeror shall review and complete **Appendix Q, Quality Assurance Strategy** when submitting their proposal. The DOS expects this section to include at a minimum:

1. High level proposed QA approach;
2. Proposed testing and promotion process;
3. Proposed user acceptance process;'
4. Responsibility for each of the above (e.g. Offeror, DOS, County Election Officials, etc.); and
5. Expected Deliverables to adhere to the QA strategy.

Offeror Response

Quality Management will be executed through the inherent Agile Process of product delivery and acceptance. All deliverables must be tested and accepted by the PA DOS.

Delivery of integrated functionality will occur in sprint review testing sessions and formally in the testing events outlined in the Testing Plan.

Prior to any go live, several quality acceptance gates should occur:

- Review of user stories in during the sprint review
- Review of full system in user acceptance testing to ensure gaps are fully identified
- Acceptance of the security measures
    - Security scans on code and environment show no high-level concerns
    - Security standards are met
- Load Testing
    - The ability of the system to support all types of users is verified by PA DOS
- Legal review by PA DOS to ensure PA statutes are satisfied by product

Our talented development team includes individuals that have implemented several elections related applications in numerous jurisdictions. This experience makes development of your SURE replacement product more effective and highly efficient. We focus on building quality applications and code from the beginning rather than testing the finished product to identify and fix the bugs within it. To ensure the quality of code propagation between environments, our team treats deployments as part of a development workflow, not as an afterthought.

MM. Testing Strategy. The Offeror shall describe their proposed test standards and methods used to ensure the proposed solution is working properly during implementation, maintenance of the solution, or enhancements of the solution. The response shall address test plan creation, test case and/or script generation, test phases, the execution of the test plan, and proposed participation by the Department and/or county election officials. The Offeror shall also describe system testing and user acceptance testing (UAT) in their test place approach and whether they will incorporate manual testing, automated testing, or both manual and automated testing. If the Offeror proposes an automated testing tool, please detail the automated testing tools being proposed and any requirements for using those tools. The Offeror is responsible for functional and regression testing to prepare the system for go-live and on-going maintenance and support following implementation in addition to any testing completed by DOS and county election officials.

Offeror Response

Quality control and testing procedures shall be driven by requirements and design and shall adhere to detailed test plans. BPro uses TFS for issue and project tracking. All requirements, including their functionality and design, are tracked in TFS for the development staff. After development work is complete, testing is carried out by both development staff, the QA team, and business analysts (BAs). This testing is based on DOS provided acceptance criteria and includes individual requirement testing, unit tests, and system tests. Upon the success of all testing, the software is ready for release to the PA DOS staff for their sprint review testing. If issues are identified by either the PA DOS Product Owner, BPro will log the issues and the development team will fix them. After issues have been fixed, they can be re-tested through the sprint review process.

Details of the formal testing events of the project will be provided in ***Testing Plan.***

NN. Service Level Agreements (SLA). Offeror shall acknowledge and meet or exceed the level of service as established in **Appendix H, Service Level Agreements Vendor Hosted**. The Offeror shall state its understanding and acceptance of the Service Level Agreements as stated by DOS. The selected Offeror shall provide a status report as described in **Section XII. Reports and Project Controls**.

Offeror Response

BPro has fully reviewed Appendix H. If selected, BPro will commit to developing mutually agreeable Service Level Agreements and will provide status reports as described in Section XII.

OO. Policies and Standards. DOS requires a solution that shall adhere to applicable laws related to voter registration, elections, campaign finance and lobbying disclosure or any additional statutes or regulations that may become law before or during the implementation period. The Offeror shall acknowledge and adhere, but not limited to, all laws as outlined below. The Offeror shall comply with all federal, state, and local policies and regulations.

1. **Federal statutes**
   - The Civil Rights Act, 42 U.S.C. §§ 1971 & 1974
   - The Voting Rights Act, 42 U.S.C. §§ 1973-1973bb-1
   - The Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. §§ 20301–20311
   - The National Voter Registration Act of 1993, 52 U.S.C. §§ 20501–20511
   - The Help America Vote Act, Subchapter III, 52 U.S.C. §§ 20182–21102
   - The Voting Accessibility for the Elderly and Handicapped Act, 42 U.S.C. §§ 1973ff-1973ff-7
2. **State statutes**
   - The Pennsylvania Election Code, Act of June 3, 1937, P.L. 1333, as amended, 25 P.S. §§ 2600–3591
   - The Pennsylvania voter registration law, Part IV of Title 25 of the Consolidated Statutes, 25 Pa. Cons. Stat. §§ 1101–1906
   - The Uniform Military and Overseas Voters Act, Chapter 35 of Title 25 of the Consolidated Statutes, 25 Pa. Cons. Stat. §§ 3501–3519
   - The lobbying disclosure law, Chapter 13A of Title 65 of the Consolidated Statutes, 65 Pa. Cons. Stat. §§ 13A01–13A11
   - The Campaign Finance Reporting Act, 25 P.S. §§ 3241-3260b
3. **State regulations**
   - Elections, Part VIII, Subpart D. of Title 4 of the Pennsylvania Code, 4 Pa. Code §§ 171-182
   - Establishment, Implementation and Administration of the Statewide Uniform Registry Of Electors, Chapter 183 of Title 4 of the Pennsylvania Code, 4 Pa. Code §§ 183.1–183.18

- Lobbying Disclosure, Part III of Title 51 of the Pennsylvania Code, 55 Pa. Code §§ 51.1–69.1
- Redistricting, Part VIII, Subpart F. of Title 4 of the Pennsylvania Code, 4 Pa. Code §§ 191-193.

Offeror Response

BPro's TotalVote system currently complies with all the Federal statutes listed above and complies with similar state laws and regulations from our current statewide customers. If selected. Pennsylvania's TotalVote system will comply with all the statutes and regulations listed above.

PP. Accessibility Needs. The Commonwealth's Executive Order 2016-03, 2016-03 - Establishing "Employment First" Policy and Increasing Competitive Integrated Employment for Pennsylvanians with a Disability, states that Commonwealth employees with disabilities may require accommodations of assistive technology in order to perform the functions of their jobs. DOS will further the objectives of providing appropriate accommodation and support through the contracts resulting from this RFP. Offerors must provide an accessibility and language plan and assistive technology for the products and services of this RFP, as applicable. DOS also requires all electronic and information technology accessible to people with disabilities to be compliant with Section 508 of the Rehabilitation Act of 1973. Additionally, the Offeror shall describe how accessibility testing will be accomplished to ensure the solution is in compliance with Web Content Accessibility Guidelines 2.0 standards, at a minimum. All public-facing portions of the proposed solution must be mobile friendly, meet or exceed WCAG 2.0 and be available in other languages as identified by the DOS.

Offeror Response

BPro has always made accessibility a priority. Between Voter Registration and Election Night Reporting, our systems are valuable to all citizens and should be available to any citizen on any device, regardless of ability. In today's mobile-friendly environment, assistive technologies are no longer cost prohibitive and most phones and tablets feature assistive technologies that allow most people the opportunity to see or hear the information contained in our systems.

BPro is committed to ensuring that its government websites and applications, whether public facing or internal, are accessible to people with disabilities. All the government pages on these websites and applications will meet W3C Web Content Accessibility Guidelines (WCAG), conforming to Level AA conformance of as stated by Federal Section 508.

In order to ensure Section 508 and WCAG 2.0 compliance, BPro follows the following procedures:

Build Accessibility into New Website Development and Major Redesign Efforts

1. Plan for accessibility up front
2. Strategic planning to build accessibility into a website development or redesign project is a key first step. A strategic plan for web accessibility covers many areas beyond actual content development and visual design. A comprehensive plan includes accessibility

considerations for required training, tool selection, quality assurance testing. It is important to start early in order to reduce the risk of making early decisions that become expensive to change or remediate later. The W3C Web Accessibility Initiative (WAI) has published guidance in the document Strategic Planning for Web Accessibility.

3. Integrate accessibility throughout the development lifecycle
4. Accessibility is best approached as an integral and ongoing activity. Integrate accessibility throughout the project from early planning to final deployment.
5. Incorporate both automated and manual accessibility assurance
6. Use a combination of automated scanning and manual testing as an integral part of your overall quality assurance process.

Conduct Website Testing and Remediation

1. Use automated website accessibility scanning tools – BPro uses Webaim (WAVE TOOL) & Lighthouse Audit (Chrome developer tool) at 2 different phases; beginning of design and after completion of all development.
2. Automated website testing tools can 'crawl' through the pages of a website and evaluate certain aspects of accessibility. These tools can be used to provide some indication of the likelihood that the website could pose accessibility problems for users. Automated scanning provides an important first-pass 'screening' that can identify if a website is not accessible or does not comply with accessibility standards by testing for the absence of valid required elements and/or attributes.
3. Conduct manual accessibility tests – This can be done by any number of third-party disability advocates or assigned to client to complete. We have used Lighthouse for the Blind and have proposed testing with the National Federation of the Blind.
4. Manual testing requires a tester to play the role of an end user and use most or all features of the application to help ensure accessibility. The tester must be expert in web accessibility and proficient in the use of input device alternatives and other assistive technologies. It is good practice to include persons with disabilities as testers for manual testing.

QQ. Language Access. The Offeror and the proposed solution shall support the Department's efforts to implement greater accessibility through improved language access to users consuming public-facing resources, notifications, correspondences or other materials or means that may reach a consumer of DOS business services. The Offeror shall recognize that Pennsylvania is a diverse jurisdiction where many consumers rely heavily on languages other than English. The Offeror shall also propose a solution that's flexible and configurable to support multiple languages in state and county jurisdictions for public users and county election officials. Election officials must provide language services once key thresholds are met through demographic data. Please reference https://www.justice.gov/crt/language-minority-citizens for more information.

Offeror Response

TotalVote systems are currently available in five languages (in addition to English) around the country: Spanish, Chinese, Korean, Tagalog and Vietnamese. Customers provide translations and BPro provides a system that is flexible enough to support translations into multiple languages.

Additionally, Washington state voters can request to receive a ballot in over 20 languages. While the VoteWA system does not translate into all 20+ languages, voters can receive a ballot through the VoteWA system.

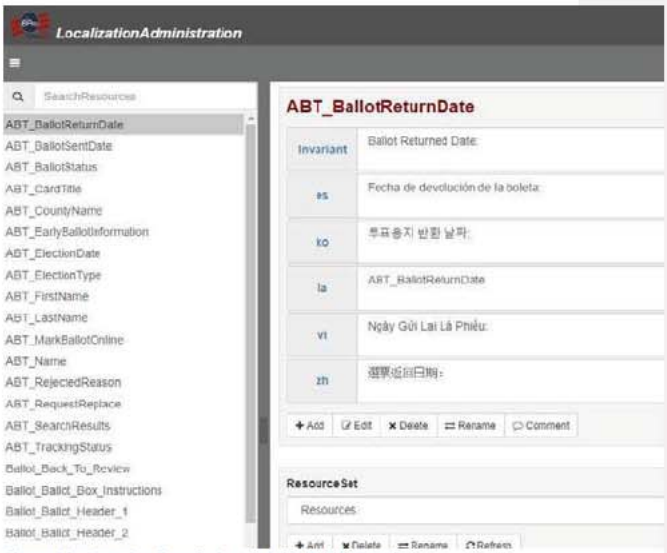


Figure 11 - Inserting Translations for the Public Portal

RR. Customer Service Transformation. In accordance with the Commonwealth's Executive Order 2019-04 – Establishing a "Citizen-First" Government and Promoting Customer Service Transformation, the following shall apply to ensure improvement to digital interactions with citizens and individuals and entities that conduct business with or on behalf of the Commonwealth (each a "Business Partner"). Customer Service Transformation was launched to help the Commonwealth achieve these objectives and is based on the following six (6) design principles:

1. A single online destination for services;
2. Secure access to services through a single login;
3. Consistent and user-friendly online experience across all services;
4. A consolidated and streamlines digital footprint;
5. A single phone number to direct citizens or Business Partners to the services they are seeking.

Offerors are expected to acknowledge these principles. The selected Offeror shall align their performance and deliverables under the Contract awarded from the RFP with these principles.

Additional information regarding the design principles and requirements can be found in **Appendix I, Customer Service Transformation; Design Principles and Requirements**.

Offeror Response

Whenever possible, BPro systems will allign TotalVote system performance and deliverables under the Contract awarded from the RFP with the principles outlined above.

SS. Disaster Recovery (DR). The selected Offeror must employ reasonable DR procedures to assist in preventing interruption in the use of the solution. Offeror shall describe its disaster recovery plans for testing and maintaining operations during disasters and how it will integrate with DOS and Commonwealth DR operations.

Offeror Response

Data Corruption

To minimize the risk of potential data corruption, you have two options. First, you can manage a custom backup strategy. You can store your backups on-premises or use the Point in Time Restore database recovery that includes several elements: Full database backup once a week, differential database backups once a day, and transaction log backups every 5 minutes. Full and differential backups are replicated across data centers to ensure availability of backups in the event of a disaster. If data is corrupted, Point in Time Restore can be restore data to the last known uncorrupted point.

Network Outage

When parts of the network are down, you may not be able to get to your application or data. For this failure mode, a network outage results in application downtime until the network is restored. There are strategies to minimize the possibility of a complete network outage, which are balanced against operating costs to achieve an acceptable level of risk. Network outages do not typically contain a data corruption risk except any transaction that is in process when the outage occurs. Network outages are generally rare.

Failure of Dependent Service

Many services can experience periodic downtime, especially with this type of application that relies on outside data sources and interfaces. Most of the time those outside sources are out of your control and you must wait until service is restored. Notification of failed services and interfaces is built-in to TotalVote and viewable to users with appropriate permissions. Outside sources could be driver's licensing, SSA, felon database, or death records.

Datacenter Down

BPro seeks to avoid this type of disaster by hosting on [redacted]

Offeror shall provide detailed information regarding its DR systems, architecture/frameworks, capabilities, governance, and procedures. Offeror shall conduct annual disaster recovery exercises at a mutually agreeable timeframe with involvement with the Commonwealth, county election officials and key stakeholders.

Offeror Response

[redacted]

Performance

[redacted]

Capacity

[redacted]

Scalability

[redacted]

Redundancy

[redacted]

Availability

The application is written on consistent .Net technology with a standard SQL backend and is fully web-enabled. This application requires no special installation on the average user workstation. The architecture readily supports many web applications for distribution of public information, and can readily grow into future technology, with the potential for smartphone applications.

Recoverability

[redacted]

Point in Time Restore is designed to recover a database to a specific point in time within the backup retention period supported by the service tier of the database. Restoring creates a new database with the same service tier that was in use at the chosen restore point and the lowest performance level supported by that tier.

[redacted]

Monitoring Capability

[redacted]

[redacted]

Network Load Balance and Cluster Support

[redacted]

The selected Offeror shall perform and deliver a report of exercises findings with annual updates to disaster recovery procedures. Offeror shall describe how its DR plans support compliance with the required system availability as described in **Appendix L, Non-Commonwealth Hosted Requirements**, **Appendix H, Service Level Agreements Vendor Hosted**.

Offeror Response

[redacted]

Upon request from the Commonwealth, the selected Offeror shall participate in the Commonwealth disaster recovery tests to ensure continuity of operations. Participation may include, but not be limited to, ensuring the ongoing data communications with various systems interfacing with the selected solution.

The Offeror shall provide co-location services in both a primary and a secondary/disaster recovery data center for hosting the Department of State's environments in the proposed solution. The Offeror shall develop a plan that describes how the switch would occur.

Offeror Response

If selected, BPro will participate in Commonwealth disaster recovery tests to ensure continuity of operations. BPro has engaged in similar efforts with our current customers.

[redacted]

The proposed DR solution should be constructed to implement resources and processes for a critical Commonwealth application to the following service levels:

- RPO – Recovery Point Objective -> 4 hours
- RTO – Recovery Time Objective -> 8 hours
- WRT – Work Recover Time -> 2 hours
- MTD – Maximum Tolerable Downtime -> 12 hours

Offeror Response

BPro agrees to implement resources and processes for our DR solution that meet your requested service levels.

TT. Emergency Preparedness. To support continuity of operations (COOP) during an emergency, including a pandemic, the Commonwealth needs a strategy for maintaining operations for an extended period of time. One part of this strategy is to ensure that essential contracts that provide critical business services to the Commonwealth have planned for such an emergency and put contingencies in place to provide needed goods and services.

1. Describe how you anticipate such a crisis will impact your operations.
2. Describe your emergency response continuity of operations plan. Please attach a copy of your plan, or at a minimum, summarize how your plan addresses the following aspects of preparedness:

    a. Employee training (describe your organization's training plan, and how frequently your plan will be shared with employees)
    b. Identified essential business functions and key employees (within your organization) necessary to carry them out
    c. Contingency plans for:
        i. How your organization will handle staffing issues when a portion of key employees are incapacitated due to illness.
        ii. How employees in your organization will carry out the essential functions if contagion control measures prevent them from coming to the primary workplace.
    d. How your organization will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts, chain of communications (including suppliers), etc.
    e. How, when, and how often your emergency plan will be tested, and if the plan will be tested by a third-party.

1. Describe how your emergency response continuity of operations plan may integrate with DOS, county election officials and Commonwealth plans or scheduled tests.

Offeror Response

BPro has developed individual plans for the continuity of operations with every current VR/EMS customer and has included COOP development as part of the Pennsylvania deployment schedule. If selected, BPro will develop a Pennsylvania COOP plan that is fully approved by DOS.

[redacted]

Several BPro employees work from home full time and all employees have the ability to do so in an emergency. All BPro staff have a current copy of contact information for every BPro employee and contractor. Key BPro staff have the ability to connect to systems through Wi-Fi hotspots from cellular devices.

If an emergency affects Pierre, SD or BPro employees, the President of BPro or his designees will work to allocate resources, based on the type of crisis and the necessary resources. While external employees may be cut off, Pierre staff are easily accessible without any form of digital communications. BPro has designated key employees to provide services in the event of a large-scale emergency.

If selected, BPro will work closely with DOS to develop Pennsylvania's COOP, which will be tested on an annual basis. BPro does not allow for 3rd party testing, due to the proprietary data contained within the system and our contractual obligations to secure that data.

UU. High Availability. The activities and services performed by the DOS and county election officials around voter registration, election management, campaign finance and lobbying disclosure are crucial. During peak times, such as 50 days leading up to an election, the solution cannot experience any unplanned downtime. The solution should be designed to be reliable, robust, and continuously available to state and county election officials.

Core availability requirements are:

1. Windows of availability:
   - **a.** Outside of major election windows: 7:00 AM EST to 6:00 PM EST
   - **b.** Election Day: 5:00 AM EST to 2:00 AM EST (the following morning)
   - **c.** UOCAVA voter support: extended hours based on need
   - **d.** Election Day/Night: extended hours based on the election

e. Campaign finance deadlines: extended hours based on nee
f. Lobbying Disclosure filing deadlines: extended hours based on need
g. Petition Filing deadlines: extended hours based on need

2. Within these windows, availability must be greater than 99.99%
3. Planned maintenance windows are outside of the window of availability unless otherwise agreed upon by the DOS.

Offeror Response

BPro has over a decade of experience supporting election systems during peak election periods. During the windows defined above, there will be no planned maintenance and TotalVote availability will be greater than 99.99%.

X. Security.

1. **Threat Environment.** The Offeror shall describe their understanding of the current threat environment as it relates to elections and how it applies to the systems and interconnections that are addressed in your proposal. Offer shall describe the threat modeling methodology used. Please provide an assessment of the severity of threats and identify and align mitigation approaches to the threats. Also, describe how you monitor on-going security threats and respond to evolving threats, including monitoring for vulnerabilities. Additionally, the Offeror shall describe their ability to receive real-time threat information and act on shared information to mitigate a threat. Finally, the Offeror shall indicate if they participate in information sharing networks, including the Sector Coordinating Council of the Election Infrastructure Subsector (EIS-SCC), the Information Technology Information Sharing & Analysis Center (IT-ISAC), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and others as required by DOS.

Offeror Response

[redacted]

BPro will work with the DOS on any other sharing networks or practices as required.

2. **Security and Disaster Exercises.** As requested by the Department, the Offeror shall actively participate in any security or disaster recovery exercises to test, improve, and update documentation for security or disaster scenarios. The Offeror shall also participate in debrief meetings, otherwise known as a meeting to identify lessons learned, and implement recommendations at the approval of the Department.

Offeror Response

If selected and requested by the Department, BPro will actively participate in security or disaster recovery exercises. BPro has already participated in similar activities with customers, as well as federal, state and county election administrators, security and IT personnel, and other cyber security experts.

3. **Cybersecurity Risk and Remediation.** The Offeror shall describe their process for identifying cybersecurity risks and mitigating them in the election environment and solution, and how the implementation of the mitigation process will increase the likelihood of success on the current proposal. Please be specific and provide examples of how this process has been successful in both confirming appropriate implementation and identifying required changes. Also, please include any internal, lab testing, or third-party testing you regularly employ within your organization and solutions.

Offeror Response

[redacted]

4. **Cybersecurity Responsibility.** The Offeror shall describe the expected scope of cybersecurity-related tasks under this contract and who is responsible for executing those elements. Also, please describe how you will monitor service, development processes, and other solution components to adhere to established security requirements of this proposal. Additionally, please specify the security controls you intend to employ in the proposed solution. This should include any hardware, software, and physical security measures, and any risks they mitigate or residual risks resulting after implementing these controls.

Offeror Response

[redacted]

5. **System Security Plan.** The Offeror shall provide a system security plan, with a quarterly report to DOS, for implementing security requirements and controls for the proposed solution, per NIST special publication 800-18. The plan will be finalized post-award with DOS. If a detailed plan is not available, please provide an outline of such plan along with examples of security plans for similar projects in scope you have been awarded and successfully implemented. Also, please describe if you have a responsible disclosure policy for vulnerabilities. Additionally, detail assignment/ownership of tasks, processes, procedures, and responsibilities for the Offeror, DOS and county election officials when implementing and adhering to the requirements and controls of the plan.

Offeror Response

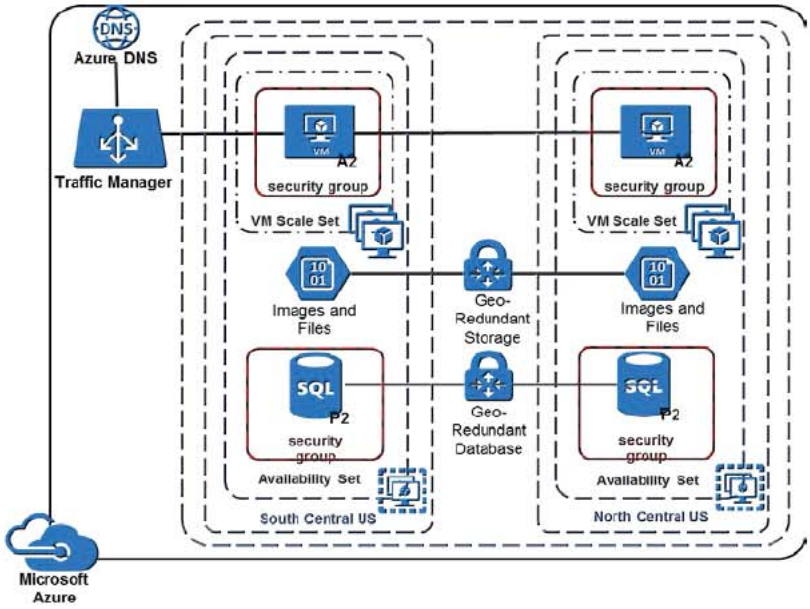
BPro has included a System Security Plan draft as part of this response. This System Security Plan provides an overview of the security requirements and describes the controls in place to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is an asset vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the information system. The security safeguards implemented meet the policy and control requirements set forth in this System Security Plan (SSP). All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

6. **Security Architecture.** The Offeror shall provide an in-depth description of the proposed solution's security architecture, to include proposed

architecture diagrams and data flow diagrams. Fully describe how the architecture will ensure security of election infrastructure.

Offeror Response

[redacted]



7. **Identity and Access Management.** The Offeror shall provide an in-depth description of the proposed solution's ability to conform and integrate with Commonwealth access requirements. Please refer to the Commonwealth's ITP-SEC014 and ITP-SEC037 and Management Directive 2019-04. In the proposed solution, DOS administrators must be able to cancel user's sessions.

Offeror Response

Active Directory (AD) can be used as single sign-on between all applications, including TotalVote. Users are only required to sign on to TotalVote once and can then navigate through all modules, including Campaign Finance, GIS, Petitions, and Election Management. Global System Administrators and other system administrators (as designated by DOS) will be authorized to cancel user sessions and remove certain users from the system (with the option to archive temporary user roles). TotalVote roles also have a configurable expiration date and

time, so roles can be active only during specified periods. If Active Directory is used, then user sessions can be cancelled through AD by authorized users. Cancel user sessions would be for hanging processes and can be accomplished through AD or through server.

8. **DOS Traffic Light Protocol.** The Department has created a policy regarding the identification, marking, handling, storage and protection of Election Infrastructure (EI) information. This policy applies to all DOS employees, contractors, consultants, and other whom access to information covered by this policy is granted. The selected Offeror must describe their understanding of the policy and agree to and acknowledge the policy in their response. You may find the policy in **Appendix R, PADOS Traffic Light Protocol Policy_Election Security.**
Offeror Response

BPro is familiar with a similar TLP through our involvement in the EI-ISAC and, if selected, will utilize Pennsylvania's TLP policy.

9. **Data Security.** The Offeror shall describe any techniques, solutions, technologies or other elements used by the proposed solution to secure the data in the solution and in any other data files in use, in transit and at rest. The Offeror shall also describe their approach to cryptography, including which cryptographic modules and protocols are in use for the proposed solution, and how you conduct key management, where applicable.
Offeror Response

[redacted]

TotalVote's data is encrypted in transit, at rest, and all PII fields are encrypted inside the database to secure Personally Identifiable Information (PII) data. For the majority of users with roles that allow them to view PII, direct access to the database is limited to specific IP addresses. Database user accounts utilized by TotalVote are setup with minimal permissions so access to the database structure and ad hoc queries is not allowed.

[redacted]

Transport Layer Security 1.2 (TLS) for all connections. There are numerous benefits to using TLS including strong authentication, message privacy, and integrity (enables detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, ease of deployment and use.

10. **Cloud Security.** If the proposed solution uses cloud service technologies, the Offeror must obtain and maintain FedRAMP moderate certification. Please describe your approach to using cloud service technologies and whether you currently have a FedRAMP certification or not. If the Offeror does not have a current certification, please detail your approach to obtaining the requested certification and specify the timeline for certification.

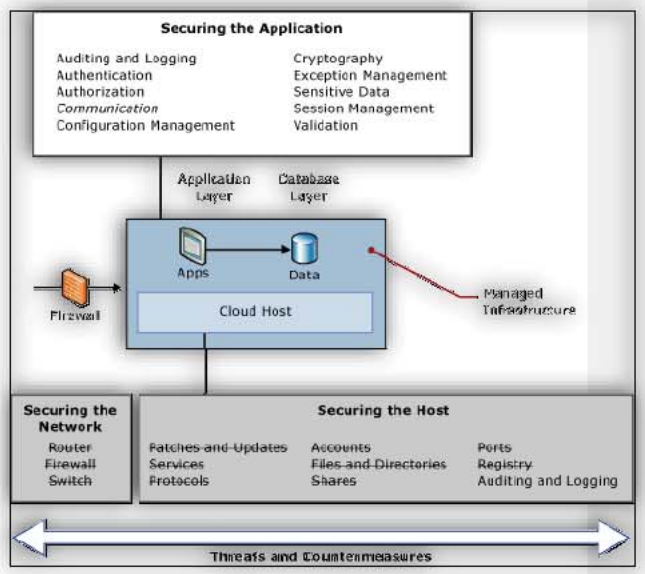
    The Offeror shall also describe how the proposed cloud-hosted solution will support the DOS information security compliance requirements as described in the Commonwealth ITPs. The Offeror shall also include all security options that are available, whether or not they will be used.
    Offeror Response

[redacted]

[redacted]

FedRAMP is a mandatory U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.

[redacted]



11. Security Features. The Offeror shall explain any other security features and capabilities of the proposed solution and processes. For example, does the Offeror have the capability for the following?

1. Does the solution protect the audit logs? (i.e., encryption, hashing, etc.)

The TotalVote solution protects the audit logs through encryption and hashing.

2. Does the Offeror's documentation contain security auditing procedures?

Yes, security auditing procedures are included in TotalVote documentation.

3. Does the Offeror provide digitally signed programs or whitelisted applications?

Yes, TotalVote uses digitally signed programs and APIs.

4. Does the Offeror's solution prevent unauthorized access?

[redacted]

5. Does the Offeror implement any specific hardening procedures and standards in the proposed solution?

TotalVote uses secure coding practice standards.

6. What password features are contained within the proposed solution?

[redacted]

7. Does the Offeror's solution contain any remote technology?

For enabling the smooth operations, BPro can provide Remote Access to the TotalVote network from external network for a few limited employees. Remote access to the TotalVote network is strictly controlled and BPro will take all appropriate steps to safeguard the network from remote access vulnerabilities.

8. Does the Offeror conduct any independent security audits with third parties?

BPro performs security audits in accordance with its contractual obligations. This includes security audits by DHS, National Guard and private companies. In addition to these security audits, BPro is researching options for utilizing an independent security audit organization through our relationship with the EI-SCC.

9. Does the Offeror or the proposed solution have any other security features that may not be covered above?

BPro regularly participates in security forums, conferences and other events attended by election professionals, vendors and thought leaders from around the country.

Offeror Response

BPro has responded to each individual question above.

12. **Endpoint Protection.** The Offeror shall confirm whether or not they have advanced endpoint protection for any component that is part of the core service offering. All systems accessing the core service offering must have advance malware detectoin along with traditional anti-maleware software. Specifically, the advance malware softare must allow root-cause analysis with forensics showing how infection occurred along with actions maleware took.

Offeror Response

[redacted]

Endpoint protection outside of TotalVote solution is the responsibility of the PA DOS and the counties. Advanced

13. **Media Handling and Disposal.** In addition to adhering to Commonwealth disposal requirements, the Offeror must also meet minimum requirements subject to the approval of the DOS. Minimum requirement must include, but are not limited to:
    - **a.** Ensure that media is disposed of securely and safely when no longer required, using formal documented procedures.
    - **b.** Sanitize equipment containing storage media prior to disposal (reference best practices such as NIST SP 800-88 Guidelines for Media Sanitation or equipment disposal procedures documented at the Commonwealth of Pennsylvania) and:
        - **1)** Destroy, securely overwrite, or make unavaialble DOS or county election official identifiable data.
        - **2)** Destroy, securely overwirte, or make unavailble software consistent with the software licensing agreement.
    - **c.** Ensure the safe and secure disposal of sensitive media.
    - **d.** Ensure that system documentation is protected against unauthorized access.
    - **e.** Ensure media containing information is protected against unauthorized access, misuse, or corruption during transportation or storage beyond the DOS's physical boundaries.

Offeror Response

BPro will utilize the NIST SP 800-88 Guideline for Media Sanitization. BPro will destroy or securely overwrite DOS and/or county election PII. The software agreement will be consistence the destruction, secure overwrite or make unavailable language with regards to Media Handling and Disposal.

BPro will ensure the safe and secure disposal of sensitive media in our control. All system documentation will be located on BPro's SharePoint and protected against unauthorized access, both internally and externally. Access will only be given to team members who are working on the PA project. All PA media will be protected from unauthorized access, misuse or corruption whether the data is physically present at BPro or in-transit to our remote workers.

14. **Secure Development and Configuration Practices.** The selected Offeror shall describe its application development and configuration practices, including any subcontractor development and configuration practices, and how it will reasonable protect the security, confidentiality and privacy of DOS, county election official, and individual data who may be considered as part of the solution. Specifically, the Offeror shall state whether it will adhere to the following:
    - **a.** Microsoft Secure Coding Guidelines for the .NET framework;

b. CERT Secure Coding Standards;
c. OWASP Secure Coding Principles;
d. Privacy by design principles;
e. Federal Trade Commission's Fair Information Practice Principles; or other principles not covered above.

Offeror Response

BPro will adhere to the framework, standards and principles identified above. BPro understands that security is a critical concern for the development, implementation and management of the Pennsylvania system and security is at the core of the solutions we offer our customers. Our strategy for addressing this concern is two-fold:

- Secure coding practices ensure that the code is structurally sound and free of any major structural issues that could cause the data, applications, or systems to be exposed to a high-level of risk
- Implement an active, dynamic security architecture consisting of technology and process that creates an active, operational paradigm for managing security and mitigating risks.

Secure coding will focus on developing code that minimizes and securely authorizes access to code objects, applications, and data to ensure that access is coming from a trusted source, whether that source is other internal code, other components, or system administrators/users. Data encryption will be employed to ensure that voter registration data is secure while being stored in the database, manipulated as a part of a function, or in transit from one function to another to ensure that only authorized functions, procedures, or users can gain access to that data. Input checks and validations will be performed at all ingress points into the application whether through direct input received from the web front-end interface or through transfers from function to function or component to component to ensure that no malicious code can infiltrate the system in any way through application ingress points.

These coding practices, coupled with the following five-part approach to implementing and managing the information security architecture for the system, will provide the most effective and efficient level of protection and the highest level of risk mitigation.

This five-part approach is comprised of the following:

1. Vulnerability Management and Remediation
2. Event Monitoring
3. Privilege Management & Auditing
4. Computer Incident Handling
5. Security Architecture Design & Implementation

15. **Project Work.** All work related to this RFP must be completed within the continental United States.

Offeror Response

All work related to this RFP will be completed in the United States. BPro adheres to this policy 100% of the time for all work we do.

16. **Passwords.** The solution shall require and support the use of complex, secure, and unique passwords for all systems users for authorization. The passwords shall not contain any aspect of the user's name and will be checked against a dictionary of known-bad password choices. Maintenance of systems passwords shall be configurable by the DOS and provide flexibility to meet national, federal, and Commonwealth of Pensnylvania password requirements. The solution shall also provide flexibility to configure user password requirements based on user roles and permissions.

Offeror Response

When a password is entered by a user, the entered alphanumeric values are replaced with an asterisk "*". Passwords are stored encrypted within the system, not as clear text or a value from which the password may be derived. Passwords policies are configurable and are currently configured to meet your requirements.

17. **Multi-factor technologies.** The solution shall require and support the use of multi-factor technologies for authentication and authorization. The multi-factor technologies must be reviewed and approved by the DOS.

Offeror Response

TotalVote can provide multi-factor authentication through a combination of Yubikeys (or eTokens), phone applications like Microsoft Authenticator or Duo, and username/password login. While most users will access the system from a specifically assigned computer (using the IP address as one of their MFA factors), TotalVote allows specifically assigned users to access TotalVote from any device through a current browser using other DOS-approved MFA technologies.

18. **Removal of System Access.** The Offeror must establish processes and procedures for the timely removal of system access for employees, contractors, and subcontractors when duties change or when separating from service.

Offeror Response

Global System Administrators and other system administrators (as designated by DOS) will be authorized to remove certain users from the system (with the option to archive temporary user roles). TotalVote roles also have a configurable expiration date and time, so roles can be active only during specified periods.

19. **Sessions.** The Offeror and the proposed solution must support appropriate management of sessions on system components to include:
    - **a.** Establish procedures to shut down or reauthorize inactive sessionsafter a defined and reasonable period of inactivity;
    - **b.** Restrict user access to shared systems, especially those extending across the Department's boundaries, in according with access control policy and requiremtns of the business applications
    - **c.** Ensure that access to operating systems is controlled by a secure log-on procedure.

Offeror Response

TotalVote's session policy currently meets DOS requirements in every deployment.

20. **Remote Access.** The Offeror and the proposed solution must meet requirement subject to the review and approval by the DOS. At a minimum, remote access requirements shall include but not limited to:
    - **a.** Policies and procedures for remote access to mitigate the threat or risk posed by users or devices authorized to connect remotely to the proposed solution and infrastructure including but not limited to:
        1) Monitoring practices for remote access sessions;
        2) Requirements for remote access devices;
        3) Remote access session controls that conform to the principle of least privilege;
    - **b.** Ensure mitigation is not susceptible to end-user modification.
    - **c.** Use industry standards for remote access solutions;
    - **d.** Adhere to the Commonwealth's remote access policies; and
    - **e.** Ensure that remote access solutions use equivalent technologies that require multi-factor autheitcation and include documentation of the configuration.

Offeror Response

For enabling the smooth operations, BPro can provide Remote Access to the TotalVote network from external network for a few limited employees. Remote access to the TotalVote network is strictly controlled and BPro will take all appropriate steps to safeguard the network from remote access vulnerabilities.

Remote Access is configured in accordance with BPro's minimum requirements:

- Remote access controls shall be provided with sufficient safeguards through robust identification, authentication and encryption of the traffic.

- Secure remote access is strictly controlled.
- Control is enforced via two factor-based authentication with 256-bit AES (Advanced Encryption Standard) / 3DES (Data Encryption Standard) encryption.

21. **User Auditing.** The Offeror and the proposed solution must ensure system controls are effectively enforcing access policies with review and approval by the DOS. The controls must include:

a. Periodically review user access rights based on the risk to the data, application, or system using a formal process; and

b. Implement mechanisms to monitor the use of privileges.

Offeror Response

A history of all activity for a voter record is logged in the Change History activity log. In addition to tracking all changes to the voter record, the system also retains auditing information such as:

- User
- Date and Time completed
- Source

22. **General Security.** The Offeror shall describe how the proposed solution will meet or exceed the following:

a. Describe how the Offeror and/or proposed solution will protect private voter information. Also, in general, how will the solution protect sensitive infromation.

Offeror Response

The TotalVote Voter Registration module is not only a statewide voter registration list, but a full voter administration package. The system includes several confidential fields, including driver license numbers, dates of birth, partial social security numbers, along with information about confidential voters. Providing functionality and security for the system is a high priority. The data stored in the TotalVote Voter Registration module is private and BPro takes multiple precautionary security measures to ensure data safety.

Data encryption will be employed to ensure that voter registration data is secure while being stored in the database, manipulated as a part of a function, or in transit from one function to another to ensure that only authorized functions, procedures, or users can gain access to that data. Input checks and validations will be performed at all ingress points into the application whether through direct input received from the web front-end interface or through transfers from function to function or component to component to ensure that no malicious code can infiltrate the system in any way through application ingress points.

These coding practices, coupled with the following five-part approach to implementing and managing the information security architecture for the system, will provide the most effective and efficient level of protection and the highest level of risk mitigation.

This five-part approach is comprised of the following:

1. Vulnerability Management and Remediation
2. Event Monitoring
3. Privilege Management & Auditing
4. Computer Incident Handling
5. Security Architecture Design & Implementation

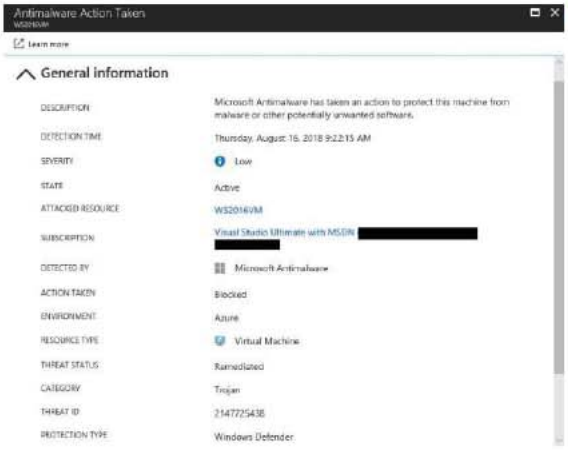
b. Describe how the Offeror and/or proposed solution will protect infrastructure from malware.
Offeror Response

[redacted]

c. Describe how the Offeror and/or proposed solution will warn the DOS of the risk of phishing attacks.
Offeror Response

TotalVote needs SMTP to send system emails to end users. This can be done with an external SMTP vendor like SendGrid or through your internal email system. Making sure that Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain Message Authentication, Reporting and Conformance (DMARC) are enabled, configured and functioning is critical in protecting any environment to phishing attacks.

d. Describe how the Offeror and/or proposed solution will warn the DOS of malware attacks.
Offeror Response



[redacted]

Figure 12 - Malware Warning in the Azure Security Center

e. Describe how the Offeror and/or proposed solution will protect against Denial of Service attacks.
Offeror Response

[redacted]

f. Describe how the Offeror and/or proposed solution will protect against identity spoofing.
Offeror Response

[redacted]

g. Describe how the Offeror and/or proposed solution will protect data from tampering.
Offeror Response

All actions in TotalVote are logged at the database level in a separate audit table. If data is deleted in TotalVote is not deleted in the database. No end user has direct access to the database to delete information; their only access is in TotalVote via their assigned credentials. Reports will be created for to allow the DOS Security Team and County Officials to the review the changes for training and/or investigative purposes.

h. Describe how the Offeror and/or proposed solution will log system and user activity.
Offeror Response

Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

i. Describe how the Offeror and/or proposed solution will authenticate and authorize users, including how the solution will utilize two-factor or multi-factor authentication.
Offeror Response

[redacted]

WW. Operations and Procedures. The Offeror shall provide and/or describe in detail their operations and procedures:

1. Escalation. The Offeror shall describe their organizational chain-of-command for escalating problems needing resolution.

Offeror Response

External to Internal Escalation:

The client initially records and prioritizes in the ticketing system. If an item is not addressed in a timely manner, the BPro BA assigned to the project should be alert by the client. If the BPro BA is unable to be reached, the BPro Project Manager can be utilized for an expedited response.

Internal Escalation:

The BPro BA assigned to the project is the primary source for issue escalation and resolution. They utilize the ticketing system so that the Product Manager and Development Manager can accurately account for a prioritize resources for the resolution of reported items. Once the ticket has been accounted for and the proper information has been included in the issue, the ticket is scheduled and assigned. If the ticket is not assigned to a staff member for resolution, the BPro BA has the authority to work directly with development staff to resolve critical issues.

2. Sensitive Information. The Offeror shall define sensitive functions and sensitive positions and describe how individuals involved in sensitive functions and with access to sensitive information are trained and tested for knowledge and job performance. Also, describe your process for how access to sensitive functions relates to an individual's assignment as key personnel. Additionally, please describe your process for granting personnel access to sensitive functions or information. The Offeror shall also describe confidentiality and privacy approaches for protecting personal or sensitive information or data.

Offeror Response

Access to sensitive data will only be given to the appropriate roles and permissions are granted and restricted by DOS and county administrators. Our system allows an authorized user to create a "Status Flag" for a voter with any protections. Once this Status Flag is created, only authorized users can view the voter record and the voter record does not appear in any exports or searches. Confidential voters are usually required to vote by mail in order to keep their name and information off the poll roster. Specialized training and sensitive training materials can be provided for these users.

With the amount of sensitive information that is contained on many voter materials, redaction is another important privacy tool. Redaction can block out Social Security Numbers, Driver's License Numbers, Birthdates, Signatures and other materials both in the TotalVote system an in reports run through the system. Redacted information is only viewable to authorized users or processes, which are established setting user roles.

3. **Information and Communication.** The Offeror shall detail and describe their process for moving data, whether digitally or physical, while maintaining appropriate security protection and data integrity. This includes relationships between the Offeror and subcontractors, proposed subcontractors, government, where applicable. Also, please list applicable security requirements that apply to your security protocols or products.

Offeror Response

BPro will work with DOS to ensure all security protocols are followed while moving data. It is our experience that every state has different rules and procedures for moving data and as the system provider, it is BPro's responsibility to comply with every customers' unique rules and procedures. While building Arizona's new system, this meant physically meeting and exchanging data stored on an encrypted drive. Encryption keys were sent separately, ensuring that data was secure throughout the entire process. In Washington, no data is allowed outside the state's environment, which meant BPro conducted all development on Washington servers.

4. **Documentation.** The Offeror shall describe how it will update and maintain application and process documentation. All documentation shall be stored within the Commonwealth on Commonwealth resources. The selected Offeror shall maintain and update system documentation associated with each functional and technical release that, at a minimum, depicts the functional and technical requirements, design, key decisions, interface, integration, database design, data flow diagrams, data dictionary, entity relationship diagrams, workflow diagrams, report layouts, data, security, technical, test, test tools, user manuals, backup, recovery, and restart procedures. Documentation also includes adding and maintaining documents within the source code as appropriate. The selected Offeror shall commence documenting creation upon notice to proceed. Creating legacy documentation is not required.

Documentation includes the following categories:

a) **Technical Documentation**. Describes the technical architecture of the system. This documentation describes at a minimum the system functions, application procedures, error troubleshooting guides, relational database design, data dictionary, performance specifications, program descriptions, release notes, and dependency diagrams.

b) **System Operations Documentation.** Describes the steps and procedures needed to operate the system. This shall include system administration procedures, system start up and shut down procedures, dependency diagrams, deployment procedures, backup and recovery procedures, archival and restoration procedures, batch job procedures, security procedures, and maintenance procedures.

c) **System Standards Manual.** Describes the standards used to develop the applications such as coding methodology, naming conventions, and other similar items.

d) **User Manual.** Describes all the essential information for the user to utilize the system, including but not limited to system capabilities, operating instructions and step by step procedures for each user action.

Offeror Response

BPro will provide technical documentation, system operations documentation, system standards manual, and the user manual through the course of the project as we have provided in our other solutions.

Initial system technical documentation and system operations documentation will be created toward the start of the project and will be updated throughout the course of the project. During M&O, if newly defined requirements result in a brand-new feature or a change to user experience, BPro will update the user manuals and guides to reflect the changes to the system.

End user support, including user manuals and guides, is available within the TotalVote application and accessible through any browser. The user manual will be a set of user guides for each main module of the system along with user login and permissions guides.

5. **Patch Management.** The Offeror shall describe their process for deploying updates or upgrades to solution infrastructure, hardware, software or other related solution components. Please also describe the process for approvals needed on both the Offeror and DOS. The Offeror shall describe both in band and out of band patch procedures. The description should also address vulnerability detection and security remediation, patching speeds, and incident response and escalation procedures. In the event a product or solution component can't be readily updated, describe controls and monitoring that will be used to identify suspicious access or activity.

Offeror Response

BPro's patch management is outlined in Section 11 of the Implementation Plan provided in this response.

6. **Lifecycle Management.** The Offeror shall describe their lifecycle management process for information technology. Does the Offeror have a standardized lifecycle process? Also, please describe your experience and policies in using lifecycle management for work of the same scope of this project. Describe the processes in place to manage hardware and software

and how do they ensure security is addressed appropriately in addition to ensuring the solution meets business needs?

Offeror Response

BPro utilizes automated tests, client input, and evolving security and technology standards to drive product lifecycle. Additionally, BPro maintains a log of potential features and works with clients to develop these features into robust solutions. This development with the client occurs through joint application development sessions, on-site visits, and by personally working with the customer to learn the challenges faced in their jurisdiction.

[redacted]. With world class security and infrastructure experts focused on the environment, BPro can focus on continuing to develop and deploy TotalVote systems and technology enhancements.

7. **Audits and Analysis.** The Offeror shall detail and describe audits, security audits, penetration analysis, or third-party audits or analysis performed at routine intervals. If conducted, please provide copies of those audits or analysis. Also, the Offeror may be subjected to external audits, or penetration analysis by an organization of DOS' choosing. This would also include any requests by DOS to audit the solution. This may occur at the planning stage, implementation, as a confirmation of proper implementation, or during operations. The DOS will have the right to request reasonable adjustments at the Offeror's expense where those requests are based upon audit findings pertaining to the solution or hosting.

   If conducted, please provide examples of prior security testing and evaluation reports, vulnerability assessment, and any related reports. Additional, DOS may require contractors and their suppliers to provide security testing reports for projects similar in scope that details the effectiveness of security controls. The solution shall be flexible to meet audits as requested by DOS. Audits may include, but are not limited to:

   1. Solution functions
   2. System architecture
   3. Security
   4. Reports
   5. Notices
   6. Financial

Offeror Response

BPro is a member of Election Infrastructure- Subsector Coordinating Council (EI-SCC) and InfraGard, a non-profit organization serving as a public-private partnership between US businesses and Federal Bureau of Investigation (FBI) that shares information to better secure our country's infrastructure.

BPro will work with the DOS on auditing and analyzing the TotalVote Solution including Campaign Finance and Lobbying Disclosure. Audit criteria for analysis should include Facilities, Data Security, Data Sharing, Policies (that restrict access to applications, data and system functions), Account creation/controls and Authentication & Authorization controls.

8. **Infrastructure tracking.** The offeror shall have a process to document, track, and audit all infrastructure. The Department will have access to the infrastructure tracking process and documentation.
Offeror Response

[redacted] Access to this information can be granted to approved Department personnel.

9. **Certification.** The Offeror shall provide evidence and describe any certifications or registration that demonstrate the organization's adherence to national standards or principles. Please also detail how you monitor adherence to those processes. Also, provide evidence and examples of your documented processes.
Offeror Response

Unlike tabulation equipment, there is currently no national certification process for Voter Registration, Election Management, Election Night Reporting and Campaign Finance systems. That may change in the future and BPro is actively participating in efforts to create national standards, including the Center for Internet Security's (CIS) *Security Best Practices for Non-Voting Election Technology*. BPro is also monitoring similar efforts by NIST and MITRE.

In Texas, BPro's "bottom-up" TotalVote system has passed the Texas certification process for exchanging voter registration data between Travis County's system and the state's TEAM database.

10. **Supply Chain Management.** The Offeror shall provide specific detail in their approach to supply chain management and the selection process for suppliers. Please provide information including, but not limited to:

1. How do you assess and rank the risk of suppliers?
2. How do you review content from non-U.S. sources?
3. How do you review suppliers and their products to ensure they do not contain vulnerabilities or malicious content?
4. How is information regarding supply chain issues shared among the Offeror and suppliers?
5. What is your proposed approach to evaluate replacement components or new technology to ensure adequate security?

6. How do you monitor compliance of suppliers to requirements of the contract? Describe any processes or auditing suppliers to maintain security or requirements of the contract.
7. How do you manage technology that is no longer supported by the supplier? Please describe your transition process with the supplier to ensure requirements are met and how you maintain communication with DOS.

Offeror Response

[redacted]

11. Services Provided. The Offeror shall provide managed services needed to monitor, maintain, and administer the hosted solution. These services shall include system administration, application administration, patching and maintenance services, monitoring and alerting services, release management, change management services, infrastructure management, routing and firewall services, security and intrusion prevention, and a high-speed network backbone for database servers. The Offeror shall be responsible for building, maintaining, and managing the hardware and software at the data center(s). The following hosted services shall be included, but not limited to:

1. Server updates and critical patches
2. Hardware firmware updates
3. Virtualization management and security updates
4. Internal data center network services (routing, security, VLANs, zoning, etc.)
5. Maintain and monitor data backups
6. Data replication management
7. Infrastructure management
8. Compliance
9. Annual penetration testing
10. TLS certificate management
11. Secure file transfer

Offeror Response

[redacted]

XX. Copy to New Election. The steps necessary to hold an election will not vary from election to election. The proposed solution shall have the capability to copy setup from

one election to another. The solution shall be capable of supporting multiple election types and setup. (ex: Presidential Election, Municipal Election, Special Election, etc.)

Offeror Response

TotalVote provides a Copy Election function, called Scheduled Contests, which includes a feature that determines active contests for the new election definition based on the term length of contests in previous election. For example, the office of President was on the Primary and General ballot in 2012 and has a 4-year term so when Copy Election is used for the 2016 Primary and General elections, the office of President is automatically placed on the ballot. The same rule applies for districted offices, like Mayor. When setting up an election, users can preview the offices that will appear on the ballot and then simply execute the election setup process. Any unexpired terms will need to be added manually. Primary election winners and unopposed candidates are rolled over to the General election automatically so those candidates and contests do not need to be rekeyed.

TotalVote also copies all polling place and precinct configurations from the most recent same type election. Multiple elections are completely supported throughout TotalVote.

SCHEDULE RACES

For: 2016 General - 11/8/2016

2018 ▾ Election Year

Setup Election Races Adds all races below to the current election

Race	Office Seq #	Vote For	Term Length	District Type	District Name	Primary Non-Partisan	Primary Partisan	General
United States Representative	110	1	2	Congressional	District 1	☐	☑	☑
United States Representative	110	1	2	Congressional	District 2	☐	☑	☑
United States Representative	110	1	2	Congressional	District 3	☐	☑	☑
Secretary of State	210	1	2	Statewide		☐	☑	☑
State Treasurer	220	1	4	Statewide		☐	☑	☑
Commissioner of Public Lands	230	1	4	Statewide		☐	☑	☑
State Representative	300	1	2	Legislative	District 1	☐	☑	☑
State Representative	300	1	2	Legislative	District 10	☐	☑	☑
State Representative	300	1	2	Legislative	District 11	☐	☑	☑
State Representative	300	1	2	Legislative	District 12	☐	☑	☑
State Representative	300	1	2	Legislative	District 13	☐	☑	☑
State Representative	300	1	2	Legislative	District 14	☐	☑	☑
State Representative	300	1	2	Legislative	District 15	☐	☑	☑
State Representative	300	1	2	Legislative	District 16	☐	☑	☑
State Representative	300	1	2	Legislative	District 17	☐	☑	☑
State Representative	300	1	2	Legislative	District 18	☐	☑	☑
State Representative	300	1	2	Legislative	District 19	☐	☑	☑
State Representative	300	1	2	Legislative	District 2	☐	☑	☑
State Representative	300	1	2	Legislative	District 20	☐	☑	☑
State Representative	300	1	2	Legislative	District 21	☐	☑	☑
State Representative	300	1	2	Legislative	District 22	☐	☑	☑
State Representative	300	1	2	Legislative	District 23	☐	☑	☑
State Representative	300	1	2	Legislative	District 24	☐	☑	☑

Figure 13 - Scheduled Races allows users to copy previous elections

YY. Training. The Offeror shall describe their approach to training users, which includes both DOS and county election officials, and system administrators as well as available training services. The DOS requires training as part of the RFP to implement the solution, maintain the solution, and train DOS and county election officials on system functionality and workflow. The Offeror shall describe their training offerings, methodologies and approaches for various system users. The DOS has several tools to offer for training purposes, which include Skype, SharePoint sites, OneDrive, and Zoom. The selected Offeror and DOS shall collaborate and mutually agree upon training setup, location, offerings, course criteria and resources to prepare DOS and county election officials for implementation, maintenance and support, enhancements or other solution requirements, as needed. The DOS estimates approximately 20 Commonwealth employees and roughly 400-500 county election officials for training sessions. When training system users, a staging or testing environment shall be made available during and after implementation. The staging or testing environment shall mirror the configuration and functionality of the production environment to simulate real-world training conditions.

Offeror Response

User Training for TotalVote will take place after development has been completed for all modules and prior to User Acceptance Testing (UAT). BPro will use a "train the trainer" methodology to train DOS personnel to become "super users" of the software. This train-the-trainer training will be led by the BPro Training Lead and TotalVote lead subject matter expert. After the DOS personnel are adequately trained, they will be prepared to handle support and training for all end users including County staff. DOS personnel will join BPro trainers for two weeks of regional trainings around the state for County staff. This will serve to both train County staff and reinforce the expertise of DOS "super users" in the TotalVote system.

All hands-on software training (for both DOS and County user training sessions) will take place in a Training (Staging) environment configured identically to the Production environment.

Training Approach and Curriculum

For the "train-the-trainer" training sessions, BPro will work with the DOS to finalize a user training schedule and plan. The scope of the DOS training shall encompass two parts: 1) State user training, and 2) Training County users on all TotalVote modules.

BPro will provide the following on-site "train the trainer" sessions for DOS-designated training staff:

- Provide training to DOS trainers on all modules completed throughout the Project (relevant to both State and County users)
- Assist DOS staff in the use of BPro-provided training materials
- Facilitate a dry run of the training session and make recommendations to DOS staff on clarity, flow, and accuracy of training presentation
- Make modifications to training materials as necessary

Training for DOS-designated training staff will be conducted by BPro on-site over the course of one week (Monday through Friday). Attendance for all five days of training is required for DOS-

designated training staff. Locations, training equipment, and printed materials will be provided by the DOS office (training materials will be created by BPro and provided electronically to the DOS prior to training.) During the course of each day, BPro will demonstrate the components of all modules. Users will log in and practice functional tasks in small groups at individual workstations, while using individual logins from a variety of user groups for both State and County permissions.

Every day, the training will focus the content on:

- Training Materials
- Module overview
- How to perform designated tasks within each module
- How to verify output of tasks
- Reporting
- Review

After the completion of the "train the trainer" week of training sessions, DOS staff and BPro staff will conduct hands-on training over the course of two (2) weeks for County staff. This training will be held in regional locations throughout the state that ensure the highest levels of participation. The DOS and BPro will coordinate the final schedule, arrangements, and communication for regional County trainings.

BPro shall provide the following activities regarding on-site training for County staff:

- Assist with the setup of the training facilities, such as setting up a dedicated workstation with hardware for printing, scanning, and document imaging
- Attend all training sessions for the entire duration to answer any questions DOS cannot answer and provide assistance regarding system operation
- Assist in troubleshooting technical issues that may arise during initial setup or during the sessions

For the County training, BPro will conduct formal review sessions to allow the trainers an opportunity to review and provide feedback on each training session for improvement. (Feedback may be gathered verbally or from feedback forms collected from attendees at the County trainings.) A short review session at the end of each day would be valuable to discuss areas for training improvement, as well as a weekly report submitted on Fridays to wrap up all findings during each of the training sessions. A final post-mortem with DOS staff and BPro will be conducted via conference call after all regional trainings are complete with BPro producing a final User Training report for DOS.

For each Voter Registration system BPro has deployed, we continue to provide training and support after go-live. This support will continue in the Commonwealth of Pennsylvania, by phone and web conferencing, with in-person training options also available. A great example is the regional training program BPro participates in for North Dakota. For two weeks every two years, BPro and ND DOS staff travel to regional locations around the state and provide full day

training on our systems. Another example is using annual conferences as an opportunity to further train County staff. BPro conducts a training session at South Dakota's annual conference of county auditors where BPro presents refresher materials, participants learn about system upgrades, and there is ample opportunity to ask questions about the TotalVote system. Cost for these in-person trainings is extra and BPro will work with DOS to determine the best continuing education opportunity for the PA DOS TotalVote system.

ZZ. Offeror Reporting Requirements Post-Award. The selected Offeror must describe, document and/or notify the DOS regarding:

1. Ownership, Financing, Employees, Hosting Location. The Offeror shall immediately notify the Commonwealth of any changes to information on the Offeror's employees and affiliates, locations, company ownership, company size, ability to provide support, team, partners, or changes in third-party agreements. Additionally, the Offeror must provide information on foreign ownership/financing, data hosting, and production for any hardware or software products, including any potential conflict of interest that may have developed for employees and affiliates;

2. Advisory Notices. System advisory notices issued for any piece of software or hardware deployed in the Commonwealth of Pennsylvania regardless of whether the incident behind the notice occurred in Pennsylvania;

3. Security Measures. And any planned or updated security testing or risk/vulnerability assessments conducted by the Offeror or a third-party with results or findings;

4. SOC 2 Reporting. Offeror must provide annual American Institute of Certified Public Accountants (AICPA) Attestation Standard (AT) Sec. 101 Service Organization Control ("SOC") 2, Type 2 Certification (AT Sec. 101 SOC 2, Type 2), or an equivalent certification approved by the Commonwealth. Equivalent certifications include, but are not limited to: International Organization of Standards (ISO) 2700x certification; certification under the Federal Information Security Management Act (FISMA); and AT Sec. 101 SOC 3 (SysTrust/WebTrust) certification.

If selected, BPro will notify DOS if any of the event of any ownership changes, security test results or system advisory notices relevant to DOS. As noted throughout this document, BPro will conduct an annual SOC 2 audit of the Pennsylvania TotalVote system and provide DOS with results.

VII. Supplier Reporting Requirements Post-Award. The selected Offeror shall describe, document and/or notify the DOS regarding:

1. Ownership, Financing, Employees, Hosting Location. Any changes to information on the Supplier's employees and affiliates, locations, company size and ability to provide support. Additionally, the supplier must provide information on foreign ownership/financing, data hosting, and production for any hardware or software products, including any potential conflict of interest that may have developed for employees and affiliates;

2. Advisory Notices. System advisory notices issued for any piece of software or hardware deployed in the Commonwealth of Pennsylvania regardless of whether the incident behind the notice occurred in Pennsylvania;

3. Security Measures. And any updated security testing or risk/vulnerability assessments conducted by the Supplier or a third-party; Security testing or risk/vulnerability assessments shall be conducted on an annual basis with results shared with the Department of State.

a. Source Code Escrow Post-Award. The selected Offeror must deliver a Source Code and extended code Escrow Package to an Escrow Agent and enter into an escrow agreement on commercially reasonable terms subject to the provisions of this Contract.

1. The selected Offeror shall deliver a Source Code Escrow Package to an Escrow Agent and enter into an escrow agreement on commercially reasonable terms subject to the provisions of this Contract within **thirty (30)** days of the execution of this Contract.

2. If at any time during the term of this Contract, the Offeror provides a maintenance release, upgraded version of the Licensed Software, or any additional changes impacting source code, the Offeror must, within **ten (10)** days deposit with the Escrow Agent.

3. The Commonwealth reserves the right, at any time, either itself or through a third party contractor, upon **thirty (30)** days written notice, to seek verification of the Source Code Escrow Package.

4. The "Source Code Escrow Package" shall include at a minimum the following:

a) A complete copy in machine-readable form of the source code and executable code of the Licensed Software, including any updates or new releases of the product;

b) A complete copy of any existing design documentation and user documentation, including any updates or revisions; and/or

c) Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code. Such instructions must include all tools used to generate executable code.

5. The Source Code Escrow Package may be released from escrow to the Commonwealth, temporarily or permanently, upon the occurrence of one or more of the following:

a) The Offeror becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business or assets, becomes subject to any proceeding under bankruptcy or insolvency law, whether domestic or foreign;

b) The Offeror has wound up or liquidated its business voluntarily or otherwise and the Commonwealth has reason to believe that such events must cause the Offeror to fail to meet its warranties and maintenance obligations in the foreseeable future;

c) The Offeror voluntarily or otherwise discontinues support of the provided products or fails to support the products in accordance with its maintenance obligations and warranties.

6. If the Commonwealth desires to obtain the Source Code Escrow Package from the Escrow Agent upon the occurrence of an event in this Section, then:

a) The Offeror must comply with all procedures in the Escrow Contract;

b) The Commonwealth must maintain all materials and information comprising the Source Code Escrow Package in confidence in accordance with this Contract;

c) If the release is a temporary one, then the Commonwealth must promptly return all released materials to Offeror when the circumstances leading to the release are no longer in effect.

7. Upon release from the Escrow Agent pursuant to an event described in this Section, the Offeror automatically grants the Commonwealth a non-exclusive, irrevocable license to use, reproduce, modify, maintain, support, update, have made, and create Derivative Works.

8. Further, the Commonwealth must have the right to use the Source Code Escrow Package in order to maintain and support the Licensed Software

so that it can be used by the Commonwealth as set forth in this Contract.

9. Any Derivative Works to the source code released from escrow that are made by or on behalf of the Commonwealth must be the sole property of the Commonwealth.

Offeror Response:

- Describe the approach to establishing and maintaining an escrow agreement and the terms of such agreement:

- Describe how the Offeror will ensure the Commonwealth can access the source code in escrow:

- Describe the process for ensuring the escrow package is updated regularly with all source code (including all configurations, customizations, enhancements, documentation, and tools necessary to utilize the source code):

BPro will comply with the escrow requirements. In other solutions we've used our TFS instance as the escrow and given access to approved personnel.

VIII. Tasks/Work Plan. Describe in narrative form your technical plan for accomplishing the work using the task descriptions as your reference point. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique (PERT) or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach.

A. Implementation Planning. The selected Offeror shall provide implementation planning services. Offeror shall submit a draft implementation plan with its proposal. The implementation plan shall include, at a minimum, the following;

1. Description of your implementation approach and plan
2. Specific summary of solution products and services to be utilized
3. Describe how the proposed products and services will meet the requirements of the RFP
4. project schedule and timeline, which must include major milestones and start/finish dates;
5. resource staffing plan indicating roles, responsibilities, when staff will be actively engaged on the project, percentage of their time that will be dedicated to the project;

6. Dependencies;
7. rolls and responsibilities (e.g., the Offeror, DOS, County Election Officials, etc.);
8. development and testing of interfaces;
9. solution security testing;
10. issue tracking process and log;
11. defect management;
12. quality assurance;
13. implementation schedule and dependencies;
14. knowledge transfer activities;
15. go & no-go criteria decision points; and
16. roll-back provisions;
17. and post-implementation review;
18. Project meetings and planning meetings.

The selected Offeror shall meet with the DOS to review the draft implementation plan and gather any additional details required to finalize an implementation plan. A finalized implementation plan shall be submitted to DOS within fourteen (14) calendar days of receiving the notice to proceed. A final plan, revised based on DOS feedback, shall be delivered to DOS within five (5) business days of receiving DOS feedback. The implementation plan shall be updated throughout the project as requested by DOS. The final implementation plan must be approved by the DOS.

Offeror Response

The draft implementation plan is included below.

1. Description of your implementation approach and plan

To complete Pennsylvania's TotalVote Project to the satisfaction of the stakeholders, BPro holds the following statement as the primary goal:

"First, to deliver maximum value to our customers while conducting business successfully under the current business rules and second to deploy a sound system foundation and architecture that allows for easy adoption of changing business needs and can easily conform to data sharing requirements necessary to add functionality in the future."

BPro's TotalVote Team has a track record of delivering successful projects on time and on budget, while working closely with our customers to provide them tremendous improvements in technology. The system architecture of TotalVote uses leading technologies available in the industry and is readily adaptive to new technology. Our team respects the requirement to "deliver maximum value to our customers while conducting business successfully…" knowing that successful elections must go on, even while large process changes are in play.

If selected, our project management and delivery methodology will be a collaborative approach with the Commonwealth of Pennsylvania's (PA) Department of State (DOS) and will build on three key ingredients:

- PMI based project management framework
- Agile and Iterative Approach to application development
- Continuous Stakeholder Engagement and Stakeholder satisfaction

The Project Management methodology used throughout the project will align with standards from the Project Management Institute (PMI), Project Management Body of Knowledge (PMBOK). BPro's project management team will work closely with the PA DOS TotalVote project management team during the initial project planning to develop an overall project plan which will form the basis for this project and will form the umbrella under which the software implementation takes place.

The methodology we propose for implementing this project mirrors closely that which was used for the New Mexico, Arizona, and Washington's projects with modifications based on the lessons learned from both projects. We present a hybrid project lifecycle that uses a combination of predictive and agile components. This model recognizes that software implementation projects contain both definable work (such as production rollout and training) and high-uncertainty work (such as new design and new features). The predictive and agile approaches are discussed in more detail below.

Predictive Approach

The characteristics of a predictive approach are fixed requirements (they do not change frequently) with activities that are performed once for the project in a single delivery. The activities are typically executed in a serial manner. The plans for these activities are living documents and progressively elaborated with detail as requirements and constraints are identified by the team. Our experience has taught us that upfront detailed planning that specify "what" to deliver and "how" works well in these situations.

To that end, the team will develop and use detailed plans and checklists to carry out data migration, architecture design/build, data interface design/build, transition to operations, training, and production rollout activities. Proposed project deliverables will include the following items:

- Data Migration and Conversion Plan
- Architecture Diagrams
- Transition to Operations checklist
- Training manual(s)
- Production Rollout checklist

For each of these areas, we envision specialty teams with members from both BPro and the PA DOS teams. The BPro team will allow developers who are actively working on software be focused on their construction work and not be active participants in the production planning until their development is completed.

Agile-Based Software Development Approach

The standard software development process at BPro is Agile. Their Agile-based approach follows the principle that the highest priority is to satisfy the customer through early and continuous delivery of working software. Software modules are built using an iterative sprint approach with frequent check-ins with the customer to validate the results. Sprints either two or three (2 or 3) weeks with a release at the end of the sprint prior to the sprint review. These timeframes may be adjusted depending on the project constraints and requirements. Prior to each sprint, the development team meets with the Product Owner (PA DOS's primary business owner) to decide what items to include in the next iteration and flesh out the detailed requirements and acceptance criteria for those items. Once work is completed by developers, the team and Product Owner (and other stakeholders) hold a review session to allow the Product Owner to provide feedback, identify bugs, and accept or reject the work. Following every other sprint, the development team will meet internally to identify areas of improvement for the next iteration, as well as identify those things that are working well. This meeting is referred to as a "retrospective" in agile parlance. The goal is to continuously improve the development team's delivery and performance.

Planning, communication, and coordination play pivotal roles in the success of this agile-based process, although it is done differently from the predictive approach. BPro carries out high level planning at the outset of the development process (for example, a work breakdown structure to view scope) with detailed planning done by the development team and Product Owner occurring during each sprint. Requirements refinements are detailed later than in a prescriptive model, that is, just before development. This "just in time" planning ensures requirements specifications are current and allows the developers to work while the specifications are still fresh in mind. The Product Owner has full authority and responsibility to prioritize business requirements according to their business value, set acceptance criteria, and help developers understand exactly what is needed. The acceptance criteria specified by the Product Owner will be the basis of building the component and equally the basis for the tests for that component to determine acceptance.

With a complex project of this scope, there will be changes as the system is built. BPro will incorporate changes as they are identified into the development process rather than viewing them as disruptive and unwelcome. BPro proposes the software requirements be broken into features based on major components with a formal review to occur after each module is delivered. During development within each sprint, quality will be baked in through the use of developer and business analyst (BA) testing of the software requirements along with the acceptance criteria as specified by the Product Owner. BPro will plan the UAT testing jointly with the PA DOS team to make sure it is a smooth and effective process.

Under the Agile umbrella, the TotalVote system is amenable to necessary changes that take advantage of technology opportunities to improve elections and to meet changing election mandates.

Detailed Requirements

BPro will provide a walk-through of the TotalVote software to the PA DOS team to demonstrate how the TotalVote software generally meets each requirement. However, a high-level demonstration will not capture hidden requirements, subtle gaps or changes that the Product

Owner may request later when the stated requirements are analyzed in depth during iteration reviews. Even those requirements marked as "ready out of the box" will undergo review and acceptance by the Product Owner during the testing events of the project. We have learned through experience that while a high-level demonstration is helpful in identifying some obvious gaps in functionality, it is not sufficient for customer acceptance. Missed requirements, design changes, and subtle gaps can best be discovered by examining each and every business requirement in depth and having the Product Owner provide the details and acceptance criteria for each.

While most of the requirements are met "out-of-the-box" in at least one of our six statewide implementations, PA DOS will have small variances that will require configuration. As members of the PA DOS know, no two state elections are exactly the same. BPro currently provides Voter Registration systems in Arizona, Hawaii, New Mexico, North Dakota, South Dakota, and Washington. Each project is very different due to unique customer requirements and state laws. South Dakota has been using their system since 2012, North Dakota went live in 2015, Hawaii in June 2017, New Mexico in December 2017, Washington in June 2019, and Arizona in November 2019. BPro works to deliver projects within the timeframe and budget in coordination with our clients. The relationships we have built with our clients continue to this day, and each successful partnership has led to an expansion to the scope of work of BPro's projects in each state. We are very proud of the relationships we have developed, and we plan to continue our partnerships as each state's needs evolve. We expect to develop a similar relationship with the PA DOS.

Customization Approach

Our proposal and pricing cover all requirements and customizations that are presented in the RFP. We are committed to delivering this application with every requirement in the RFP to be compliant with Commonwealth election laws and HAVA, regardless of the effort or hours it will take to do so. While we have developed most of your requirements in one of our other state implementations, the requirements we have marked as customization will require further development to satisfy your requirements that have not been implemented elsewhere. We have built customization time into our proposed project schedule.

While the actual amount of effort and hours needed for customization will be known after the requirements analysis phase, all current RFP requirements and their customized implementation as elaborated and documented in the requirements specification during the analysis phase, is covered within the proposed pricing and will be delivered as per the approved specifications at no extra cost.

Integration Assessment and Design

BPro will pair our subject matter experts (SMEs), who have been involved with every state implementation BPro has produced, with subject matter experts within PA DOS to assess the complexity of the data and protocols related to any interfaces required for the solution. We have tools (web services) and templates for field mapping, as well as protocols we will use to produce the interface design documents necessary to transfer the required information in and out of the system.

We will hold a series of meetings to identify the appropriate protocols, necessary data, and appropriate timing of any required data flows. One of the deliverables from these meetings will be the *E.1 Solution Interface and Design Document*. This document will be a specific set of plans, including a detailed analysis of the protocols, fields, and frequencies of all interfaces to and from the new TotalVote system and interfacing agencies.

Quality Assurance Approach

Our talented development team includes individuals that have implemented several elections related applications in numerous jurisdictions. This experience makes development of your SURE replacement product more effective and highly efficient. We focus on building quality applications and code from the beginning rather than testing the finished product to identify and fix the bugs within it. To ensure the quality of code propagation between environments, our team treats deployments as part of a development workflow, not as an afterthought.

BPro understands the importance of configuration management and version control in delivering large scale, mission critical applications like TotalVote. Hence, we implement industry standard best practices using Microsoft's proven configuration management suite, Team Foundation Server, popularly known as TFS. TFS provides source code management, version control, code branching, and automated code build functions that BPro leverages for release management and version control.

In addition to the capabilities of the tool, BPro has strict process discipline on who has access to different code branches and which personnel are authorized to build binary releases and package them for deployment. Prior to releasing a build, the following processes are strictly followed:

1. Development is done according to defined and approved requirements captured within TFS to meet the customer's needs.
2. All functionality is tested by our functional team to ensure it meets the intended requirement.
3. The scope of a release is discussed and agreed upon with the customer or their designated representative on our team (i.e., the project manager or functional manager).
4. All releases are subject to smoke testing prior to deployment and are first tested for regression and successful function by our development staff.
5. Comprehensive release notes are prepared and communicated to the receivers - both internal testers and customers, so that they know the content of the release and scope of their testing.
6. Branching of development releases, internal release, scheduled production releases, and emergency releases is strictly controlled.

The BPro project manager will ensure that the release numbering, management, and approval processes are defined, discussed, and approved with DOS early in the project and these established processes are followed throughout the project to ensure clean releases and good working applications during testing, user acceptance, and finally in production environments.

2. Specific summary of solution products and services to be utilized

While the TotalVote software delivers base functionality common across all customers, each feature is configurable to meet unique requirements of state and county customers across the country. The multitude of regulations regarding elections at the county, state, and federal levels demand this flexibility. We also customize our project management processes to fit with our customer's organizations. BPro will utilize proven solution products and services they have experience using on similar projects.

Solution Products

The solution products BPro plans to use are existing modules from our module library. The version of the base module will be chosen based upon the functionality which most closely fits the PA DOS's business requirements. The module will be customized to bridge any gaps found between the base functionality and the business needs of DOS.

The existing solution modules which will be evaluated for use in the PA DOS's project are:

- Voter Registration Management
- Election Management
- Candidate Management
- Ballot Creation
- Canvassing
- Scanning/Imaging
- Data Exchanges and Interfaces
- Voter Information Portal
- Election Night Reporting
- Point Addressing
- Campaign Finance
- Lobbyist Tracking

Development Tools

The development tools that BPro plans to use for this project include:

1) Microsoft Team Foundation Service (TFS) – industry leading service to track and manage code reviews. It will be used for managing software tasks (the "how" will we code) associated with business requirements (the "what" will we code) as well as for bug tracking and resolution. TFS will allow us to track business requirements and provide requirements traceability (RTM) from business requirements to software requirements.
2) Visual Studio 2019 - Microsoft SQL Server
3) Microsoft Office Products – The BPro scrum team will use Office products for creating workflow process diagrams and other supporting system documents.

Services

The services provided for the PA DOS TotalVote project will include BPro's project management services, development team services, and post-production customer service assistance. BPro provides these services to ensure the project is delivered to meet the business and technical needs of this RFP. The BPro scrum team will align with the PA DOS technical and business staff to deliver a quality replace for the legacy SURE system.

3. Describe how the proposed products and services will meet the requirements of the RFP

BPro's proposed solution for the Commonwealth of Pennsylvania's SURE replacement is BPro's TotalVote suite of products with complete features to cover every aspect of Voter Registration and Election Management. With BPro's combined experience providing Voter Registration, Election Management, Petition Management and Lobbyist Tracking systems, we have a full comprehension of the significance of the effort to manage voter registrations, and how thoroughly vetted, well-maintained voter records are an integral part of the overall success of every election. We integrate data across all TotalVote modules to provide seamless management of voter districts with Candidate Filing, Elections and Petition Management, Ballot Entitlement, Ballot Styles, Voter Engagement, and Election Night Reporting.

Election Management – TotalVote's EMS module is an intuitive, user-friendly system that is used by states and counties around the country to set up every aspect of an election. Many jurisdictions have made the switch from using the EMS system provided by their tabulation vendor and now use TotalVote EMS as their primary system for setting up elections. This is possible because TotalVote EMS is compatible with all the major tabulation systems and exports from TotalVote do not need to be manipulated before being exported to the tabulation vendor's system.

In TotalVote, the DOS can create a statewide election and define the election based on the type of election (primary, general, etc.), races on the ballot, districts, counties, and parties that are included in the election. Once the DOS has set up an election, authorized county users can further define local races that are part of a statewide election and manage the local portions of statewide elections. In addition, authorized county users can use TotalVote to create local-only elections and manage every aspect of them. TotalVote provides a comprehensive set of parameters to manage all details of any election. During the Requirements Analysis phase of the project, we expect to identify additional specific parameters needed for Pennsylvania.

Candidate Management - One of the primary components of the election management module of TotalVote is candidate management. Candidates can register in person or through TotalVote. As each candidate is certified, information is pulled from the voter registration record and linked to the appropriate contest. The Candidate Table contains all identifying information, including a unique Candidate ID Number.

Ballot Creation - Once the ballot definition information is entered into the system, TotalVote seamlessly creates every ballot style, automatically in a single step. TotalVote also builds ballots in multiple languages and is currently used by four states to build multilingual ballots in a combined five languages. A ballot style is created for every precinct part and duplicate ballot styles are combined and connected to all applicable splits. The system includes multiple safeguards for quality assurance by allowing the County to error check throughout the process. After the necessary ballot styles are determined, TotalVote presents sample ballots for review before releasing it to the printing vendor. TotalVote also indicates the number of ballots necessary for each precinct. Once the accuracy of ballot styles is verified, the file is exported for printing. At that point, sample ballots can be released to the public through the Public Portal.

TotalVote is currently available in five languages (in addition to English) around the country: Spanish, Chinese, Korean, Tagalog, and Vietnamese. The structure is in place for multiple languages so all that is needed is for the customer to provide the translation for each language your state needs to offer [see Section VI.QQ for a sample]. For example, Washington state voters can request to receive a ballot in over 20 languages. While the VoteWA system does not translate into all 20+ languages, voters can receive a ballot through the VoteWA system.

Canvassing - TotalVote's Election Canvassing module is used to provide election canvassing for all statewide and local elections. After the completion of the Election Night Reporting, the TotalVote canvassing module is utilized in the canvassing process at the State and County levels. After provisional ballots are processed, TotalVote automatically provides a canvassing report for the County Canvassing Board. No extra data entry is required because the data is pulled from the previously imported or entered returns data. PA DOS's canvassing system would include creation and customization of all necessary reports.

Scanning/Imaging - The scanning utility within TotalVote is used to create digital images of paper-based records, extract information from the images, and associate the information with the correct records stored in the system. Paper records are scanned by a commercial-off-the- shelf (COTS) digital scanner that creates a computer-based digital image of the document for storage in TotalVote. Depending on the form and content, information from the image is extracted using Optical Character Recognition (OCR) and Barcode decoding. Using information extracted from the image or through manually entered information by an operator, the images are "indexed". This means a digital image is assigned a numerical reference to associate it with a particular voter. Indexing allows the digital image to be stored and accessed from the voter record, which eliminates the need to store or manually retrieve paper records.

Voter Information Portal - TotalVote feeds the backend data for all Public Portal functions. When on the Public Portal, a public user can search for and interact with registration and election data in the TotalVote database. The Public Portal is accessible, easy to navigate, mobile-friendly, and can support multiple languages (currently TotalVote supports five languages). If a registered voter wants to specifically look up their own personal information, they would need to enter a few identifying factors, such as name, address, or date of birth to access their own record.

Election Night Reporting - TotalVote's Election Night Reporting system is compatible with all major tabulation systems and results are updated automatically when a vote tabulator file is

uploaded into TotalVote. Web visitors will be able to navigate a map of the Commonwealth of Pennsylvania and drill down to view results and voter turnout by State, County, Congressional District, Legislative District, Senatorial District, School District, Tax District, and Precinct (if available) from any device. TotalVote also flags possible recounts for any of the reported contests based on Pennsylvania's statutes.

Point Address Data - BPro has spent a considerable amount of time over the last six years analyzing the integration architecture for incorporating GIS functionality into voter registration processes and functions. Careful consideration is required to ensure customer acceptance, flexibility to accommodate changes or updates, and maintainability over extended product life. This analysis was performed with the fundamental requirements for voter registration at its core rather than trying to tailor voter registration to fit GIS. BPro believes the result of this analysis has yielded a well-designed architecture for incorporating GIS functionality into voter registration processes and brings considerable improvements in efficiency and accuracy when implementing TotalVote as the new Pennsylvania voter registration solution.

Our approach is based on several relevant customer and industry factors that are listed below:

- Voter Registration department employees are NOT GIS software operators. In the rare instance the Voter Registration department has a skilled GIS operator, our approach takes full advantage of the resource.
- Most jurisdictions that are interested in integrating GIS functions with Voter Registration systems have a GIS department or group, whether at the State or County level.
- For jurisdictions that do not have a GIS department or group, GIS support can be provided by a third-party service bureau, either by a private or public entity.
- The most prevalent GIS software used by States or Counties is the ESRI product suite, but other products are supported. Existing software licenses can be leveraged to minimize implementation expense.
- GIS-based maps and layers required for integration with Voter Registration (VR) do not change often so GIS software skills are needed infrequently.
- GIS and Voter Registration products have different revision and update cycles so need to function through defined interfaces that allow the products to be updated independently of one another.
- Address maintenance and precinct assignment are the primary functions of VR/GIS integration.

Embracing these relevant factors, BPro has developed a robust, near and long-term solution for VR/GIS functionality. BPro has developed a standalone software product for managing point address data that has the capability of obsoleting the historical, error prone street index file. Our standalone VR/GIS solution sits between GIS software products and TotalVote. BPro's GIS software product provides the functions necessary to maintain point address data and accommodates changes over time from both GIS data and Voter Registration requirements. Our product provides interfaces to ingest GIS data and services, present the information to VR operators in an understandable user interface and supports address maintenance required for

management of voter registration rolls over time. VR operators are NOT required to be skilled GIS operators but only require typical office-type computer user skills.

To take advantage of existing GIS infrastructure, minimize implementation expense, maintenance and VR operator skills, all GIS map layers used by our solution are built externally. This can be performed by a variety of resources, including a VR department GIS operator, a County or State level department or group, a service provided by BPro, or an independent third-party provider. Constructed map layers are imported into our GIS solution where they are stored and maintained under revision control. Using Open Source map display tools, our solution allows users to turn on/off map layers with simple menu selections to present simultaneous layer display to accomplish the task at hand. This approach eliminates the costly licensing fees, hardware infrastructure, and operator expense of GIS software for the VR department.

To initialize our solution with point address data, our recommendation is to purchase commercially available point address data from a third-party provider, which typically provides over 90% match rate when compared to the existing street index and the remaining address require review by VR officials. Only address points are used to simplify the data management. Any area that does not have geolocated points (measured locations), uses geocoded points that are estimated locations along a street segment. These spatially located geocoded points are tracked by our solution to provide a vast improvement over street index ranges and can be upgraded to geolocated points over time. Upgraded geocoded points can originate from updates to the commercial data source, local GIS departments, and even measurements performed by the VR department using a handheld device. Our solution provides a means for VR operators to compare an existing point to a new point and determine the best representation for VR purposes. This approach supports jurisdictions with sophisticated GIS operations and jurisdictions with no GIS background. TotalVote continues to provide support for the traditional street index file but also conversion to a point address system at any time into the future, which matches the potential environment in Pennsylvania. Our architecture will support counties that have already integrated with a GIS system, allow other counties to upgrade to a point address solution as part of the new system implementation, or support street file management that can be upgraded in the future at the county's option.

As part of the initialization process, address validation is performed against the existing addresses stored by the VR system. A comparison report is generated that lists the discrepancies between the point address data and the addresses on file. The discrepancies are resolved by VR operators by updating the point address with any missing addresses, creating alias street names that are linked to the primary name, identifying business addresses and creating points or areas that are valid registration locations but do possess traditional address references. An example of the latter is where a homeless citizen claims a resident location, our solution allows a VR administrator to add a point and treat it like any other address. This capability can also be used when other address questions arise to provide flexibility in the face of exceptions giving complete control over address management.

TotalVote's GIS software can integrate with existing addressing solutions at either the County or State level. In order to optimize the integration, a system analysis is required that accounts

for the existing workflows of the existing addressing system, data maintenance, and user requirements. With BPro's background in addressing systems, the integration architecture can be mapped out in a simple, straightforward method that all parties can approve to arrive at the most efficient integration. This effort would be performed as part of the Gap Analysis period of the implementation project.

Campaign Finance – Benefits from using BPro's Campaign Finance system can be realized by political parties, candidates, organizations, and the general public by utilizing useful tools for filing and viewing campaign finance information. This effective solution securely records and searches for campaign and PAC income, expenses, contributions, and loans in a user-friendly system that will also help candidates and political parties meet campaign finance reporting deadlines.

While deploying TotalVote's Campaign Finance System, great care will be taken to not only construct a complete application that meets the Commonwealth of Pennsylvania's laws, but also include helpful user functions for committee data management.

TotalVote reduces the time it takes campaigns to track down and fill out paper campaign reports and offers a complete web-based system that organizes and distributes desired forms online. As soon as data is entered into the system, TotalVote Campaign Finance accurately places the data into the online form. Once online, all campaign finance forms are easily retrieved when searching for a form.

TotalVote's Campaign Finance system reduces the burden of campaign finance filing for political parties, candidates, and organizations, while providing a greater level of transparency for the general public.

BPro Services – The services provided for the PA DOS TotalVote project will include BPro's project management services, development team services, and post-production customer service assistance. BPro will serve as the sole point of contact for the implementation of the TotalVote system. Services will be provided as outlined in the contract terms.

Development Platform - TotalVote is a modern, robust, browser-based application developed on the Microsoft .NET Framework platform using Microsoft SQL Server database. TotalVote is a top-down solution using a centralized statewide database for all modules. TotalVote can run in many environments utilizing Microsoft SQL Server (2016 Standard or newer preferred) and Windows Server. We do not need any additional equipment to what is currently in the DOS environment.

4. Project schedule and timeline, which must include major milestones and start/finish dates

The high-level draft WBS that shows overall execution of the PA DOS TotalVote is outlined below. The WBS will be updated and refined during the project planning phase at the beginning of the project.

Work Breakdown Structure (WBS)

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Pennsylvania DOS TotalVote Project**	**463 days**	**Mon 3/2/20**	**Tue 12/28/21**		
2	**Project Kick-off Meeting**	**8 days**	**Mon 3/2/20**	**Wed 3/11/20**		
3	Schedule Project Kick-off Meeting	2 days	**Mon 3/2/20**	Tue 3/3/20		BPro PM
4	Conduct Project Kick-off Meeting	1 day	Wed 3/11/20	Wed 3/11/20	3FS+5 days	BPro PM
5	**Project Management**					
6	*Deliverable B.1: Weekly Status Report*	*455 days*	*Mon 3/9/20*	*Wed 12/22/21*	*3FS+3 days*	BPro PM
7	Project Status Meetings	455 days	Mon 3/9/20	Wed 12/22/21	3FS+3 days	BPro PM
8	*Deliverable B.2: Submit Final Implementation Report*	*3 days*	*Thu 12/23/21*	*Tue 12/28/21*	*6*	BPro PM
9	**Project Initiation**	**6 days**	**Mon 3/2/20**	**Mon 3/9/20**		
10	Establish Project Stakeholders	0.5 days	Wed 3/4/20	Wed 3/4/20	3	BPro PM
11	Establish Project Team	0.5 days	Wed 3/4/20	Wed 3/4/20	10	BPro PM
12	Establish Project Team Roster	0.5 days	Thu 3/5/20	Thu 3/5/20	11	BPro PM
13	Establish Core Team Members	0.5 days	Thu 3/5/20	Thu 3/5/20	12	BPro PM
14	Establish Requirements Analysis Schedule	3 days	Fri 3/6/20	Tue 3/10/20	13	BPro PM
15	Communicate Schedule to Core Team	1 day	Wed 3/11/20	Wed 3/11/20	14	BPro PM
16	**Project Planning**	**239 days**	**Mon 3/2/20**	**Tue 2/9/21**		
17	**Project Management Plans**	**45 days**	**Mon 3/2/20**	**Fri 5/1/20**		
18	*Deliverable A.1: Finalized Implementation Plan*	10 days	Mon 3/2/20	Fri 3/13/20		BPro PM

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
19	Develop Project Schedule	5 days	Mon 3/2/20	Fri 3/6/20		BPro PM
20	**Develop Project Management Plan (PMP)**	**35 days**	**Mon 3/16/20**	**Fri 5/1/20**	**18**	
21	Develop Requirements Management Plan	5 days	Mon 3/16/20	Fri 3/20/20	15	BPro PM
22	Develop Risk Management Plan	5 days	Mon 3/23/20	Fri 3/27/20	21	BPro PM
23	Develop Issue Management Plan	5 days	Mon 3/30/20	Fri 4/3/20	22	BPro PM
24	Develop Change Control Management Plan	5 days	Mon 4/6/20	Fri 4/10/20	23	BPro PM
25	Develop Communications Management Plan	5 days	Mon 4/13/20	Fri 4/17/20	24	BPro PM
26	Develop Quality Management Plan	5 days	Mon 4/20/20	Fri 4/24/20	25	BPro PM
27	Develop Time Management Plan	5 days	Mon 4/27/20	Fri 5/1/20	26	BPro PM
28	**Requirements Analysis and Specifications**	**33 days**	**Mon 3/2/20**	**Wed 4/15/20**		
29	Requirements Gap Analysis to TotalVote Baseline	10 days	Thu 3/12/20	Wed 3/25/20	15	BPro Team, PA DOS
30	Enter user stories into TFS	10 days	Mon 3/2/20	Fri 3/13/20		BPro BA
31	*Deliverable C.1: Finalized Requirement documents*	*5 days*	*Thu 4/9/20*	*Wed 4/15/20*	*33*	BPro BA
32	*Deliverable C.2: Requirements Traceability Matrix*	*5 days*	*Thu 3/26/20*	*Wed 4/1/20*	*29*	BPro BA
33	*Deliverable C.3: GAP analysis document*	*5 days*	*Thu 4/2/20*	*Wed 4/8/20*	*32*	BPro BA
34	**Infrastructure - Configuration of Environments**	**80 days**	**Tue 3/10/20**	**Tue 6/30/20**		
35	Configure and Set-up Development Environment	10 days	Tue 3/10/20	Mon 3/23/20	9	BPro Dev Team
36	*Deliverable D.1: Submit Configuration Confirmation Report - Development*	*5 days*	*Tue 3/24/20*	*Mon 3/30/20*	*35*	BPro PM
37	Configure and Set-up Staging Environment	10 days	Tue 4/7/20	Mon 4/20/20	36FS+5 days	BPro Dev Team
38	*Deliverable D.1: Submit Configuration Confirmation Report - Staging*	*5 days*	*Tue 4/21/20*	*Mon 4/27/20*	*37*	BPro PM
39	Configure and Set-up Production Environment	10 days	Tue 5/5/20	Mon 5/18/20	38FS+5 days	BPro Dev Team

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
40	*Deliverable D.1: Submit Configuration Confirmation Report - Production*	*5 days*	*Tue 5/19/20*	*Tue 5/26/20*	*39*	BPro PM
41	Configure and Set-up Disaster Recovery Environment	10 days	Wed 6/10/20	Tue 6/23/20	40FS+10 days	BPro Dev Team
42	*Deliverable D.1: Submit Configuration Confirmation Report - Disaster Recovery*	*5 days*	*Wed 6/24/20*	*Tue 6/30/20*	*41*	BPro PM
43	*Deliverable E.1: Solution Interface and Design Document*	***20 days***	*Mon 3/16/20*	*Fri 4/10/20*	*30*	BPro Product Manager, BPro BA
44	**Software Development Life Cycle (SDLC) Plans**	**309 days**	**Thu 4/16/20**	**Wed 7/7/21**		
45	*Deliverable G.1: Develop Test Plan*	*10 days*	*Thu 4/16/20*	*Wed 4/29/20*	*28*	BPro PM
46	*Deliverable G.1: Develop Test Scenarios*	*10 days*	*Tue 6/22/21*	*Wed 7/7/21*	*127SF*	*BPro BA*
47	*Deliverable H.1: Develop Data Migration, Conversion, and Validation Plan (See Data Conversion Block for the map)*	*10 days*	*Thu 4/30/20*	*Wed 5/13/20*	*45*	*BPro PM*
48	*Deliverable K.1: Develop Configuration and Release Management Plan*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	*BPro PM*
49	**Transformation Management Plans**	**20 days**	**Thu 5/14/20**	**Thu 6/11/20**		
50	*Deliverable I.1: Develop COOP/Disaster Recovery Plan*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	BPro PM
51	*Deliverable J.1: Develop Training Plan*	*10 days*	*Fri 5/29/20*	*Thu 6/11/20*	*50*	BPro PM
52	**Data Conversion and Validation**	**336 days**	**Tue 3/10/20**	**Tue 7/6/21**	**9**	
53	**Initial Data Collection and Clean-up**	**55 days**	**Tue 3/10/20**	**Tue 5/26/20**		
54	Get Initial Datasets from PA DOS & Counties	15 days	Tue 3/10/20	Mon 3/30/20		PA DOS PM
55	Data Staging, Analysis	10 days	Tue 3/31/20	Mon 4/13/20	54	BPro SQL DBA
56	Data Clean-up with Counties and DOS	20 days	Tue 4/14/20	Mon 5/11/20	55	BPro SQL DBA,PA DOS
57	Analysis and Clarification Sessions	20 days	Tue 4/14/20	Mon 5/11/20	55	BPro SQL DBA
58	Document Clarifications	10 days	Tue 5/12/20	Tue 5/26/20	57	BPro SQL DBA
59	**Data Migration and Conversion**	**336 days**	**Tue 3/10/20**	**Tue 7/6/21**		

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
60	*Deliverable H.1: Develop Data Mapping and Translation Documents (Data Dictionary)*	*10 days*	*Wed 5/27/20*	*Tue 6/9/20*	*58*	BPro SQL DBA
61	*Deliverable H.2: Develop Data Conversion Schedule*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	BPro PM
62	Data Migration and Conversion - Dev Environment	5 days	Wed 6/10/20	Tue 6/16/20	60	BPro SQL DBA
63	Data Migration and Conversion - Staging Environment	5 days	Wed 6/17/20	Tue 6/23/20	37,62	BPro SQL DBA
64	*Deliverable H.3: Submit Final Conversion Test Results (After success conversion to Test) Translation Documents (Data Dictionary)*	5 days	Tue 3/10/20	Mon 3/16/20		BPro PM
65	Data Migration and Conversion - Production Environment	5 days	Tue 6/15/21	Mon 6/21/21	39,64,115	BPro SQL DBA
66	Data Migration and Conversion - Disaster Recovery Environment	5 days	Tue 6/22/21	Mon 6/28/21	41,65	BPro SQL DBA
67	*Deliverable H.3: Submit Final Conversion Test Results (After success conversion to Disaster Recovery) Translation Documents (Data Dictionary)*	5 days	Tue 6/29/21	Tue 7/6/21	66	BPro PM
68	**Development Construction & Customization**	**280 days**	**Wed 6/17/20**	**Mon 7/26/21**	**35,62**	BPro Dev Team
124	*Deliverable F.1: Fully Configured Solution and Interfaces*	*5 days*	*Tue 7/27/21*	*Mon 8/2/21*	*68*	BPro PM
125	**Training**	**65 days**	**Tue 6/15/21**	**Wed 9/15/21**		
126	Update Training Plan	5 days	Tue 6/15/21	Mon 6/21/21	115	BPro PM
127	Create Training Materials	25 days	Wed 7/7/21	Tue 8/10/21	118	BPro BA
128	*Deliverable J.2: Provide Training Documentation & Materials*	*5 days*	*Wed 8/11/21*	*Tue 8/17/21*	*127*	BPro BA
129	Coordinate Training Locations, Schedule, and Organization	5 days	Tue 6/22/21	Mon 6/28/21	126	BPro PM
130	*Deliverable J.4: Conduct DOS User Training Sessions*	*5 days*	*Wed 8/18/21*	*Tue 8/24/21*	*127FS+5 days*	BPro BA
131	*Deliverable J.3: Conduct County User Training Sessions*	*10 days*	*Wed 9/1/21*	*Wed 9/15/21*	*130FS+5 days*	BPro BA
132	**User Acceptance Testing (UAT) #1**	**10 days**	**Thu 9/16/21**	**Wed 9/29/21**		
133	UAT Testing Support	5 days	Thu 9/16/21	Wed 9/22/21	131	BPro Team
134	Prepare UAT Results and Completion Report	5 days	Thu 9/23/21	Wed 9/29/21	133	BPro PM

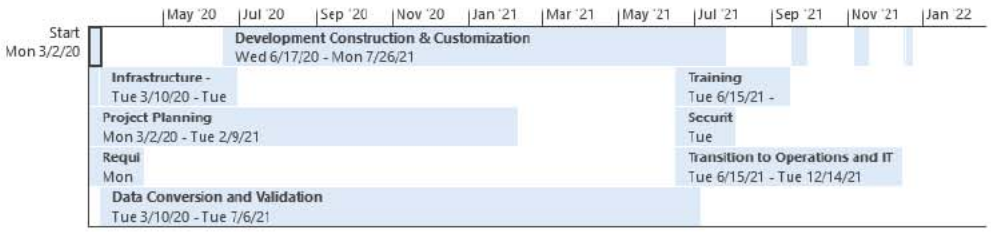
	Task Name	Duration	Start	Finish	Predecessors	Resource Names
135	Incorporate UAT Test Feedback into TotalVote	10 days	Thu 9/30/21	Wed 10/13/21	132	BPro Dev Team
136	**User Acceptance Testing (UAT) #2**	**10 days**	**Fri 11/5/21**	**Thu 11/18/21**		
137	UAT Testing Support	5 days	Fri 11/5/21	Thu 11/11/21	135	BPro Team
138	Prepare UAT Results and Completion Report	5 days	Fri 11/12/21	Thu 11/18/21	137	BPro PM
139	Incorporate UAT Test Feedback into TotalVote	10 days	Fri 11/19/21	Mon 12/6/21	136	BPro Dev Team
140	**Documentation**	**347 days**	**Mon 3/2/20**	**Tue 7/13/21**		
141	Prepare Interface and Service Diagram	5 days	Mon 3/2/20	Fri 3/6/20		BPro Product Manager
142	Prepare database model and schema for core tables	5 days	Tue 6/22/21	Mon 6/28/21	141,146	BPro SQL DBA
143	Prepare high-level security architecture diagram	5 days	Tue 6/29/21	Tue 7/6/21	142	BPro Product Manager
144	Prepare application architecture diagram	5 days	Wed 7/7/21	Tue 7/13/21	143	BPro Product Manager
145	**Security and IT Policy Compliance**	**35 days**	**Tue 6/15/21**	**Tue 8/3/21**		
146	Prepare Security Design Checklist	5 days	Tue 6/15/21	Mon 6/21/21	115	BPro Product Manager
147	Provide Application Security Assessment Support	10 days	Tue 6/22/21	Tue 7/6/21	146	BPro Product Manager
148	Collaborate with PA DOS IT to evaluate and prioritize security vulnerabilities	20 days	Wed 7/7/21	Tue 8/3/21	147	BPro Product Manager
149	Provide documentation of security coding practices	5 days	Wed 7/7/21	Tue 7/13/21	147	BPro Product Manager
150	***Deliverable L.1: Provide Stress and Load Testing Support***	***5 days***	***Thu 9/30/21***	***Wed 10/6/21***		
151	Load and Stress Test Readiness	5 days	Thu 9/30/21	Wed 10/6/21	132	BPro Dev Team
152	**Transition to Operations and IT Training**	**127 days**	**Tue 6/15/21**	**Tue 12/14/21**		
153	**Deployment Readiness**	**127 days**	**Tue 6/15/21**	**Tue 12/14/21**		
154	Update Implementation and Deployment Plan	25 days	Tue 6/15/21	Tue 7/20/21	115	BPro PM
155	Prepare User Documentation	20 days	Wed 8/18/21	Wed 9/15/21	128	BPro Product Manager

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
156	Conduct Implementation Readiness Checks	10 days	Fri 11/19/21	Mon 12/6/21	132,136	BPro Product Manager
157	Prepare Systems Operations Documentation	30 days	Thu 9/16/21	Wed 10/27/21	155	BPro Product Manager
158	Conduct training to state technical staff	2 days	Thu 10/28/21	Fri 10/29/21	157	BPro Product Manager
159	Perform tasks in transitions to operations checklist	1 day	Tue 12/7/21	Tue 12/7/21	156	BPro Product Manager
160	*Deliverable K.2: Submit Final Release Package*	*5 days*	*Wed 12/8/21*	*Tue 12/14/21*	*159*	BPro Product Manager
161	**Production Deployment**	**2 days**	**Wed 12/15/21**	**Thu 12/16/21**		
162	Review production readiness checklist	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
163	Data cut-over from legacy system	1 day	Wed 12/15/21	Wed 12/15/21	153	PA DOS
164	Production Data Conversions	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro SQL DBA
165	Production Application Cutover	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
166	County and State Testing of Implemented Sites	1 day	Thu 12/16/21	Thu 12/16/21	165	PA DOS
167	**Project Closeout**	**5 days**	**Fri 12/17/21**	**Thu 12/23/21**		
168	Prepare and Process Project Closeout Checklist	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Product Manager
169	Update all system documentation for project closeout	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
170	*Deliverable H.4: Submit Final Conversion Report*	*1 day*	*Fri 12/17/21*	*Fri 12/17/21*	*161*	BPro PM
171	Complete warranty and transition to maintenance and operations	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
167	Go-Live Support	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Dev Team
168	**Project Closeout**	**5 days**	**Fri 12/17/21**	**Thu 12/23/21**		
169	Prepare and Process Project Closeout Checklist	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Product Manager
170	Update all system documentation for project closeout	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
171	*Deliverable H.4: Submit Final Conversion Report*	*1 day*	*Fri 12/17/21*	*Fri 12/17/21*	*161*	BPro PM

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
172	Complete warranty and transition to maintenance and operations	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
173	**Maintenance and Support Annual Tasks**	**1 day**	**Mon 12/27/21**	**Mon 12/5/24**	**168**	
174	Application Stabilization Support	4 weeks	Mon 12/27/21	Mon 1/24/22	167	BPro Dev Team
175	Enter maintenance period	0 days	Sat 1/1/22	Sat 1/1/22		
176	Provide maintenance and release schedule in early January	5 days	Wed 1/5/22	Tue 1/11/22		BPro Product Manager
177	Update COOP/Disaster Recovery Plan	5 days	Thu 12/1/22	Wed 12/7/22		BPro Product Manager
178	Provide maintenance and release schedule in early January	5 days	Thu 1/5/23	Wed 1/11/23		BPro Product Manager
179	Update COOP/Disaster Recovery Plan	5 days	Fri 12/1/23	Thu 12/7/23		BPro Product Manager
180	Provide maintenance and release schedule in early January	5 days	Fri 1/5/24	Thu 1/11/24		BPro Product Manager
181	Update COOP/Disaster Recovery Plan	5 days	Sun 12/1/24	Thu 12/5/24		BPro Product Manager
182	**Non-MVP Project Work Placeholder (Start Date and Duration will be coordinated with PA DOS PM)**	TBD	2022	2022	168	BPro Dev Team

Timeline

The timeline of the main portion of the project excluding the maintenance years is as shown:



Any tasks identified during the development construction phase of the project which are not considered to be part of the minimum viable product (MVP) will be moved to a non-MVP project work placeholder block. This work will be done after the project has been moved to production. The 2022 start date and duration of this placeholder block will be determined at the beginning of the project and adjusted prior to the end of the project to fit the business needs of PA DOS and their 2022 schedule.

5. Resource Staffing Plan Indicating Roles, Responsibilities, When Staff Will Be Actively Engaged on The Project, Percentage of Their Time That Will Be Dedicated to The Project

BPro, Inc. will staff the project with adequate resources to complete the project within the agreed upon timelines associated with this project.

The PA DOS will provide adequate staff to support this project. PA DOS will coordinate with state, county, and any other key external resources to assist with testing the system within the designated testing timeframes of this project.

BPro Staff, Roles and Responsibilities

Project Role		Responsibilities	Percentage of Time Dedicated to Project
BPro Project Manager	Kari Stulken (Key Personnel)	• Project Manager for the project from BPro. • Responsible for managing all project management tasks, scheduling, and communication regarding the project. • Develop and maintain Project Plan documents and Project Schedule in collaboration with the DOS PM. • Coordinate with the DOS PM for deliverable walkthroughs, demonstrations, testing, and approval processes. • Manage BPro resources for production of deliverables. • Ensure delivery of deliverables as per project schedule. • Serve as the Scrum Master.	• 100%
BPro Account Manager	Kari Stulken (Key Personnel)	• Serve as the single point of contact for the Commonwealth. • Serves as BPro's Project Contract Manager. • Ensure effective communication and coordination of releases and upgrades to the solution.	• 25%
BPro Solutions Architect (Product Manager)	Kevin Kumpf (Key Personnel)	• Provide technical expertise in the design and architecture of the solution. • Design the solution architecture for the businesses.	• 75%

		• Ensure compliance to solution architectural design in the implementation of the project. • Provide architectural guidance to the project team. • Explain technical issues and IT solution strategies to stakeholders and other IT professionals. • Keep an accurate record of materials used, expected deliverables, and milestones achieved. • Ensure that solution milestones are accomplished on time and within budget. • Ensure that solution architecture (software and programs) are designed in sync with the needs of the business and the business's hardware. • Review the proposal of vendors and suppliers to ensure that quality inputs are delivered at the least possible cost. • Monitor the activities of external developers on IT solution projects. • Identify and mitigate existing business risks associated with solution architecture.	
BPro Testing Lead	Laura Heckmann (Key Personnel)	• Define, plan, and coordinate all types of testing. • Identify, plan, and manage test resources, tasks, activities, issues, and risks throughout the project's software development lifecycle. • Document and manage risks and issues related to testing and ensure defects are properly documented and tracked to closure. • Create comprehensive project test plan to ensure the system meets all approved requirements.	• 50%
BPro Business Analyst Lead	Dakota Bixler (Key Personnel)	• Analyze user stories to support Sprint planning and development efforts. • Act as the liaison among stakeholders in order to understand the structure, policies, and operations of the entities. • Recommend solutions that enable the PA DOS to achieve its goals. • Work with other assigned staff to gain general familiarity with overall systems functions and analyze defects and requests for change.	• 100%

		• Provide general and technical design guidance and assistance.	
BPro Technical Lead	Joe Faddoul (Key Personnel)	• Responsible for ensuring that all technical aspects of the projects are addressed. • Responsible for all technical design. • Oversees implementation of the designs. • Provide general and technical design guidance and assistance. • Develops technical documentation. • Help the DOS PM assess BPro's technical capabilities in implementing the proposed architecture and technical solution and supporting it post implementation. • Ensure BPro implements the required configuration and staging environments. • Oversee delivery of hosting, platform, and system interfaces in accordance with requirements and design. • Oversee system configuration, unit, and integration testing deliverables submissions and provide approval. • Oversees BPro work relating to technical aspects of implementation and testing. • Provide inputs into technical knowledge transfer and mentoring as applicable.	• 25%
BPro Training Lead	Dakota Bixler (Key Personnel)	• Coordinate all training requirements and tasks. • Interact with project and program staff to understand the business area, such as participating in design and development. • Develop training materials. • Assist with scheduling training. • Provide recommendations on training rooms and equipment. • Develop individual training or knowledge transfer plans. • Create, distribute, collect, and review training or mentoring session feedback. • Modify training materials as appropriate. • Maintain quality service by establishing and enforcing organization standards. • Design system training manuals or supporting solution documentation by identifying and describing information needs, submitting initial versions for DOS review, and revising and editing the final copy of the training materials.	• 25%

BPro Developers	Staff Developers	• Responsible for executing tasks and producing deliverables as outlined in the RFP.	• N/A

Human Resources

While our team members are highly skilled and bring solutions ready to delivery, the PA DOS TotalVote Project requires participative leadership from the Department of State's Team to implement the solution in a manner that has buy-in from DOS and county staff and fits your business process. Especially during the development phases, development team members and the DOS business experts will communicate regularly regarding business requirements ("stories" in Agile parlance) details, prioritization of work items, and acceptance criteria. Developers will check in frequently with the Product Owner to make sure they are meeting the Product Owner's expectations. This feedback loop is the key to making sure BPro delivers value early and also gives DOS the ability to view progress often and gain confidence in the team's ability to deliver what is needed.

BPro looks forward to the opportunity to work with the PA DOS staff to bring technology improvements to your elections mission. BPro is prepared for the PA DOS Team to actively participate in planning, requirements analysis and specifications, requirements prioritization, release planning, acceptance criteria specification, sprint reviews, and acceptance testing. At the same time, we understand that DOS and county staff have limited availability

Our proposed project leadership team has experience in delivering large technology changes to elections including Voter Registration and Election Management, Election Night Reporting (ENR), Campaign Finance, Candidate Filing, and online public services for our citizens and we stand committed to quality deliveries to our clients.

In addition to the key personnel outlined in the previous section, the following disciplines are supported by senior level resources that will lead key support areas:

- ***Database Analyst (DBA):*** The DBA will work with the PA DOS DBA to create processes for transfer of Pennsylvania's VR and election data and images to TotalVote. Duties include map fields, create extract, transmit and load procedures (ETL), and coordinate with Bas and QAs for data integrity and quality standards.
- ***System Analyst (SA):*** The SA has extensive domain knowledge (i.e. elections) and prior experience of implementing similar systems, plus the technical design understanding and implications of implementing various features and functions in the system. BPro's SA understands how to design application functionally and technically and will work with the subject matter experts on how to best design the PA DOS TotalVote application for the Commonwealth of Pennsylvania's needs.
- ***Systems Engineers:*** BPro's system engineers will lead activities for installation and implementation of system and network infrastructure components meeting security and configuration standards.

6. Dependencies

Dependencies to the project include the following:

- Having clear requirements at the beginning of the project or refined prior to the development sprint they are taken into for construction.
- The development and test environments are set up and ready for the first development sprint.
- The data to be converted and migrated for the project is ready at the beginning of the project so it can be tested and reviewed throughout the course of the project.
- The award and contracting tasks are concluded in early 2020 so the project can start as close as possible to March 2, 2020.

The project schedule was organized so that information can be gathered during the requirements validation and analysis tasks not only for the requirements included in the RFP but also the standard terms can be identified. There will be a development sprint 0 iteration included in the development construction block so that the TotalVote screens can be updated with the standard terms Pennsylvania uses along with adding any additional fields critical to the system. The data conversion process will start prior to the development tasks so that the Pennsylvania data can be used for initializing the system. It is generally preferred by our clients to see their own data in the TotalVote system instead of mocked up voter records.

7. Roles and Responsibilities (e.g., the Offeror, DOS, County Election Officials, etc.)

BPro's roles and responsibilities were detailed above in *Section 5 of the Implementation Plan*.

DOS and County Election Officials Staff, Roles, and Responsibilities

Project Role		Responsibilities
Project Sponsor	Kathy Boockvar, Secretary of Department of State	• Executive Sponsor
Project Director	TBD (Key Personnel)	• Executive Project Director • Final decision-making authority for DOS for all project issues. • Overall responsibility for success and execution of the project for DOS. • Project Contract Manager.
Product Owner	TBD (Key Personnel)	• Gives overall guidance and direction for the project.

		• Provides technical assistance and guidance for IT security and IT infrastructure. • Responsible for detail and acceptance criteria for all requirements of the project.
DOS Project Manager	TBD (Key Personnel)	• Serves as DOS Project Manager for the project. • Responsible for managing DOS project management tasks, scheduling, and communication regarding the project. • Works with BPro PM to review and approve project plan documents and project schedule. • Coordinate with the BPro PM for deliverable walkthroughs, demonstrations, testing, and approval processes. • Manages DOS and County Election Administrator resources for input and collaboration on the various project deliverables • Reviews, approves, and accepts project deliverables in coordination with Project Director. • Ensure delivery of BPro deliverables are per project schedule and contract. • Oversees and direct DOS business analysts. • Makes day-to-day decisions on the project regarding tasks, schedule, and coordination of resources.
DOS business analysts	TBD (Key Personnel)	• Assists with DOS project deliverables and responsibilities • Helps gather, review, clarify, and document functional requirements to implement the BPro TotalVote Software and System. • Provides other project assistance as required.
DOS Technical Lead	TBD	• Overall coordination of IT for DOS.
County Election Administrators User Group	TBD	• Subject Matter Experts. • Assists with testing of user story functionality. • Participates in user acceptance testing events. • Provides feedback to DOS PM on system testing results.

8. Development and Testing of Interfaces

BPro has helped Arizona, Hawaii, New Mexico, North Dakota, South Dakota, and Washington increase the efficiency of their voter registration process by developing interfaces to other federal and state agencies that generate important data for maintaining accurate voter registration rolls. As technologies have advanced and government agencies have replaced their legacy systems with more modern Information Technology architecture, BPro has developed more and more efficient data sharing protocols that enable greater efficiency for the management of external data. Through our proven experience, BPro has the expertise necessary to take advantage of new state and federal interfaces as new systems continue to become available.

Interfaces are built using a team approach with the team members from Commonwealth of Pennsylvania's DOS and BPro technical resources. BPro uses standard web services to communicate with other entities. This approach provides a secure, well-known, and flexible means of exchanging information. BPro has built interfaces with a wide variety of federal and state-based systems that help verify voter information, create and print ballots, and record and report election results. Listed below are some of the interfaces implemented in TotalVote in various jurisdictions. This list continues to grow as new systems become available.

On the federal/national level, TotalVote currently integrates with:

- USPS and National Change of Address (NCOA) information through Melissa Data
- American Association of Motor Vehicle Administrators (AAMVA) and Social Security Administration (SSA)
- Electronic Registration Information Center (ERIC)
- Cross Check
- VIP 5.1 Specification

On the state and county level, TotalVote integrates with:

- Point addressing and district data
- Department of Health/Vital Records (Deaths)
- Department of Corrections
- Department of Motor Vehicles
- Statewide Voter Records
- Online Voter Registration
- Ballot Printers, Sorters and Tabulators
- Electronic Pollbook systems

BPro will work in concert with the PA DOS technical team to develop an interface plan that will describe the current interfaces and to-be interfaces. The plan will include a testing strategy.

Attribute Listing for Current and To-Be Interfaces:

A. Interface Protocol (web service, file)
B. Source/Target Identification (Description)
C. Security Requirements
D. Frequency
E. Rules for record rejection (if applicable)
F. Alerts/notifications when service not available or file transfer fails (for example, email notification, home queue item)
G. External Implementation Needs (for example, existing interface code, firewall port information, technical specifications from each tabulation vendor)
H. Dependencies (for example: internet connectivity, databases up and running)
I. Detailed Testing Procedures – operational and functional tests
J. Action (keep as is, modify, build, retire)

Interfaces will be developed during the development construction and customization phase of the TotalVote project. Those identified to be in scope of this project include the following:

- Lobbying Disclosure System
- Campaign Finance System
- Department of Health – Deceased Voter
- Pollbooks
- PennDOT
- ERIC
- PA DOS Secure FTP
- Pre- and Post-Election Audits

The actual scheduling of the development will take place after the initial survey of interfaces and analyses (as documented in the plan) is complete. We anticipate participation by DOS in surveying the current interfaces and providing the attribute information listed above. For those interfaces developed or owned by an external entity, BPro will require their participation as well in the description, modification, and testing of those interfaces.

9. Solution Security Testing

Security is a top priority for BPro. Elections are the backbone of our democracy and any security breach could undermine the public's confidence in the electoral process. With the focus hackers put on Voter Registration systems in the 2016 election cycle, BPro has continued to enhance system security to ensure our systems and our customers stay ahead of those who wish to destabilize our democracy. Thus, BPro understands that security is a critical concern for the development, implementation, and management of the PA DOS TotalVote Project. Our strategy for addressing this concern is two-fold. First, focusing on adhering to secure coding

practices to ensure that the code is structurally sound and free of any major structural issues that could cause the data, applications, or systems to be exposed to a high-level of risk. And second, to implement an active, dynamic security architecture consisting of technology and process that creates an active, operational paradigm for managing security and mitigating risks.

Utilizing PennDOT's driver's license system, TotalVote will validate users' identities to Level of Assurance (LOA) 2. As a result of the sensitivity of the data stored within TotalVote, BPro will perform SOC-2 Type 2 audits via an independent auditor to report annually on the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the control description specifically relating to this contract. The auditor's report will conform to the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Reporting on Controls at a Service Organization published by the American Institute of Certified Public Accountants (AICPA). The auditors will conduct a Service Organization Controls (SOC) 2, Type 2 SSAE 18 audit. BPro will provide the auditor with access to all systems, facilities, information and people required perform the audit. The control objectives of the audit shall be at a minimum, equivalent to those required under the General Accounting Office Federal Information Systems Computer Audit Manual (FISCAM) for performing all work. The procedures and report will meet the FISCAM requirements and shall include application systems testing. Each review will follow guidance provided by GAO's FISCAM Manual and include a corrective action plan. BPro will review the report, respond to each finding, and identify its proposed corrective actions. BPro's response will be received by the GTR/GTM within twenty (20) days after the contractor receives a copy of the audit report. The auditor's annual reports shall cover operations from effective date of full servicing capacity through the first year.

10. Issue Tracking Process and Log

BPro's issues management process focuses on identifying and resolving issues experienced within the life of the project. Since issues can arise with no warning, the PA DOS TotalVote project needs to have an approach identified to handle these unexpected matters that can either negatively or positively impact the project.

Issues may take the form of problems, gaps, inconsistencies, or conflicts. Issues will be recorded and tracked in the Issues Log. The issues log will record the issue and responsibility assignment so the issue can be tracked as soon as it is identified through resolution. The resolution will be recorded for future reference and project learning.

Decisions are also marked in the Issues Log for understanding and acknowledgement of decisions that have been made that affect the direction of the project.

Impediments are considered to be temporary issues that are preventing work from progressing forward. When a work task cannot move forward before something else is accomplished or

corrected, that is an impediment. Documenting these kinds of issues serves to present clear understanding to the team that this issue is impacting progress of the project.

The BPro Project Manager will revisit the status of the Issues Log at each project meeting with the intent of:

a. Updating current status of any identified issues
b. Following up on action items previously assigned
c. Developing new action items as needed
d. Adding new issues as needed

An Issues Log will be the record of concerns and unknowns identified during the life of the project. The Issues Log is a list reported in the project status report and is regularly reviewed at project meetings. The Issues Log template which will be used in the project status report is as follows:

Issue ID#	Issue Title/Description	Report Date / Resolved Date	Status (Active, Closed)	Action Plan

Figure 14 - Issue Tracking Template

11. Defect Management

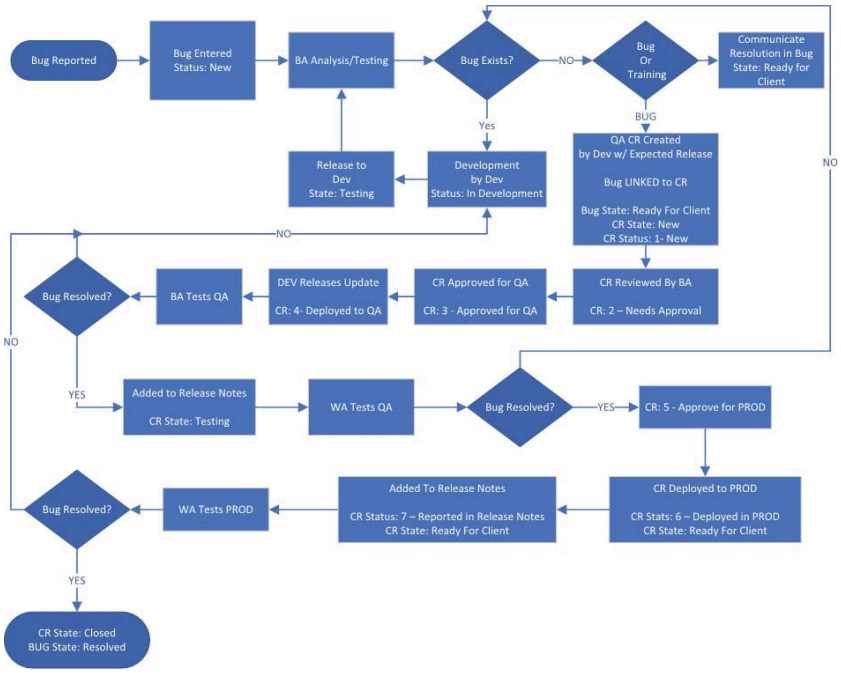
Defects will be managed using BPro's TFS. TFS will house all bugs or defects reported within the testing events of the project. When bugs are inserted into TFS, the bugs and any associated tasks will be assigned for resolution. The bug's progress will be tracked through TFS.

When bugs are reported to BPro, the Product Owner or DOS BA will need to include details of the bug including steps to reproduce it so that the bug can be efficiently analyzed by a BPro BA and assigned for resolution. The DOS Product Owner or BA should also include a severity when the bug is reported.

These items will be used as the basis for reports, lists, and statistics. The bugs or defects will be tracked from initial report through resolution using the following steps when testing the items included in the release:

a) Establish test execution steps
b) Record Pass/Fail of a test using the state field of the TFS item
c) Record the reasons for failure of a test within TFS comments and related fields. This includes:
    i. Steps to reproduce the defect
    ii. Add attachments with screenshots
    iii. Identify severity of the defect
    iv. Identify the priority of the resolution of the ticket

The below workflow process diagram (from Washington's VoteWA system) shows the steps associated with the BPro TotalVote defect management process:



12. Quality Assurance

Quality control and testing procedures shall be driven by requirements and design and shall adhere to detailed test plans. BPro uses TFS for issue and project tracking. All requirements, including their functionality and design, are cataloged in TFS for the development staff. After development work is complete, testing is carried out by both development staff and a business analyst (BA). This testing includes individual requirement testing, unit tests, and system tests. Upon the success of all testing, the software is ready for release to the PA DOS Product Owner for sprint review testing. If issues are identified by the PA DOS Product Owner, BPro will log the issues or bugs and the development team will address them. After issues or bugs have been resolved, they can be retested through the sprint review process.

Testing and Promotion Process

BPro will employ a structured testing process. BPro executes various levels of testing to ensure quality control throughout the development process:

- **Unit Testing**: Our developers will create software from requirement details and Unit Test the component(s) developed comparing the performance to the acceptance criteria of the requirement. Unit Testing is done by the developer prior to the component code being promoted for further testing.
- **Integration Testing**: Unit tested software components are promoted to our internal BPro Test system where BPro Test Leads or Business Analysts (BA) conduct their testing from the business process perspective across multiple components to ensure that all parts continue to work together. Integration testing is done against the whole of the system for all areas changed.
- **Regression/System Testing**: The Staging environment should be the same configuration as the Production system for final testing to ensure all components are working together; this testing is performed by PA DOS's TotalVote Team.
- **Sprint Review Testing**: After each development sprint release, BPro will deliver components of the system which were completed during the sprint. The PA DOS Product Owner will inspect the delivered user stories and provide feedback. These sprint review software deliveries are an opportunity to develop familiarity with the solution. Since individual requirements are delivered, it is not uncommon for complete process flows to not flow smoothly until the entire set of workflow components are delivered. Early testing of the delivered components allows the Product Owner to confirm that user stories are present to satisfy the complete workflow.

User Acceptance Testing

User Acceptance Testing is performed and managed by the PA DOS TotalVote Team in the Staging or Test environment with known defects documented. With Agile Development Methodology, as each sprint is verified by our Business Analyst, releases will be delivered to the TotalVote Test system. The BPro Business Analyst will demonstrate the delivered components to be tested. Prior to testing, the team will have already concurred on acceptance criteria, test methods to be used, and known defects. The PA DOS Team will then perform acceptance testing on the delivered components. PA DOS may perform varying degrees of acceptance testing, potentially including integration testing, depending on the degree to which other system application components are dependent on the delivered component.

Release Strategy

BPro's development and release strategy for this project is to work with your team to break the deliverable *F.1 - Fully Configured Solution and Interfaces* into units that can be packaged and implemented in "iterative" deliveries, also called sprints. Sprints are expected to be 3 weeks in length. At the end of each sprint, the code will be packaged as a release. This allows both teams to focus on quality of short-term goals and build upon previous deliveries to reach the overall project goal. With each version release, a list of detailed changes is documented to inform Pennsylvania's DOS Team of the items included in the release.

Release Numbering Standard

For release management, BPro will use the following numbering system:

- [Major Version].[Minor Version].[Last 2 Digits of Year + Day of Year]. [Build number for that day]

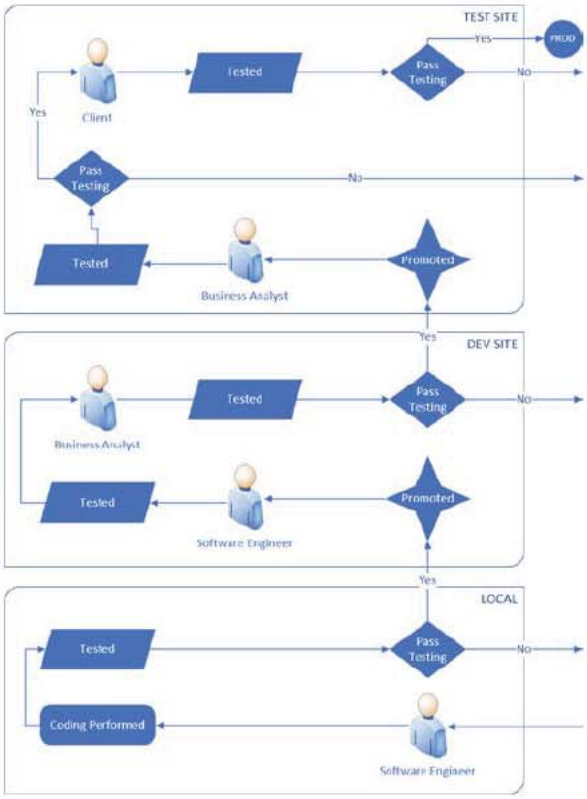
Example: 1.3.19098.1

This procedure will ensure each version of software released from BPro will have a unique version identifier.

Environments

[redacted]

Testing and Release Process



Defect Tracking

If the deliverable performs as documented in the Acceptance Criteria for that requirement, then the test is considered passed. A testing activity is logged against that deliverable and the status of the deliverable is updated. As the project progresses towards completion, the project is accumulating deliverables that have passed acceptance testing.

If the deliverable does not perform as expected, a "fail" testing activity is logged against the requirement. PA DOS TotalVote users will log the defect to TFS for defect tracking. Defects are prioritized to isolate those that are causing greater negative impact. If a satisfactory work around to a defect cannot be established and the process involved is critical to the function of the office, then the defect is prioritized as a critical issue that must be fixed immediately. Beyond that there are levels of High, Medium and Low priority that are determined in coordination with the PA DOS team leads. Prioritization allows BPro to focus work on defects that need the most immediate attention.

Quality Assurance Deliverables Chart

Key Activity	Deliverables	Key Personnel/ Responsibility	Acceptance Criteria
1. High level QA Approach	Quality Management Plan	BPro Lead Quality Analyst BPro PM PA DOS PM PA DOS Lead Test Resource	Accepted by Project Directors of both teams
2. Testing and Promotion	Unit Testing Integration Testing Release Demo	BPro Developer BPro Lead BA	Meets requirement acceptance criteria
3. System Testing (i.e. Integration, Conversion, Regression, Usability etc.)	Usability Testing Regression Testing Conversion Testing	BPro Lead BA PA DOS BA/SME BPro DBA PA DOS DBA PA DOS Product Owner PA DOS BA/SME	Meets requirement acceptance criteria
4. Test Plans/Case Development	Advise on Test Plans/Case	BPro Lead QA	Stated in Quality Management Plan
5. Test Plans/Case Development	Develop Test Cases	PA DOS BA/SME	Stated in Quality Management Plan
6. User Acceptance Testing	Acceptance Testing	PA DOS Product Owner	Stated in Quality Management Plan

BPro will continue to build on the accessibility compliance that has already been done to TotalVote during previous implementations. BPro has always placed a priority on accessibility and the TotalVote system has been previously tested to both Section 508 and WCAG 2.0 accessibility standards. WCAG 2.0 has become the standard for accessibility testing and BPro engaged the Washington state chapter of Lighthouse for the Blind to provide accessibility consulting and testing of all public facing TotalVote systems during the Washington VoteWA project in early 2019.

Beyond accessibility, all BPro public facing systems are built with responsive design, which ensures an optimal user experience on screens of any size, including mobile devices. TotalVote is also able to display multiple languages and is used by four states to build multilingual ballots in five languages.

Data Conversion Strategy
The Data Conversion effort is a key success factor for the PA DOS TotalVote Project. Bad data can overshadow everything else that is positive about a project. Further, quality testing a data conversion can be problematic because it is impractical to open and review every record and sampling is not very effective. BPro has developed a conversion process that ensures that all data is successfully mapped and accurately transferred into the TotalVote system. BPro ensures a quality delivery of data and images and will affirm the team's confidence in the new system implementation. Our conversion process includes a number of data validation techniques, both automated and manual, to ensure all data is transferred correctly.

BPro is experienced with the data structure of voter registration data and data conversions through our successful delivery of election systems in several states. This includes building the State of South Dakota's Voter Registration system, which changed from a bottom-up model to a top-down model with the implementation of TotalVote. In addition, BPro has built data exchanges for our customers to participate in both ERIC and Cross Check, in order to compare voter registration data with other states.

PA DOS Resources Needed
BPro recommends that a Database Analyst (DBA) from the PA DOS TotalVote Project Team will work directly with BPro's DBA to create processes to extract data and images from the legacy systems. BPro proposes that the PA DOS DBA is added to the project team at Project Initiation to assist with the data conversion efforts.

Data Extraction and Preparation
Together the DBAs of both teams will create extract, transmit, and load procedures (ETL) for moving the data and images to TotalVote. The DBAs will coordinate with the Business Analysts to ensure the processes for conversion deliver a product with data integrity, meeting all quality standards, and created in TotalVote in a manner that is fully consumable into the business process and software logic of the BPro system.

Data Mapping Rules
The PA DOS DBA Team will provide a data dictionary of the legacy system's data structure and full data extracts. The BPro DBA will work to fully analyze the data sets against the data structure of every field. BPro will document the mapping of data to the TotalVote system and present small trial conversions for verification. Legacy fields that do not have an "exact fit" will be reviewed with the PA DOS TotalVote Team to determine the best course. For example: does the field contain data that needs to be used as input to logic on the TotalVote system, and if yes, how must the value in the field be stored in TotalVote?

BPro has special routines to evaluate all the unique code values for all fields that are coded, such as district, precincts, polling places, etc. These fields will usually be evaluated first and confirmed with PA DOS TotalVote team.

Resources for Data Scrubbing
The BPro DBA may identify outlying data that does not fit the definition of the field and requires "data scrubbing" or cleanup in preparation for conversion. Data scrubbing may be necessary on both the state and county level. These will be logged as conversion tasks. The PA DOS DBA will manage the tasks associated with data cleanup. These tasks may be handed off to be managed by various members of the PA DOS team depending on the nature of the problem and who owns the process that manages the data.

Strategies for Final Conversion
With final conversion, the legacy systems should remain searchable to be used as a reference for the new TotalVote system conversion. BPro's process does not rely on data sampling to ensure quality data. BPro's conversion process will verify the converted content of all tables by comparing metrics supplied by backend queries against the legacy systems.

These are a few standard BPro practices during final conversion validation:

- When a data set is harvested from Pennsylvania's legacy systems for a conversion, the legacy data is retained as a query-able database.
- A series of counting queries are built to evaluate the content for each field. For an example – one query is built to count of the number of records that have the first name beginning with each level of the alphabet, returning an array of the 26 letters and a record count for each. (Another query would count the same for middle name, and another for last name, etc.) These queries are compiled in preparation for testing the conversion.
- BPro performs the conversion and applies the dataset to TotalVote tables.
- Testing the conversion: Inside the TotalVote application, the user searches on first name of "A*" (wildcard) and a count is returned. That count should match the query from the legacy system. This search is repeated for all letters of the alphabet and matched against the original SQL query results. There should be no exceptions that cannot be accounted for.
  - The example is repeated for all text fields. Tests can also be run for the last character in a text string.
  - The same example is used for numeric fields, testing for the first digit, and/or the last digit value, and retrieving value (0-9) counts for each field.
  - Date fields can be counted for months (how many birth dates in May), or counts of the day values, or counts of the year values.

13. Implementation Schedule and Dependencies

Implementation Schedule
The official Project Schedule is the document which governs the project's work tasks and due dates. Any changes to the below mentioned task dates will be primarily maintained in the

Project Schedule; this document is a secondary source and will be updated through new document version releases.

Below are events on the Project Schedule related to the development and configuration of the system:

Task Name	Duration	Start	Finish	Predecessors	Resource Names
Deployment Readiness	**127 days**	**Tue 6/15/21**	**Tue 12/14/21**		
Update Implementation and Deployment Plan	25 days	Tue 6/15/21	Tue 7/20/21	115	BPro PM
Prepare User Documentation	20 days	Wed 8/18/21	Wed 9/15/21	128	BPro Product Manager
Conduct Implementation Readiness Checks	10 days	Fri 11/19/21	Mon 12/6/21	132,136	BPro Product Manager
Prepare Systems Operations Documentation	30 days	Thu 9/16/21	Wed 10/27/21	155	BPro Product Manager
Conduct training to state technical staff	2 days	Thu 10/28/21	Fri 10/29/21	157	BPro Product Manager
Perform tasks in transitions to operations checklist	1 day	Tue 12/7/21	Tue 12/7/21	156	BPro Product Manager
Deliverable K.2: Submit Final Release Package	*5 days*	*Wed 12/8/21*	*Tue 12/14/21*	*159*	BPro Product Manager
Production Deployment	**2 days**	**Wed 12/15/21**	**Thu 12/16/21**		
Review production readiness checklist	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
Data cut-over from legacy system	1 day	Wed 12/15/21	Wed 12/15/21	153	PA DOS
Production Data Conversions	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro SQL DBA
Production Application Cutover	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
County and State Testing of Implemented Sites	1 day	Thu 12/16/21	Thu 12/16/21	165	PA DOS
Go-Live Support	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Dev Team
Project Closeout	**5 days**	**Fri 12/17/21**	**Thu 12/23/21**		
Prepare and Process Project Closeout Checklist	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Product Manager
Update all system documentation for project closeout	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
Deliverable H.4: Submit Final Conversion Report	*1 day*	*Fri 12/17/21*	*Fri 12/17/21*	*161*	BPro PM
Complete warranty and transition to maintenance and operations	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM

BPro developers will provide dedicated support and monitoring from the start of the implementation tasks through the end of the production deployment.

Implementation readiness can be broken down into the following:

1. TotalVote Application readiness
2. Data readiness
3. User readiness
4. Deployment Platform/Production Environment readiness

Implementation Dependencies
Dependencies impacting the implementation schedule are found in the below four subsections on readiness: application, data, user, and production environment.

A production readiness checklist will be compiled for this project and reviewed with the PA DOS PM and other key staff in preparation for production.

Application Readiness
The TotalVote application will undergo extensive cycles of testing and feedback consolidation to be ready for deployment. Here is a summary of activities:

1. Development followed by unit, functional, and user testing of the entire application over several sprint code releases.
2. Completion of TotalVote functionality and data testing by the PA DOS designated test teams.
3. Incorporation of the feedback and defect fixes to ready the application for user acceptance testing.
4. Perform User Acceptance Testing (UAT).
5. During UAT, testing of all the system interfaces will be performed and functionality of the associated systems and applications confirmed.
6. In parallel with conducting UAT, BPro will update the plans associated with the Project Management Plan and other supporting project documentation.
7. After UAT session is completed, developers will address any issues which were identified.
8. PA DOS designated test teams will conduct a second UAT session.
9. Finalization of the application based on user testing results will mark the completion of the system and transition the project to the Go or No-Go decision point.

Data Readiness
BPro's approach to data conversion and readiness is outlined in the Data Conversion Plan**.** Summary of activities is as follows:

1. All data conversion will be completed in conjunction with the completion of application development and in preparation for TotalVote functionality and data testing.
2. The PA DOS will test their data and provide approval on completeness and accuracy of data during the TotalVote functionality and data testing sessions.

3. Data will be tested with the application in the Staging environment to ensure the data and application work well with each other.
4. Every step of application testing will include indirect testing of data using application functionality.
5. At any point, feedback on data issues will be reviewed, analyzed, and data mapping documentation updated to ensure that the data has been converted accurately and in its entirety.

User Readiness
BPro's approach to user readiness is to engage the users early with the TotalVote application so that they can get adequate time to get comfortable with and trained in the new system.

BPro's approach to user training will be outlined in the ***Training Plan.*** Details of the training materials to be used will be covered in BPro's approach to data conversion and readiness outlined in the training materials provided for user training sessions.

Production Environment Readiness
BPro's detailed approach to the TotalVote Production environment, its readiness, and deployment is described in this plan.

To ensure that the readiness for the Production environment, BPro will conduct the UAT sessions on a simulation of the production on a Staging environment. That will allow the team to work out the details and all technical aspects of the environment during the formal testing sessions of the project. Environment readiness will include the technical testing of the system.

Test Data Migration
Prior to the final data migration, the team will run at least one test migration to identify problems or bottlenecks and to capture metrics at key migration checkpoints. The resulting timing metrics will provide the input for scheduling of the final conversion. This conversion approach ensures that all records are correctly transferred without the need to conduct random spot checks of data from individual records. It also provides timing statistics necessary for scheduling the conversion. In addition to being more efficient, BPro's conversion strategy has proven to be more effective in each implementation we have successfully completed.

14. Knowledge Transfer Activities

BPro recognizes that change is challenging for an organization and should be addressed at the project, program, and portfolio levels. While is it outside the scope of this project for BPro to provide organizational change management for the organization, at the project level there are steps we can take to help in the transition. According to the PMI Practice Guild for Managing Change in Organizations, "Consider mobilizing stakeholders, purposely and continuously, as the most important aspect of implementing change other than defining clear measures of success."

BPro will support the Commonwealth of Pennsylvania to share the vision of this project through delivering a quality product to demonstrate success. Throughout the project, the BPro team will work collaboratively with the PA DOS team to review and provide feedback for revising the communications plan during project execution. That plan will help guide us to respond to some of the environmental or contextual shifts that occur during the project (as listed in the *PMI Managing Change in Organizations Practice Guide*), including:

- Resistance to or acceptance of a change that is greater than anticipated or comes from unanticipated sources,
- Unforeseen transition or integration issues,
- Unforeseen conflicts among people/groups related to the change,
- Challenge or unsuitability of project outputs due to changing circumstances, sponsor pressure, apathy, or missteps,
- Changing management support for the effort, and
- Changes in the assumptions that are the basis for anticipate outcomes.

As the team works with those stakeholders who will be directly impacted by the new systems, we'll be sensitive and aware that some participants may be resistant. We'll share our observations with the DOS team to help identify issues before they build or spread.

The BPro team makes it a priority to establish trust with our stakeholders through open, respectful, and honest communications.

Training Plan

User Training for TotalVote will take place after development has been completed for all modules and prior to User Acceptance Testing (UAT). BPro will use a "train the trainer" methodology to train DOS personnel to become "super users" of the software. This train-the-trainer training will be led by the BPro Training Lead and TotalVote lead subject matter expert. After the DOS personnel are adequately trained, they will be prepared to handle support and training for all end users including County staff. DOS personnel will join BPro trainers for two weeks of regional trainings around the state for County staff. This will serve to both train County staff and reinforce the expertise of DOS "super users" in the TotalVote system.

All hands-on software training (for both DOS and County user training sessions) will take place in a training (Staging) environment configured identically to the Production environment.

Training Approach and Curriculum

For the "train-the-trainer" training sessions, BPro will work with the DOS to finalize a user training schedule and plan. The scope of the DOS training shall encompass two parts: 1) State user training, and 2) Training County users on all TotalVote modules.

BPro will conduct the DOS training sessions in person over the course of five (5) days on site in Pennsylvania. BPro will provide the following on-site "train the trainer" sessions for DOS-designated training staff:

- Provide training to DOS trainers on all modules completed throughout the Project (relevant to both State and County users)
- Assist DOS staff in the use of BPro-provided training materials
- Facilitate a dry run of the training session and make recommendations to DOS staff on clarity, flow, and accuracy of training presentation
- Make modifications to training materials as necessary

Training for DOS-designated training staff will be conducted by BPro on-site over the course of one week (Monday through Friday). Attendance for all five days of training is required for DOS-designated training staff. Locations, training equipment, and printed materials will be provided by the DOS office (training materials will be created by BPro and provided electronically to the DOS prior to training.) During the course of each day, BPro will demonstrate the components of all modules. Users will log in and practice functional tasks in small groups at individual workstations, while using individual logins from a variety of user groups for both State and County permissions.

Every day, the training will focus the content on:

- Training Materials
- Module overview
- How to perform designated tasks within each module
- How to verify output of tasks
- Reporting
- Review

After the completion of the "train the trainer" week of training sessions, DOS staff and BPro staff will conduct hands-on training over the course of two (2) weeks for County staff. This training will be held in regional locations throughout the state that ensure the highest levels of participation. The DOS and BPro will coordinate the final schedule, arrangements, and communication for regional County trainings.

BPro shall provide the following activities regarding on-site training for County staff:

- Assist with the setup of the training facilities, such as setting up a dedicated workstation with hardware for printing, scanning, and document imaging
- Attend all training sessions for the entire duration to answer any questions DOS cannot answer and provide assistance regarding system operation
- Assist in troubleshooting technical issues that may arise during initial setup or during the sessions

For the County training, BPro will conduct formal review sessions to allow the trainers an opportunity to review and provide feedback on each training session for improvement. (Feedback may be gathered verbally or from feedback forms collected from attendees at the County trainings.) A short review session at the end of each day would be valuable to discuss

areas for training improvement, as well as a weekly report submitted on Fridays to wrap up all findings during each of the training sessions. A final post-mortem with DOS staff and BPro will be conducted via conference call after all regional trainings are complete with BPro producing a final User Training report for DOS.

For each Voter Registration system BPro has deployed, we continue to provide training and support after go-live. This support will continue in the Commonwealth of Pennsylvania, by phone and web conferencing, with in-person training options also available. A great example is the regional training program BPro participates in for North Dakota. For two weeks every two years, BPro and ND DOS staff travel to regional locations around the state and provide full day training on our systems. Another example is using annual conferences as an opportunity to further train County staff. BPro conducts a training session at South Dakota's annual conference of county auditors where BPro presents refresher materials, participants learn about system upgrades, and there is ample opportunity to ask questions about the TotalVote system. Cost for these in-person trainings is extra and BPro will work with DOS to determine the best continuing education opportunity for the PA DOS TotalVote system.

15. Go & No-Go Criteria Decision Points

Upon successful completion of the second User Acceptance Testing session, the system will be considered ready for go-live. The following is the summary of activities needed for TotalVote implementation. Final decision on go-live will be made through formal approval of the PA DOS Project Manager (PM).

Following this approval, the following activities will be performed to take the system live into the production environment:

1. TotalVote Go/No-Go Decision by PA DOS PM	Day 1 (Tuesday)
2. SURE System Shutdown	Day 2
3. Production Data Cutover	Day 2
4. Production Data Conversion	Day 2-4
5. TotalVote Application Production Deployment	Day 5 (Monday)
6. State Data Validation in TotalVote Production	Day 5-9 (Monday – Friday)
7. County Data Validation in TotalVote Production	Day 5-9 (Monday-Friday)
8. TotalVote Live in Production	After Completion of Validation
9. System Deployment Support Starts	Day 5

The completion of these activities marks the successful delivery of the PA DOS TotalVote system. At this point, TotalVote will be in Production mode.

16. Roll-back Provisions

BPro's development approach incorporates safeguards to ensure code can be rolled back in emergency situations. The code builds are stored in the Microsoft DevOps repository and are based upon the release number. These previous builds can be called up and the system can be reverted to a previous build release version. Authorization for the Production environment to be rolled back to a previous version will be reserved for decision by senior level management in PA DOS.

17. Post-Implementation Review

The TotalVote application comes with a 12-month warranty and annual support services that will commence after the completion of the main portion of the project marked by the system implementation in Production environment.

Upon the deployment and approval of TotalVote system, BPro will provide go-live support for one week followed by a 4-week period for application stabilization. Following the go-live support timeframe, the warranty and support services will commence for the TotalVote application.

BPro will also provide all updates to TotalVote documentation as part of this production deliverable.

After the TotalVote system has been deployed and the final conversion has occurred, the legacy system should remain searchable. The legacy system will be used as a reference tool for the new TotalVote system conversion. BPro's conversion process will verify the converted content of all tables by comparing metrics supplied by backend queries against the legacy system. Reports should be pulled from the legacy system by the PA DOS and used for data validation.

18. Project meetings and planning meetings

Project and planning meetings will be handled as efficiently as possible. They will be timeboxed which means the meetings will start on time and will wrap up at the time appointed to conclude.

In order to make meetings efficient, proper facilitation and preparation is required. All meetings should have clearly defined objectives so that the right people are in attendance for making the right decisions that are needed. Any issues that are discussed should have follow up and/or action items noted.

An agenda will be included for every status meeting and all other project meetings as appropriate. Agendas may take on various formats and can be included as part of the meeting invitation. Agendas will, at a minimum, include:

- Meeting title
- Date, time, and location
- List the topics of discussion

In some instances, timeframes for each topic may be stipulated to ensure the meeting stays on track and finishes on time.

Minutes are taken at status and review meetings. At meetings where minutes are taken, the following information will be included, at a minimum:

- Meeting Title
- Date and Time
- Attendees or Invitees
- Topics of Discussion
- Decisions
- Action Items

The meeting minutes and the distribution of those notes are the responsibility of the party facilitating the meeting unless otherwise stated or arrangements were made to assist.

Deliverable:

- **Finalized Implementation Plan Approved by DOS**

B. Implementation of the Solution. The selected Offeror shall perform, at a minimum, the following tasks for each implementation.

1. **Implementation Management.** The selected Offeror's Project Manager shall manage and monitor all activities during the implementation process and at a minimum provide the following:

Deliverables:

- **Weekly implementation status reports**
- **Final implementation report**

C. Requirements Management. Offeror shall describe its approach and methodology to requirements management to complete the task described below.

a. The selected Offeror shall be responsible for managing and tracking all requirements throughout the life of the contract. Requirements management

shall include but not be limited to the verification of the requirements identified by DOS in **Appendix F, Detailed Requirements,** as well as the discovery of additional requirements to ensure completeness. The Offeror shall propose a process to track the individual requirements, prioritize, and maintain the status of each.

b. The selected Offeror shall develop a requirements traceability matrix which links requirements throughout the validation process. The purpose of the requirement traceability matrix is to ensure that all the requirements aredefined for the system are reflected in the design and tested. As the design specification and test plans and scenarios are developed, the traceability matrix is updated.

c. The selected Offeror shall perform GAP analysis and include a GAP analysis as part of the Finalized Detailed Requirements Document. The GAP analysis shall be between the detailed requirements and the proposed solution. The purpose of the GAP analysis is to identify and resolve any gaps between the detailed requirements and the selected Offeror's solution to ensure that all requirements defined for the system are reflected in the solution.

d. The selected Offeror shall submit the finalized requirements document, following a discovery meeting with DOS, which includes a requirements traceability matrix and GAP analysis document. The DOS will review and provide final acceptance based on mutually agreed upon time frames between DOS and the selected Offeror.

Offeror Response

Requirements define the scope of the project and will be tracked from RFP through the completion of the project. Since the solution is not a custom developed application built from the ground up, the requirements defined in the RFP will need to be analyzed against the baseline of BPro's TotalVote application. The system will need to be analyzed for both functional and technical requirements. The requirements which will be used for defining the scope of this project will be converted by the PA DOS Product Owner with assistance by BPro into user stories.

User stories are part of the agile approach. User Stories are short, simple descriptions of a requirement told from the perspective of the person who desires the new functionality. The acceptance criteria included for each user story will be used as the basis for what development will create and for the PA DOS Product Owner to use for approval of the delivered requirement.

a. Managing and Tracking Requirements

BPro will use **Appendix F, Detailed Requirements**, from the RFP as the baseline of all requirements along with the user stories derived from those requirement sets and provided by PA DOS.

The PA DOS TotalVote functional and technical requirements and user stories will serve as the starting point to populate work items in BPro's Team Foundation Server (TFS) which will track requirements throughout the project. Software modules will be built using an Agile Scrum approach. Information on what requirements are met "out of the box" and those that need to be configured or changed will also be in TFS. BPro and the DOS Product Owner will update TFS to ensure that the work items are updated with acceptance criteria by working with the DOS Product Owner and the Development Team.

Sprint Grooming, Sprint Planning, and Sprint Review sessions will be scheduled with the PA DOS Project Team to go through each work item to build, clarify, or verify acceptance criteria for the RFP requirements.

The project will use DOS requirements and user stories provided for review and discussion with the PA DOS SMEs for clarification and elaboration.

BPro SMEs will work with the PA DOS SMEs as follows:

- Validate if the work item as listed is valid and correct.
- Elaborate the work item, if needed.
- Demonstrate how the requirement is being met in the baseline TotalVote application.

Record in TFS any work item or task that needs to be addressed.

User stories are assigned a priority by the PA DOS Product Owner. All user stories will have a priority when requirements review is complete.

- Priority 1 – Requirements are all prioritized as core functional or technical requirements.
- Priority 2 – User stories that have material efficiency impacts to the overall process being performed.
- Priority 3 – Nice to have.

The standard Sprint Planning process will be used to load a development sprint with the Product Owner and Lead Technical resources reviewing the highest prioritized stories for load.

The status of each requirement in the form of user stories will be done throughout the course of the design, development, and testing of the requirement.

The TFS state field will be the main source to identify the state of the requirement:

State	Definition of Use in Requirements
New	All work items start with a State of New including user stories for requirements.
Active	An active user story is currently being created or addressed by Development.
Resolved	Resolved is used to flag that the BPro BA has tested the item and is now ready for the client to review, test, and approve.
Code Review	Code Review is an internal BPro State for Development use. It is flags the BPro BA that the item is ready for the BPro BA to review and to test.
Failed UAT	This state denotes a user story which did not pass BA or client testing.
Removed	Removed user stories are generally duplicate stories. The reason of removal is noted in the notes sections of the TFS item.
Closed	A Closed ticket is a completed user story.

Dashboards within TFS assist with showing a visual depiction of the statuses of requirements, bugs, and issues for the project in the form of charts and graphs. TFS queries will be created to support the dashboard and other status reporting needs of the user stories.

b. Requirements Traceability Matrix

Requirements traceability matrix will be utilized on this project. This will help ensure the project's scope, requirements, and deliverables remain "as is" when compared to its baseline. The excel spreadsheet of technical and functional requirements will be used as the basis for the GAP analysis.

Once a finalized listing of requirements is approved for the project, the items within the excel spreadsheet will be imported into BPro's TFS for automated tracking, linking to other associated work items, prioritizing, managing, assigning, and status reporting.

c. GAP Analysis

A GAP analysis will be performed to review **Appendix F: Detailed Requirements** with the PA DOS project team and BPro. The GAP analysis will compare the PA DOS requirements to the current functionality of the BPro TotalVote system. Any gap identified during this review will be noted. The PA DOS Product Owner will create user stories to detail and describe the business needs required for these gaps. The user stories will be entered into BPro's TFS for tracking, managing, and monitoring through the end of the project.

d. Finalized Requirements Document

Once the GAP analysis is complete, the finalized requirements document will be provided to PA DOS. This document will include the requirement traceability matrix and associated GAP analysis document. Once PA DOS has approved this document, the requirements will be imported into BPro's TFS for tracking, prioritizing, managing, and monitoring through the end of the project.

Planning, communication, and coordination play pivotal roles in the success of the requirements management process.

BPro carries out high-level planning at the outset of the development process with detailed planning done by the development team at each sprint iteration. Using this approach, requirements are sometimes detailed later than in a prescriptive model, that is just before development. This "just in time" planning ensures requirements specifications are current and allows the developers to work while the specifications are still fresh in mind. Through the Agile/Scrum process, PA DOS has full authority and responsibility to prioritize business requirements according to their business value, set acceptance criteria, and help the development team understand exactly what is needed. The acceptance criteria specified by the PA DOS will be the basis of building the component and basis for the approval tests for that component.

With a complex project of this scope, there will be changes as the system is built. These changes can be incorporated into the development process rather than viewing them as disruptive and unwelcome. Software development for PA DOS TotalVote will be broken down into phased releases based on sprint cycles with formal testing events to occur after the end of the last development sprint release. During development within each iteration sprint, quality will be incorporated by the developers and by PA DOS through their sprint testing and review.

Deliverable: Requirements Package to include the following work products and which will be considered complete following a review and final acceptance by DOS;

- Finalized Requirement documents. accepted by DOS.
- Requirements Traceability Matrix.
- GAP analysis document

D. Configuration of Environments. The selected Offeror shall submit a confirmation report to DOS for each environment when the configuration of the platform is Ready for Use (RFU). The DOS will review and provide final acceptance based on mutually agreed upon time frames between DOS and the selected Offeror.

If Offeror hosted, the selected Offeror shall setup and configure applicable environments. Offeror shall describe its approach to the setup and configuration of the solution environments, including the number of environments, users of the environments, and timing of availability during the solution roll-out and availability

after moving into the maintenance and support phase.

Deliverables:
Configuration Confirmation Report approved by DOS
Offeror Response

TotalVote VR/EMS includes three environments and possibly four: Development, Testing, and Production. The fourth is a Training environment, which the need for this environment will be determined as the project progresses. Development is only available to the BPro team. All other environments are available to authorized Pennsylvania personnel from the state and counties. All environments, with the exception of Training, will be available after moving to maintenance and support. Each environment will be configured at least 3 months prior to use. Configuration of environments will be fully scripted and automated. This ensures each environment is configured identically.

E. Solution Interface and Design. The selected Offeror shall develop a detailed solution and interface design document, which shall also consider work and interaction with other Commonwealth agencies or third-party partners, representing a refinement of the finalized requirements for all interfaces. The selected Offeror shall work with DOS in the future to identify additional interfaces and develop design approaches as needed.

The selected Offeror shall submit a detailed solution and interface design document, addressing all interfaces, for review and approval by DOS based on mutually agreed upon time frames between DOS and the selected Offeror.

Offeror Response

Deliverables: Detailed Solution and Interface Design Document and Interface Devlivery Specification

F. Solution and Interface Configuration. The selected Offeror shall configure the solution and interfaces to meet the requirements as documented in the finalized detailed requirements and this RFP. The selected Offeror shall implement the configuration in all environments based on a mutually agreed upon time frame between the DOS and the selected Offeror. The DOS has the sole right to review and approve the solution and interface configuration.

Offeror Response

Deliverables: Fully Configured solution and interfaces reviewed and accepted by DOS.

G. Development of test plans and scenarios. The Offeror shall describe any manual or automated testing capabilities available in the proposed solution. Offeror shall describe its approach to testing for implementation of the proposed solution. The selected Offeror shall develop test plans and scenarios for both DOS and county election officials. The test plan and test scenarios shall be reviewed and approved by the DOS.

Offeror Response

The Testing Plan will be provided as a separate deliverable for this project. The Testing Plan will describe the scheduled events and methods BPro will use to conduct testing within our team and with State, County, and other stakeholders for implementation of the TotalVote system.

As BPro has matured and advanced its development approach, we realize the benefits of incorporating automated testing into the process. While not replacing manual testing, using tools, such as Selenium, greatly enhances our test coverage and execution. Our automated tests assist in preventing the promotion of code that does not pass basic functionality. This helps identify issues prior to user interaction with the software and reduces the need for emergency patches. These automated tests can also be used to stress and load test, simulating numerous transactions occurring in the system. This provides BPro the ability to address negative user interaction with the UI before the user experiences it directly.

Deliverable: Test plan and test scenarios for DOS and county election officials, reviewed and approved by DOS.

H. Data Conversion and Validation. The Offeror shall be responsible for data migration and validation tasks as described below. The Offeror will be responsible for developing, planning and validating DOS and county election official data between the existing system and the proposed solution subject to review and approval by the DOS. The time frame for data conversion and validation will be mutually agreed upon between the Offeror and the DOS.

a. Offeror shall describe its approach and methodology to data conversion and validation. Offeror shall recommend a timeline with delivery dates, conversion approach, describe the level of effort, and list any assumptions related to the conversion effort. The selected Offeror shall submit a conversion plan that, at a minimum, includes the items listed below. DOS reserves the right to add or delete items from the conversion plan.

- Clearly defined roles and responsibilities for Offeror, Commonwealth staff and county election officials when participating in the conversion;
- Controls and programs to assist in the conversion;
- A formal system to track, document, and manage conversion issues;
- Test plans to verify data has been correctly converted;
- A detailed mapping of legacy data fields to the fields in the new solution;

- A detailed conversion schedule including all steps, tasks, activities, events, milestones, and resources necessary for the selected Offeror to convert the legacy data to the new solution; and
- Resolution plan for records with conversion data issues.
- Address data must be converted according to USPS standards including Zip +4.

Offeror Response

As described in Section VI.H, the Data Conversion effort is a key success factor for replacing Pennsylvania's SURE system. Bad data can overshadow everything else that is positive about a project. Further, quality testing a data conversion can be problematic because it is impractical to open and review every record and sampling is not very effective. BPro has developed a conversion process that ensures that all data is successfully mapped and accurately transferred into the TotalVote system. BPro ensures a quality delivery of data and images and will affirm the team's confidence in the new system implementation.

BPro is experienced with the data structure of voter registration data and data conversions through our successful delivery of election systems in six states. This includes building the South Dakota and Washington Voter Registration systems, which changed from "bottom-up" to "top-down" models with the implementation of TotalVote. In addition, BPro has built data exchanges for our customers to participate in both ERIC and Cross Check, in order to compare voter registration data with other states.

Our plan for Pennsylvania is to extract as much data as possible from the state repository and then fill in any missing pieces from each of your 67 county databases. Data that may only reside in county systems would include images, signatures, and transactional history. Our conversion process includes a number of data validation techniques, both automated and manual, to ensure all data is transferred correctly. The effort may require a BPro data conversion analyst on-site at each county. Having someone on-site will shorten the time needed to extract and convert each county's data plus add a level of security by not having to send data electronically.

b. The selected Offeror shall plan and execute all activities necessary to convert the data from the current systems into the new solution, including the training, testing, and the production environment at implementation. The current application(s) in use shall continue to be usable until the fully implemented solution has been accepted by DOS.

Offeror Response

BPro's process does not rely on data sampling to ensure quality data. BPro's conversion process will verify the converted content of all tables by comparing metrics supplied by backend queries against the legacy system.

- When a data set is harvested from Pennsylvania's legacy system for a conversion, the legacy data is retained as a query-able database.

- A series of counting queries are built to evaluate the content for each field. For an example – one query is built to count of the number of records that have the first name beginning with each level of the alphabet, returning an array of the 26 letters and a record count for each. (Another query would count the same for middle name, and another for last name, etc.) These queries are compiled in preparation for testing the conversion.
- BPro performs the conversion and applies the dataset to TotalVote tables.
- Testing the conversion: Inside the TotalVote application, the user searches on first name of "A*" (wildcard) and a count is returned. That count should match the query from the legacy system. This search is repeated for all letters of the alphabet and matched against the original SQL query results. There should be no exceptions that cannot be accounted for.
    - The example is repeated for all text fields. Tests can also be run for the last character in a text string.
    - The same example is used for numeric fields, testing for the first digit, and/or the last digit value, and retrieving value (0-9) counts for each field.
    - Date fields can be counted for months (how many birth dates in May), or counts of the day values, or counts of the year values.

c. For each iteration of the data conversion, testing is required. The selected Offeror shall report test results to DOS. Test results shall be used to discover and remediate errors and to refine the process in order to achieve accurate results. Data cleansing will be performed by the Offeror and reviewed and approved by the DOS. The selected Offeror shall identify data requiring cleansing to achieve conversion success.

Offeror Response

BPro recommends that a Database Analyst (DBA) from the DOS Project Team will work directly with BPro's DBA to create processes to extract data and images from the SURE system. Together the DBAs of both teams will create extract, transmit and load procedures (ETL) for moving the data and images to TotalVote. The DBAs will coordinate with the Business Analyst(s) and the Quality Analyst(s) to ensure the processes for conversion deliver a product with data integrity, meeting all quality standards, and created in TotalVote in a manner that is fully consumable into the business process and software logic of the BPro system.

The DOS Team will provide a data dictionary of the SURE system data structure and full data extracts. The BPro DBA will work to fully analyze the data sets against the data structure of every field. BPro will document the mapping of data to the TotalVote system and present small trial conversions for verification. Legacy fields that do not have an "exact fit" will be reviewed with the DOS Team to determine the best course. For example: does the field contain data that needs to be used as input to logic on the TotalVote system, and if yes, how must the value in the field be stored in TotalVote?

BPro has special routines to evaluate all the unique code values for all fields that are coded, such as district, precincts, polling places, etc. These fields will usually be evaluated first and confirmed with DOS.

d. The selected Offeror shall perform final conversion of data into the configured and successfully tested solution, including the final conversion into the production environment at implementation. Data conversion into the production environment shall require approval by the DOS.

Offeror Response

Prior to the final data migration, the team will run at least one test migration to identify problems, bottlenecks and to capture metrics at key migration checkpoints. The resulting timing metrics will provide the input for scheduling of the final conversion. This conversion approach ensures that all records are correctly transferred without the need to conduct random spot checks of data from individual records. It also provides timing statistics necessary for scheduling the conversion. In addition to being more efficient, BPro's conversion strategy has proven to be more effective in each implementation we have successfully completed.

e. The selected Offeror shall provide the following to the DOS for review and acceptance:

- Data Conversion and Validation Plan;
- Data Conversion Schedule with dependencies and task owners;
- Final Conversion Test Results showing all Data has been successfully converted into the Test and Training Environment; and
- Final Data Conversion into the Production Environment.

Offeror Response

If selected, BPro will provide a Data Conversion and Validation Plan. The Data Conversion Plan will include the following:

- Data Conversion Schedule with dependencies and task owners
- Final Conversion Test Results showing all Data has been successfully converted into the Test and Staging environments
- Final Data Conversion into the Production Environment.

f. The selected Offeror shall submit confirmation of the successful implementation of the configured solution and interfaces into all environments agreed to with the DOS.

Deliverables:

- **Data Migration, Conversion and Validation Plan**
- **Data Conversion Schedule**
- **Final Conversion Test Results** showing all Data has been successfully converted into the Test and Training Environment; and
- **Final Data Conversion Report** showing the successful conversion and migration of the data and exceptions.

I. The selected Offeror shall work with the Department on an annual basis to review, update, and test continuity and disaster recovery plans for the proposed solution with key business partners

Deliverable:

- **A finalized COOP/Disaster Recovery Plan** and schedule to annually update and exercise the plan.

J. **Training.** The selected Offeror shall provide a training plan for both onsite and online for both the DOS, county election officials, and designated support staff. The selected Offeror shall provide a formal user guide or job aid (both hard copy and electronic format) describing in detail the use and functionality within the solution, published training documentation, and provide application training and development. The selected Offeror must establish a formal user guide or job aid for all system functionality. DOS will determine by security roles what functions the end users will utilize. The user guides or job aid shall be available online, in a secure manner, and DOS shall have the option to print or copy training materials for future training conducted by DOS. The training material shall be owned by the Commonwealth and available in editable formats. The training plan will be subject to review and approval by the DOS. The time frame for the training plan will be mutually agreed upon between DOS and the selected Offeror.

a. The selected Offeror shall design and deliver a train-the-trainers program for DOS to use to provide basic training to end-users. The selected Offeror shall provide training sessions to prepare staff designated by DOS.

Offeror Response

As detailed in previous responses, User Training for TotalVote will take place after development has been completed for all modules and prior to User Acceptance Testing (UAT). BPro will use a "train the trainer" methodology to train DOS personnel to become 'super users' of the software. This train-the-trainer training will be led by Dakota Bixler, BPro's TotalVote lead subject matter expert. After the DOS personnel are adequately trained, they will be prepared to handle support and training for all end users, including County staff. BPro trainers will join DOS personnel for two weeks of regional trainings around the state for County staff. This will

serve to both train County staff and reinforce the expertise of DOS 'super users' in the TotalVote system.

All hands-on software training (for both DOS and County user training sessions) will take place in a Testing environment, configured identically to the Production environment.

b. Offeror shall propose a training methodology for the project. At a minimum DOS requires on-site training in Harrisburg, Pennsylvania for approximately 30 DOS staff or contractors who will act as trainers to train additional system users. On-site training shall be followed by on demand web-based sessions or eLearning modules, used for reinforcement and additional skill development. The selected Offeror shall provide online training throughout the contract, and any new features, modifications, or enhancements resulting from this RFP.

Offeror Response

User Training for TotalVote will take place after development has been completed for all modules and prior to User Acceptance Testing (UAT). BPro will use a "train the trainer" methodology to train DOS personnel to become "super users" of the software. This train-the-trainer training will be led by the BPro Training Lead and TotalVote lead subject matter expert. After the DOS personnel are adequately trained, they will be prepared to handle support and training for all end users including County staff. DOS personnel will join BPro trainers for two weeks of regional trainings around the state for County staff. This will serve to both train County staff and reinforce the expertise of DOS "super users" in the TotalVote system.

All hands-on software training (for both DOS and County user training sessions) will take place in a Training (Staging) environment configured identically to the Production environment.

Training Approach and Curriculum

For the "train-the-trainer" training sessions, BPro will work with the DOS to finalize a user training schedule and plan. The scope of the DOS training shall encompass two parts: 1) State user training, and 2) Training County users on all TotalVote modules.

BPro will provide the following on-site "train the trainer" sessions for DOS-designated training staff:

- Provide training to DOS trainers on all modules completed throughout the Project (relevant to both State and County users)
- Assist DOS staff in the use of BPro-provided training materials
- Facilitate a dry run of the training session and make recommendations to DOS staff on clarity, flow, and accuracy of training presentation
- Make modifications to training materials as necessary

Training for DOS-designated training staff will be conducted by BPro on-site over the course of one week (Monday through Friday). Attendance for all five days of training is required for DOS-designated training staff. Locations, training equipment, and printed materials will be provided by the DOS office (training materials will be created by BPro and provided electronically to the

DOS prior to training.) During the course of each day, BPro will demonstrate the components of all modules. Users will log in and practice functional tasks in small groups at individual workstations, while using individual logins from a variety of user groups for both State and County permissions.

Every day, the training will focus the content on:

- Training Materials
- Module overview
- How to perform designated tasks within each module
- How to verify output of tasks
- Reporting
- Review

c. The selected Offeror shall provide system administrator training to approximately 10 DOS, Commonwealth, or contractors. This on-site training shall be held in Harrisburg, Pennsylvania.

Offeror Response

BPro will provide system administrator training in Harrisburg, PA, either concurrently to the Train the Trainer trainings or at a separate time.

d. The selected Offeror shall provide training schedule notification thirty (30) days in advance for all training session(s). Also, final training material must be delivered 5 days in advance of the training session. All training materials must be approved by DOS. The selected Offeror shall be responsible for updating training materials, upon system changes, throughout the contract term.

Offeror Response

All trainings will be scheduled at least 30 days prior and all DOS-approved will be delivered 5 days in advance of the training session. BPro will be responsible for updating training materials throughout the life of the contract.

e. The selected Offeror shall provide options for on-site, including training options held in Harrisburg, PA or satellite locations, which could be county election offices or Commonwealth facilities, for county election official trainings across the Commonwealth, or online training after the solution is implemented. The DOS shall be considered a resource to assist with identifying locations for training purposes. All training sessions, including the location and training curriculum, must be approved by DOS and can be requested by DOS, as needed. The selected Offeror shall be responsible for developing and updating training materials, with approval from DOS, prior to the training sessions.

Offeror Response

After the completion of the "train the trainer" week of training sessions, DOS staff and BPro staff will conduct hands-on training for County staff. This training will be held in regional locations throughout the state that ensure the highest levels of participation. DOS and BPro will coordinate the final schedule, arrangements, and communication for regional County trainings.

Team BPro shall provide the following activities regarding on-site training for County staff:

- Assist with the setup of the training facility(ies), such as setting up a dedicated workstation with hardware for printing, scanning, and document imaging
- Attend all training sessions for the entire duration to answer any questions DOS cannot answer, and provide assistance regarding system operation
- Assist in troubleshooting technical issues that may arise during initial setup or during the sessions

For the County training, BPro will conduct formal review sessions to allow the trainers an opportunity to review and provide feedback on each training session for improvement. (Feedback may be gathered verbally or from feedback forms collected from attendees at the County trainings.) A short review session at the end of each day would be valuable to discuss areas for training improvement, as well as a weekly report submitted on Fridays to wrap up all findings during each of the training sessions. A final post-mortem with DOS staff and BPro will be conducted via conference call after all regional training is complete, and BPro will produce a final User Training report for DOS.

Deliverable:

- **A finalized training plan** and schedule to address the needs of the project.
- **Training documentation** for designated users geared specifically toward the solution functions of each end-user. Include materials such as workbooks, exercises and examples as well as handouts and aids.
- **County user training sessions**
- **DOS user training sessions**

K. Release Management. The selected Offeror shall provide release planning, design, and prioritization services based on the agreed upon system lifecycle management methodology that defines the scope of the impacted services for each release as it relates to and impacts the solution.

1. **Requirement Management.** The Offeror shall conduct requirements sessions to collect and document fully defined requirements. The Offeror shall update or develop documentation as required. The Offeror shall manage the requirements of the release ensuring the requirements traceability.

2. **Testing.** The Offeror shall create a testing strategy and plan that ensures software quality, accessibility, and usability following the release implementation. Testing required may include, but is not limited to, unit testing, systems integration testing, accessibility and usability, security testing, regression testing, user acceptance testing, and stress and load testing.

3. **Training.** The Offeror shall provide support on an as-needed basis to the DOS in the development of training documentation and delivery depending upon the scope of the release.

4. **Documentation.** The Offeror shall update or create documentation for each release as applicable to the nature of the release. Documentation types may include, but are not limited to, technical, system operations, and user training.

5. **Release Closeout and Final Acceptance.** Within 2 business days following the release, the selected Offeror shall provide the DOS project manager with a letter certifying that the release is complete with no major issues.

   A 4 week stabilization period will follow each release implementation. During this time, the Offeror shall work with DOS to monitor the system, collect issues, conduct maintenance activities, and identify and prioritize defects. Following the stabilization period, the Offeror shall prepare the release closeout report within 5 business days.

Deliverables: Release Plans
Final Release Package to include**:**
- **Requirements Documentation**
- **Test Result Report** for all types of testing performed
- **Release Documentation**
- **Release Closeout Final Report**
- **Release Security Documentation and Testing Results**

Training Documentation creation or maintenance as needed
Training Delivery as needed

L. Stress and Load Testing. The selected Offeror shall conduct semi-annual stress and load testing so that the performance characteristics and the performance failure points of the solution may be fully understood. The Offeror shall explain its testing strategy. The Offeror shall develop stress and load testing plan and execute testing in accordance with its plan. The Offeror shall describe its strategy for stress and load testing, including how it intends to execute and manage these services.

Offeror Response

If selected, BPro will provide semi-annual stress and load testing. These tests will generate both page and transactional loads on the system to simulate real-life interaction with the product. Working with DOS, BPro will determine a baseline load of the site, typically 80% of average usage, and a maximum load, typically 125% of maximum usage. Tests will initially be executed for 10 minutes and increased to 15 and 20 minutes. Tests are executed in single functional and cross-functional to identify issues that may occur across multiple modules when they interact.

In order to provide Stress and Load Testing, BPro will provide services necessary to complete tests including:
1) Monitoring systems and databases in real time during tests;
2) Reviewing load test scripts;
3) Generating reports showing system loads and database statistics as relevant; and
4) Analyzing system reports with events during test to discover root cause.

Deliverable: Stress and Load Testing Results Report

IX. Maintenance and Support. All solution support and maintenance will be subject to review and approval by DOS. All solution support and maintenance activity time frames will be mutually agreed to between DOS and the Offeror. These tasks shall include, but not be limited to, the following:

Solution Support. The selected Offeror shall provide solution support services as described in **Section VI.DD Solution Support**.

Offeror Response

BPro will provide software maintenance support services as part of this contract effort. In addition to the standard maintenance and support contract, a mutually agreed SLA will be developed to suit DOS requirements.

The following services are provided as a part of the standard maintenance and support:

- Unlimited Over-the Phone and Email End User Support
- Unlimited Bug Fixes and training, documentation updates and technical support in support of the releases due to bug fixes.
- Patches and Upgrades to support ongoing architectural changes and MS Windows, Browser updates and Microsoft SQL Server upgrades.
- Weekly status meetings/conference calls.

1. **Maintenance.**

   a. The selected Offeror shall perform all system maintenance needed to ensure the solution remains operational and meets the requirements of this RFP.

b. The selected Offeror shall provide any software upgrade which impacts core functionality of the solution at no additional charge throughout the term of the contract.

c. The selected Offeror shall provide a maintenance and release schedule at the beginning of each calendar year through the term of the contract. DOS shall be notified of any schedule changes prior to release.

d. The selected Offeror shall notify the DOS of any additional upgrade, which is considered an additional feature to the solution and not part of the base package, when it becomes available. Anything that is considered part of the Offeror's base package shall have no additional cost to the Commonwealth. The DOS, at its sole discretion, may choose to purchase the feature. The selected Offeror must provide a written quote for the additional features, for DOS approval.

e. No system upgrade shall be performed without DOS approval, especially during deadline or election blackout periods. The selected Offeror and DOS shall mutually agree upon blackout period time periods and requirements.

Offeror Response

If selected, BPro will ensure the solution remains operational and meets the requirements of this RFP throughout the entirety of the contract. During the warranty period, DOS will receive all patches and upgrades free of charge. Patches and upgrades are also covered under the support and maintenance agreement after the warranty period expires. Major and minor upgrades are handled on a mutually agreed upon schedule, typically annual and monthly bases respectfully. Major Product Enhancements, as determined by BPro, will be quoted as a separate, additional cost. No system upgrade or product enhancement will be performed without DOS approval.

2. Change Control.

a. The change management process shall be used to manage all system changes including, but not limited to, changes for defect management, system maintenance, and enhancements. DOS currently uses a hybrid solution of ServiceNOW and Microsoft's Team Foundation Server (TFS) as its change management solution.

b. All changes to the solution must be approved by the DOS prior to the change implementation.

c. The selected Offeror shall be responsible for change management to include, but not be limited to, change request tracking, approvals process, and communication approach. Offeror shall describe its change management approach that shall be used for this project to include, but not be limited to,

how it plans to identify, evaluate, document, prioritize, categorize, resolve, and close-out changes.

d. The Offeror shall also describe how it will support DOS change management.

Offeror Response

Fixes take an elevated priority, as any bugs in the system may need to be corrected expeditiously. Internally, there is a simple error reporting screen built into the site if the user encounters a system error. This screen should be filled out and submitted by the end user to immediately report the error to BPro development staff. These system errors and any other discovered bugs (that may not prompt an error screen) need to be reported by end users (both DOS and County staff) to the DOS Project Manager. All system changes should go through the DOS Project Manager, who in turn, reports it to BPro for analysis. Bugs should be recreated by the user before being reported to BPro. An error reporting ticket template will be used to submit issues to BPro. Details shall include which user reported the error, when it was reported, and how the error was created, along with information about the "before" step and what was the expected outcome (that did not occur). DOS staff will create an online job ticket for BPro, including the error reporting template along with any additional details and screenshots. Enough detail should be provided from DOS that BPro can recreate the issue. BPro will fix the issue in the Sandbox environment and test it before letting the DOS know it has been resolved and is available to be tested on their end. With approval, the change will be ready for the next time code is updated in the Production Environment. For fixes, BPro can provide updates as requested by the DOS Project Manager on an as-needed basis. Each software release will be recorded by BPro with release number and documented with itemized fixes included in the update.

3. **User Documentation.** The Offeror shall provide electronic versions of all documentation, in a format acceptable to DOS, and employ change control processes and version control to ensure documentation is kept current for the duration of the purchase order (PO) resulting from this RFP. Where appropriate, a table of contents, an index, and keywords shall be available for information searching. DOS, at its discretion, may request or accept printed documentation on a case by case basis. User documentation shall include, but not be limited to, data models, data dictionaries, and user guides.

Offeror Response

BPro provides data models, data dictionaries, documentation for system administrators, as well as support for end users. All system documentation will be located on BPro's SharePoint and protected against unauthorized access, both internally and externally. End user support, including user manuals and guides, is available within the TotalVote application and accessible through any browser. During M&O, if newly defined requirements result in a brand-new feature or a change to user experience, BPro will update the user manuals and guides to reflect the changes to the system.

4. **Reporting.** The selected Offeror shall submit a Monthly SLA and Status reports as described in **Section VIII, Reports and Project Control**. The selected Offeror shall also describe and define the reporting capabilities of the proposed solution and which control or reporting abilities are available to both DOS and county election officials. They Offeror shall further define which reports come standard or requires customization.

Offeror Response

In addition to the TotalVote Data Generator, which allows authorized users to search almost any data in the system, BPro has developed an extensive collection of preformatted, static reports built into the main product because reporting, especially statistical reporting and voter listings, are essential to the many facets of management of elections. This is true on both the county and state level and users with appropriate permissions from both DOS and county election offices will have access to preformatted reports and use of the Data Generator. Reports can be exported to Word (rtf), Excel, CSV or printed to PDF format.

5. **Controls.** The selected Offeror shall submit an annual report on data and access controls, including where the data resides, who has access, and how access rights are maintained; encryption approach; and incident capabilities, including logging and forensics.

Offeror Response

If selected, BPro will prepare an annual report on data and access controls.

X. Exit from hosting. The Department shall have sole authority to terminate hosting services provided by the Offeror. If the Department decides to exit from hosting and either seek another hosted solution or utilize Commonwealth hosting facilities, the Offeror shall draft a hosting transition plan. The hosting transition plan shall include, but not be limited to, a timeline for all activities required to support the transfer of hosting including the installation and configuration of the software and the migration of the data and the Offeror resources that will support the effort including the project manager.

The Offeror shall assist the Department in migrating the hosted environments as they exist in the solution to another hosting provider to minimize downtime, preserve continuity of operations, and ensure no loss of data. The detail of the services to be provided and the documented exist process shall be approved by the Department during the exit planning stage. The Offeror shall assist the Department in conducting an exit from hosting test prior to the actual exit from hosting and full testing of the solution to ensure it is operational and meets all requirements.

If necessary, the Offeror shall provide all Commonwealth data in a format that is acceptable to the Commonwealth such as SQL backups. In the event other data exists (e.g. data exchange files) that is not natively stored in the solution it will be provided in a format it was stored in within the solution platform or a format acceptable to the Commonwealth.

Offeror Response

If selected, BPro will fully assist in the transition in hosting platforms or services.

Deliverables: Hosting Transition Plan
Test Plan
Test Results
Final Hosting Migration Results Report

XI. Outgoing Transition/Knowledge Transfer. The selected Offeror shall cooperate with the DOS and any subsequent contractor in any activities related to turnover of responsibilities. The selected Offeror shall also engage in on-going Knowledge Transfer activities throughout the life of the Contract. This shall include updating all system documentation, mentoring Commonwealth staff, and working with any Commonwealth partners. Knowledge Transfer shall be provided through documentation, mentoring, training, and meetings.

Additionally, the selected Offeror shall develop an outgoing transition plan when requested by DOS. The outgoing transition plan shall include, but is not limited to, content migration and knowledge transfer activities. And, the Offeror shall work with the incoming Contractor to support the seamless transition of services. The selected Offeror shall deliver a final report to DOS showing the successful completion of all turnover activities and confirmation that all Commonwealth data has been returned to the Commonwealth and that no data resides with the Offeror. This plan shall include at a minimum:

- Knowledge transfer approach;
- End use training approach (including training location, format, total training hours, number of employees trained, timing and signoff process);
- Administrator training approach (including training location, format, total training hours, number of employees trained, timing and signoff process);
- Transition/cutover approach;
- Rollout support approach (the DOS expects on-site support during rollout);
- Responsibilities for the Offeror, the DOS, or county election officials for each of the above (e.g., facilities, scheduling, training content, etc); and
- Expected deliverables to accomplish Outgoing Transition/Knowledge Transfer activities.

All Outgoing Transition/Knowledge Transfer activities are subject to DOS review and approval. The timeline for all transitions and knowledge transfer activities will be mutually agreed upon between DOS and the selected Offeror.

Offeror Response

If selected, BPro will fully assist with all Outgoing Transition/Knowledge Transfer activities as requested by DOS.

Deliverable:
Outgoing Transition Plan reviewed and accepted by DOS.

Final Report Showing the Successful Completion of Turnover Activities

XII. Reports and Project Control.

The selected Offeror shall provide project management services throughout the life of the project. The selected Offeror shall create, maintain, and execute the following plans, reports, and supporting documentation in a format agreed to by the Commonwealth. Offerors shall submit its project management methodology and/or draft plans which it proposes to use for this project. The selected Offeror must submit a final plan(s) within an agreed upon time after receiving the notice to proceed. All plans are subject to Commonwealth approval. The project management timeframes shall be mutally agreed upon between the DOS and the Offeror.

A. Project Management Plan. The project management shall include, but not limited to, the following:

1. **Project Plan.** The project plan must describe the scope of work for the project and how the scope will be managed. The project plan shall act as a confirmation of project scope, phasing, implementation objectives, and be detailed enough to ensure the product is delivered on time, within projected estimates, and meets all requirements as specified in the RFP. The project plan must include, but is not limited to:

    - Project Scope Statement;
    - Proposed project phases;
    - Team roles, including subcontractors;
    - Scope Management Process;
    - Major Milestones /Deliverables;
    - Work Breakdown Structure (WBS);
    - Timeline;
    - Critical paths;
    - Dependencies;
    - Resources;
    - Success factors; and
    - Assumptions

2. **Project Status.** Project status shall be tracked and reported on an ongoing basis. Reguarly scheduled status meetings between the DOS and the Contractor Project Manager shall be held to discuss project progress, issues, resolutions and next steps. Additionally, a Project Information Library (PIL) shall be

developed and maintained by the Contractor at a location approved by the DOS and overseen by the DOS. It shall be a single repository used to store, organize, track, control, and disseminate all information and items produced by and delivered to the project. The PIL shall include a file structure with defined access and permissions. It shall also include an interface, such as a web page or portal, where individuals can obtain project information and the latest documentation to the project team. The DOS shall be the owner of all documents available in the PIL. The DOS can provide access to a SharePoint site to assist with project status reports and other requiremetns outlined in the RFP.

The following standard reporting mechanisms shall be used:

a. Status reports
b. Issues lists
c. Risk management updates

3. **Requirements Management Plan.** The requirements management plan must describe the process and approach to manage and address requirements throughout the life of the project. The requirements management plan shall include:

- Requirements Management Process
- Roles and Responsibilities
- Requirements Traceability Matrix (RTM)

4. **Risk Management Plan.** The risk management plan must describe the approach used to manage risk throughout the life of the project, how contingency plans are implemented, and how project reserves are allocated to handle the risks. The plan will include the methods for identifying risks, tracking risks, documenting response strategies, and communicating risk information. The risk management plan shall include:

- Risk Management Process;
- Roles and Responsibilities;
- Rules/Procedures;
- Risk Impact Analysis Approach;
- Risk Owners
- Risk appetite (to coorelate between the Offeror's risk and the DOS's risk appetite)
- Tools
  - \

5. **Issue Management Plan.** The issue management plan must describe the approach for capturing and managing issues throughout the life of the project to ensure the project is moving forward and avoids unnecessary delays. The issues management plan shall include:

    - Issues Management Approach
    - Roles and Responsibilities
    - Tools

6. **Change Control Management Plan.** The change control management plan must describe the approach to effectively manage changes throughout the life of a project. The plan will include the process to track change requests from submittal to final disposition (submission, coordination, review, evaluation, categorization), the method used to communicate change requests and their status (approved, deferred, or rejected), the escalation process if changes cannot be resolved by the review team, and the process for project re-baselining. The change control management plan shall include:

    - Change Management Process
    - Roles and Responsibilities
    - Rules/Procedures
    - Change Impact Analysis Approach
    - Tools

7. **Communications Management Plan.** The communication management plan must describe the communications process that will be used throughout the life of the project. The process must include the tools and techniques that will provide timely and appropriate generation, collection, distribution, storage, retrieval and disposition of project information. The communications management plan shall include:

    - Communications Management Process
    - Roles and Responsibilities
    - Reporting Tools and Techniques
    - Meeting Types and Frequency

8. **Quality Management Plan.** The quality management plan must describe the approach used to address Quality Assurance (QA) and Quality Control (QC) throughout the life of the project. The quality management plan should identify the quality processes and practices including the periodic reviews, audits and the testing strategy for key deliverables. The plan should also include the criteria by which quality is measured, the tolerances required of product and project deliverables, how compliance is measured, and the process

for addressing those instances whenever quality measures are out of tolerance or compliance. The Qualityf Management Plan will be maintained throughout the life of the project to include changes or updates between the Offeror and the DOS. The quality management plan will include:

- Quality Management Process;
- Roles and Responsibilities;
- Tools;
- Quality Standards;
- Testing and Promotion Process;
- User acceptance process;
- Responsibilities for each of the above; and
- Expected Deliverables.

The Quality Management Plan will be mutually agreed upon between the Offeror and the DOS.

9. **Time Management Plan.** The time management plan must describe the process for controlling the proposed schedule and how the achievement of tasks and milestones will be identified and reported. The plan must also detail the process to identify, resolve, and report resolution of problems such as schedule slippage. The time management plan will include:

- Time Management Process
- Role and Responsibilities
- Tools and Techniques
- Work Plan

Where appropriate, a PERT or GANTT chart display should be used to show project, task, and time relationship.

Offeror Response

The Project Management Plan for the Commonwealth of Pennsylvania (PA) TotalVote project is considered to be a living document that will be updated routinely in coordination with the State's project manager (PM) to successfully guide the project to completion. The intent of the content is to convey the tools, techniques, and processes BPro will engage the PA Department of State's (DOS) Election Division to keep stakeholders informed, to manage expectations, and to deliver a product to the satisfaction of the project's stakeholders.

The intended audience for this document is all members of the PA TotalVote Project Team. The Project Management Plan employs standard PMP principals in managing the project that may not be well understood by all members. We consciously invite all members of the Project Team

to review any part of this document for collaborative understanding to allow us together to carry out the intended plan of this project.

Related Documents
Documents not enclosed in this file and referenced here are:

a. Project Schedule
b. Issues Log
c. Risk Register
d. Training Plan
e. Testing Plan

1. Project Plan

Project Scope Statement
The scope statement is to replace the current SURE system for the Commonwealth of Pennsylvania (PA) with a modern election system. Modules or components included in the scope of this project include the following:

- TotalVote
    - Voter Registration System
    - Election Management System
    - Petitions
    - Notifications
    - Advanced Search
    - Precinct and District Management
    - Reports
    - UOCAVA
- Voter Information Portal
- Voter Registration API
- Election Night Reporting System
- Online Absentee Application
- Data Exchanges and Interfaces
    - Lobbying Disclosure System
    - Campaign Finance System
    - Department of Health – Deceased Voter
    - Pollbooks
    - PennDOT
    - ERIC
    - PA DOS Secure FTP
    - Pre- and Post-Election Audits
- Campaign Finance System
- Lobbying Disclosure

Proposed Project Phases

The proposed project phases of the PA DOS TotalVote project include the following:

- Project Initiation
- Requirements Validation
- System modification and customization
- Training
- Formal Testing Events
- Implementation to Production State
- Transition to Maintenance

Team Roles

The following members will serve to govern the project. Each role is defined further below in *Roles and Responsibilities* of each plan within the PMP.

BPro Project Team

Role	Name
BPro Project Manager	Kari Stulken
BPro Account Manager	Kari Stulken
BPro Product Manager (Solutions Architect)	Kevin Kumpf
BPro Testing Lead	Laura Heckmann
BPro Business Analyst	Dakota Bixler
BPro Training Lead	Dakota Bixler
BPro Infrastructure and Security Lead	Joshua Daws

Scope Management Process

The scope management process includes processes that are required to ensure a successful completion of the project.

The process groups involved in project scope management are as follows:

- Collect Requirements
  - It is the process of defining and documenting stakeholders need to meet the project activities.
  - The document for collecting requirements will be refined in the project planning phase.
- Define Scope
  - The scope of the project will be detailed in the response to this RFP.
  - The scope will be refined as the requirements are evaluated during the GAP analysis task.
- Create Work Breakdown Structure (WBS)
  - The WBS was created by breaking down the project into the phases and tasks BPro will utilize during the course of this project.

    - The project schedule was based upon previous experience on similar projects.
- Verify (or Validate) Scope
    - This process includes reviewing the deliverables with the PA DOS to ensure they are completed satisfactorily and obtain formal acceptance by the PA DOS.
- Control Scope
    - This process group monitors the status of the project and product scope so that changes to the scope baseline can be managed properly.

Major Milestones and Deliverables

The deliverables of this project as outlined in the RFP are as follows:

- Implementation Planning
    - Finalized Implementation Plan Approved by DOS
- Implementation of the Solution
    - Requirements Package
    - Configuration Confirmation Report for all agreed to environment reviewed and approved by DOS
    - Detailed Solution and Interface Design Document and Interface Delivery Specification
    - Fully Configured Solution and Interfaces Reviewed and Accepted by DOS
    - Test Plan and Test Scenarios
    - Final Implementation Report
- Data Conversion and Validation
    - Data Conversion and Validation Plan Approved by DOS
    - Data Conversion Schedule
    - Final Conversion Test Results
    - Final Data Conversion Report
- Training
    - Finalized Training Plan
    - Training Documentation
    - County User Training Session(s)
    - DOS User Training Session(s)
- Exit from Hosting
    - Hosting Transition Plan
    - Test Plan
    - Test Results
    - Final Hosting Migration Results Report
- Outgoing Transition
    - Outgoing Transition Plan Reviewed and Accepted by DOS
    - Final Report Showing the Successful Completion of Turnover Activities

The delivery of these milestones will be deliverable-based and displayed in the draft schedule below.

Work Breakdown Structure (WBS)

This is the draft WBS for the PA DOS TotalVote project. It will be updated and refined at the beginning of the project during Project Initiation.

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Pennsylvania DOS TotalVote Project**	**463 days**	**Mon 3/2/20**	**Tue 12/28/21**		
2	**Project Kick-off Meeting**	**8 days**	**Mon 3/2/20**	**Wed 3/11/20**		
3	Schedule Project Kick-off Meeting	2 days	**Mon 3/2/20**	Tue 3/3/20		BPro PM
4	Conduct Project Kick-off Meeting	1 day	Wed 3/11/20	Wed 3/11/20	3FS+5 days	BPro PM
5	**Project Management**					
6	*Deliverable B.1: Weekly Status Report*	*455 days*	*Mon 3/9/20*	*Wed 12/22/21*	*3FS+3 days*	BPro PM
7	Project Status Meetings	455 days	Mon 3/9/20	Wed 12/22/21	3FS+3 days	BPro PM
8	*Deliverable B.2: Submit Final Implementation Report*	*3 days*	*Thu 12/23/21*	*Tue 12/28/21*	*6*	BPro PM
9	**Project Initiation**	**6 days**	**Mon 3/2/20**	**Mon 3/9/20**		
10	Establish Project Stakeholders	0.5 days	Wed 3/4/20	Wed 3/4/20	3	BPro PM
11	Establish Project Team	0.5 days	Wed 3/4/20	Wed 3/4/20	10	BPro PM
12	Establish Project Team Roster	0.5 days	Thu 3/5/20	Thu 3/5/20	11	BPro PM
13	Establish Core Team Members	0.5 days	Thu 3/5/20	Thu 3/5/20	12	BPro PM
14	Establish Requirements Analysis Schedule	3 days	Fri 3/6/20	Tue 3/10/20	13	BPro PM
15	Communicate Schedule to Core Team	1 day	Wed 3/11/20	Wed 3/11/20	14	BPro PM
16	**Project Planning**	**239 days**	**Mon 3/2/20**	**Tue 2/9/21**		
17	**Project Management Plans**	**45 days**	**Mon 3/2/20**	**Fri 5/1/20**		
18	*Deliverable A.1: Finalized Implementation Plan*	10 days	Mon 3/2/20	Fri 3/13/20		BPro PM
19	Develop Project Schedule	5 days	Mon 3/2/20	Fri 3/6/20		BPro PM
20	**Develop Project Management Plan (PMP)**	**35 days**	**Mon 3/16/20**	**Fri 5/1/20**	**18**	

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
21	Develop Requirements Management Plan	5 days	Mon 3/16/20	Fri 3/20/20	15	BPro PM
22	Develop Risk Management Plan	5 days	Mon 3/23/20	Fri 3/27/20	21	BPro PM
23	Develop Issue Management Plan	5 days	Mon 3/30/20	Fri 4/3/20	22	BPro PM
24	Develop Change Control Management Plan	5 days	Mon 4/6/20	Fri 4/10/20	23	BPro PM
25	Develop Communications Management Plan	5 days	Mon 4/13/20	Fri 4/17/20	24	BPro PM
26	Develop Quality Management Plan	5 days	Mon 4/20/20	Fri 4/24/20	25	BPro PM
27	Develop Time Management Plan	5 days	Mon 4/27/20	Fri 5/1/20	26	BPro PM
28	**Requirements Analysis and Specifications**	**33 days**	**Mon 3/2/20**	**Wed 4/15/20**		
29	Requirements Gap Analysis to TotalVote Baseline	10 days	Thu 3/12/20	Wed 3/25/20	15	BPro Team,PA DOS
30	Enter user stories into TFS	10 days	Mon 3/2/20	Fri 3/13/20		BPro BA
31	*Deliverable C.1: Finalized Requirement documents*	*5 days*	*Thu 4/9/20*	*Wed 4/15/20*	*33*	BPro BA
32	*Deliverable C.2: Requirements Traceability Matrix*	*5 days*	*Thu 3/26/20*	*Wed 4/1/20*	*29*	BPro BA
33	*Deliverable C.3: GAP analysis document*	*5 days*	*Thu 4/2/20*	*Wed 4/8/20*	*32*	BPro BA
34	**Infrastructure - Configuration of Environments**	**80 days**	**Tue 3/10/20**	**Tue 6/30/20**		
35	Configure and Set-up Development Environment	10 days	Tue 3/10/20	Mon 3/23/20	9	BPro Dev Team
36	*Deliverable D.1: Submit Configuration Confirmation Report - Development*	*5 days*	*Tue 3/24/20*	*Mon 3/30/20*	*35*	BPro PM
37	Configure and Set-up Staging Environment	10 days	Tue 4/7/20	Mon 4/20/20	36FS+5 days	BPro Dev Team
38	*Deliverable D.1: Submit Configuration Confirmation Report - Staging*	*5 days*	*Tue 4/21/20*	*Mon 4/27/20*	*37*	BPro PM
39	Configure and Set-up Production Environment	10 days	Tue 5/5/20	Mon 5/18/20	38FS+5 days	BPro Dev Team
40	*Deliverable D.1: Submit Configuration Confirmation Report - Production*	*5 days*	*Tue 5/19/20*	*Tue 5/26/20*	*39*	BPro PM
41	Configure and Set-up Disaster Recovery Environment	10 days	Wed 6/10/20	Tue 6/23/20	40FS+10 days	BPro Dev Team

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
42	*Deliverable D.1: Submit Configuration Confirmation Report - Disaster Recovery*	*5 days*	*Wed 6/24/20*	*Tue 6/30/20*	*41*	BPro PM
43	*Deliverable E.1: Solution Interface and Design Document*	*20 days*	*Mon 3/16/20*	*Fri 4/10/20*	*30*	BPro Product Manager, BPro BA
44	**Software Development Life Cycle (SDLC) Plans**	**309 days**	**Thu 4/16/20**	**Wed 7/7/21**		
45	*Deliverable G.1: Develop Test Plan*	*10 days*	*Thu 4/16/20*	*Wed 4/29/20*	*28*	BPro PM
46	*Deliverable G.1: Develop Test Scenarios*	*10 days*	*Tue 6/22/21*	*Wed 7/7/21*	*127SF*	*BPro BA*
47	*Deliverable H.1: Develop Data Migration, Conversion, and Validation Plan (See Data Conversion Block for the map)*	*10 days*	*Thu 4/30/20*	*Wed 5/13/20*	*45*	*BPro PM*
48	*Deliverable K.1: Develop Configuration and Release Management Plan*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	*BPro PM*
49	**Transformation Management Plans**	**20 days**	**Thu 5/14/20**	**Thu 6/11/20**		
50	*Deliverable I.1: Develop COOP/Disaster Recovery Plan*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	BPro PM
51	*Deliverable J.1: Develop Training Plan*	*10 days*	*Fri 5/29/20*	*Thu 6/11/20*	*50*	BPro PM
52	**Data Conversion and Validation**	**336 days**	**Tue 3/10/20**	**Tue 7/6/21**	**9**	
53	**Initial Data Collection and Clean-up**	**55 days**	**Tue 3/10/20**	**Tue 5/26/20**		
54	Get Initial Datasets from PA DOS & Counties	15 days	Tue 3/10/20	Mon 3/30/20		PA DOS PM
55	Data Staging, Analysis	10 days	Tue 3/31/20	Mon 4/13/20	54	BPro SQL DBA
56	Data Clean-up with Counties and DOS	20 days	Tue 4/14/20	Mon 5/11/20	55	BPro SQL DBA,PA DOS
57	Analysis and Clarification Sessions	20 days	Tue 4/14/20	Mon 5/11/20	55	BPro SQL DBA
58	Document Clarifications	10 days	Tue 5/12/20	Tue 5/26/20	57	BPro SQL DBA
59	**Data Migration and Conversion**	**336 days**	**Tue 3/10/20**	**Tue 7/6/21**		
60	*Deliverable H.1: Develop Data Mapping and Translation Documents (Data Dictionary)*	*10 days*	*Wed 5/27/20*	*Tue 6/9/20*	*58*	BPro SQL DBA
61	*Deliverable H.2: Develop Data Conversion Schedule*	*10 days*	*Thu 5/14/20*	*Thu 5/28/20*	*47*	BPro PM

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
62	Data Migration and Conversion - Dev Environment	5 days	Wed 6/10/20	Tue 6/16/20	60	BPro SQL DBA
63	Data Migration and Conversion - Staging Environment	5 days	Wed 6/17/20	Tue 6/23/20	37,62	BPro SQL DBA
64	*Deliverable H.3: Submit Final Conversion Test Results (After success conversion to Test) Translation Documents (Data Dictionary)*	5 days	Tue 3/10/20	Mon 3/16/20		BPro PM
65	Data Migration and Conversion - Production Environment	5 days	Tue 6/15/21	Mon 6/21/21	39,64,115	BPro SQL DBA
66	Data Migration and Conversion - Disaster Recovery Environment	5 days	Tue 6/22/21	Mon 6/28/21	41,65	BPro SQL DBA
67	*Deliverable H.3: Submit Final Conversion Test Results (After success conversion to Disaster Recovery) Translation Documents (Data Dictionary)*	5 days	Tue 6/29/21	Tue 7/6/21	66	BPro PM
68	**Development Construction & Customization**	**280 days**	**Wed 6/17/20**	**Mon 7/26/21**	**35,62**	BPro Dev Team
124	*Deliverable F.1: Fully Configured Solution and Interfaces*	*5 days*	*Tue 7/27/21*	*Mon 8/2/21*	*68*	BPro PM
125	**Training**	**65 days**	**Tue 6/15/21**	**Wed 9/15/21**		
126	Update Training Plan	5 days	Tue 6/15/21	Mon 6/21/21	115	BPro PM
127	Create Training Materials	25 days	Wed 7/7/21	Tue 8/10/21	118	BPro BA
128	*Deliverable J.2: Provide Training Documentation & Materials*	*5 days*	*Wed 8/11/21*	*Tue 8/17/21*	*127*	BPro BA
129	Coordinate Training Locations, Schedule, and Organization	5 days	Tue 6/22/21	Mon 6/28/21	126	BPro PM
130	*Deliverable J.4: Conduct DOS User Training Sessions*	*5 days*	*Wed 8/18/21*	*Tue 8/24/21*	*127FS+5 days*	BPro BA
131	*Deliverable J.3: Conduct County User Training Sessions*	*10 days*	*Wed 9/1/21*	*Wed 9/15/21*	*130FS+5 days*	BPro BA
132	**User Acceptance Testing (UAT) #1**	**10 days**	**Thu 9/16/21**	**Wed 9/29/21**		
133	UAT Testing Support	5 days	Thu 9/16/21	Wed 9/22/21	131	BPro Team
134	Prepare UAT Results and Completion Report	5 days	Thu 9/23/21	Wed 9/29/21	133	BPro PM
135	Incorporate UAT Test Feedback into TotalVote	10 days	Thu 9/30/21	Wed 10/13/21	132	BPro Dev Team
136	**User Acceptance Testing (UAT) #2**	**10 days**	**Fri 11/5/21**	**Thu 11/18/21**		

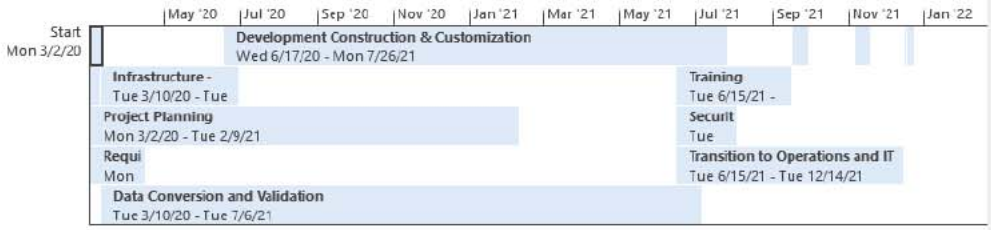
	Task Name	Duration	Start	Finish	Predecessors	Resource Names
137	UAT Testing Support	5 days	Fri 11/5/21	Thu 11/11/21	135	BPro Team
138	Prepare UAT Results and Completion Report	5 days	Fri 11/12/21	Thu 11/18/21	137	BPro PM
139	Incorporate UAT Test Feedback into TotalVote	10 days	Fri 11/19/21	Mon 12/6/21	136	BPro Dev Team
140	**Documentation**	**347 days**	**Mon 3/2/20**	**Tue 7/13/21**		
141	Prepare Interface and Service Diagram	5 days	Mon 3/2/20	Fri 3/6/20		BPro Product Manager
142	Prepare database model and schema for core tables	5 days	Tue 6/22/21	Mon 6/28/21	141,146	BPro SQL DBA
143	Prepare high-level security architecture diagram	5 days	Tue 6/29/21	Tue 7/6/21	142	BPro Product Manager
144	Prepare application architecture diagram	5 days	Wed 7/7/21	Tue 7/13/21	143	BPro Product Manager
145	**Security and IT Policy Compliance**	**35 days**	**Tue 6/15/21**	**Tue 8/3/21**		
146	Prepare Security Design Checklist	5 days	Tue 6/15/21	Mon 6/21/21	115	BPro Product Manager
147	Provide Application Security Assessment Support	10 days	Tue 6/22/21	Tue 7/6/21	146	BPro Product Manager
148	Collaborate with PA DOS IT to evaluate and prioritize security vulnerabilities	20 days	Wed 7/7/21	Tue 8/3/21	147	BPro Product Manager
149	Provide documentation of security coding practices	5 days	Wed 7/7/21	Tue 7/13/21	147	BPro Product Manager
150	***Deliverable L.1: Provide Stress and Load Testing Support***	***5 days***	***Thu 9/30/21***	***Wed 10/6/21***		
151	Load and Stress Test Readiness	5 days	Thu 9/30/21	Wed 10/6/21	132	BPro Dev Team
152	**Transition to Operations and IT Training**	**127 days**	**Tue 6/15/21**	**Tue 12/14/21**		
153	**Deployment Readiness**	**127 days**	**Tue 6/15/21**	**Tue 12/14/21**		
154	Update Implementation and Deployment Plan	25 days	Tue 6/15/21	Tue 7/20/21	115	BPro PM
155	Prepare User Documentation	20 days	Wed 8/18/21	Wed 9/15/21	128	BPro Product Manager
156	Conduct Implementation Readiness Checks	10 days	Fri 11/19/21	Mon 12/6/21	132,136	BPro Product Manager
157	Prepare Systems Operations Documentation	30 days	Thu 9/16/21	Wed 10/27/21	155	BPro Product Manager

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
158	Conduct training to state technical staff	2 days	Thu 10/28/21	Fri 10/29/21	157	BPro Product Manager
159	Perform tasks in transitions to operations checklist	1 day	Tue 12/7/21	Tue 12/7/21	156	BPro Product Manager
160	*Deliverable K.2: Submit Final Release Package*	*5 days*	*Wed 12/8/21*	*Tue 12/14/21*	*159*	BPro Product Manager
161	**Production Deployment**	**2 days**	**Wed 12/15/21**	**Thu 12/16/21**		
162	Review production readiness checklist	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
163	Data cut-over from legacy system	1 day	Wed 12/15/21	Wed 12/15/21	153	PA DOS
164	Production Data Conversions	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro SQL DBA
165	Production Application Cutover	1 day	Wed 12/15/21	Wed 12/15/21	153	BPro Product Manager
166	County and State Testing of Implemented Sites	1 day	Thu 12/16/21	Thu 12/16/21	165	PA DOS
167	Go-Live Support	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Dev Team
168	**Project Closeout**	**5 days**	**Fri 12/17/21**	**Thu 12/23/21**		
169	Prepare and Process Project Closeout Checklist	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro Product Manager
170	Update all system documentation for project closeout	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
171	*Deliverable H.4: Submit Final Conversion Report*	*1 day*	*Fri 12/17/21*	*Fri 12/17/21*	*161*	BPro PM
172	Complete warranty and transition to maintenance and operations	5 days	Fri 12/17/21	Thu 12/23/21	161	BPro PM
173	**Maintenance and Support Annual Tasks**	**1 day**	**Mon 12/27/21**	**Mon 12/5/24**	**168**	
174	Application Stabilization Support	4 wks	Mon 12/27/21	Mon 1/24/22	167	BPro Dev Team
175	Enter maintenance period	0 days	Sat 1/1/22	Sat 1/1/22		
176	Provide maintenance and release schedule in early January	5 days	Wed 1/5/22	Tue 1/11/22		BPro Product Manager
177	Update COOP/Disaster Recovery Plan	5 days	Thu 12/1/22	Wed 12/7/22		BPro Product Manager
178	Provide maintenance and release schedule in early January	5 days	Thu 1/5/23	Wed 1/11/23		BPro Product Manager

	Task Name	Duration	Start	Finish	Predecessors	Resource Names
179	Update COOP/Disaster Recovery Plan	5 days	Fri 12/1/23	Thu 12/7/23		BPro Product Manager
180	Provide maintenance and release schedule in early January	5 days	Fri 1/5/24	Thu 1/11/24		BPro Product Manager
181	Update COOP/Disaster Recovery Plan	5 days	Sun 12/1/24	Thu 12/5/24		BPro Product Manager
182	**Non-MVP Project Work Placeholder (Start Date and Duration will be coordinated with PA DOS PM)**	TBD	2022	2022	168	BPro Dev Team

Timeline

The timeline of the main portion of the project excluding the maintenance years is as shown:



Any tasks identified during the development construction phase of the project which are not considered to be part of the minimum viable product (MVP) will be moved to a non-MVP project work placeholder block. This work will be done after the project has been moved to production. The 2022 start date and duration of this placeholder block will be determined at the beginning of the project and adjusted prior to the end of the project to fit the business needs of PA DOS and their 2022 schedule.

Critical Paths

The project schedule outlined above has several critical tasks include requirements validation and analysis, development construction, training materials, training, and testing tasks.

Development tasks and user stories determined not to be associated with the critical path of the project or part of the minimum viable product will be moved to the non-MVP project work placeholder block. This non-MVP block will allow the BPro developers to focus on the technical and functional requirements of the project.

Some of the critical tasks are displayed in the following table:

Task Name	Start	Finish	Late Start	Late Finish	Free Slack	Total Slack
Pennsylvania DOS TotalVote Project	**Mon 3/2/20**	**Tue 12/28/21**	**Mon 3/2/20**	**Thu 12/5/24**	**0 days**	**0 days**
Project Kick-off Meeting	**Mon 3/2/20**	**Wed 3/11/20**	**Thu 3/26/20**	**Thu 12/5/24**	**18 days**	**18 days**
Project Planning	**Mon 3/2/20**	**Tue 2/9/21**	**Wed 7/1/20**	**Thu 12/5/24**	**86 days**	**86 days**
Data Conversion and Validation	**Tue 3/10/20**	**Tue 7/6/21**	**Tue 4/7/20**	**Thu 12/5/24**	**20 days**	**20 days**
Development Construction & Customization	**Wed 6/17/20**	**Mon 7/26/21**	**Thu 7/16/20**	**Thu 11/28/24**	**0 days**	**20 days**
Training	**Tue 6/15/21**	**Wed 9/15/21**	**Wed 8/4/21**	**Thu 12/5/24**	**35 days**	**35 days**
User Acceptance Testing (UAT) #1	**Thu 9/16/21**	**Wed 9/29/21**	**Thu 10/14/21**	**Wed 10/27/21**	**0 days**	**20 days**
Incorporate UAT Test Feedback into TotalVote	Thu 9/30/21	Wed 10/13/21	Thu 10/28/21	Wed 11/10/21	16 days	20 days
User Acceptance Testing (UAT) #2	**Fri 11/5/21**	**Thu 11/18/21**	**Thu 11/11/21**	**Wed 11/24/21**	**0 days**	**4 days**
Transition to Operations and IT Training	**Tue 6/15/21**	**Tue 12/14/21**	**Wed 10/6/21**	**Mon 12/20/21**	**4 days**	**4 days**
Production Deployment	**Wed 12/15/21**	**Thu 12/16/21**	**Tue 12/21/21**	**Wed 12/22/21**	**0 days**	**4 days**
Project Closeout	**Fri 12/17/21**	**Thu 12/23/21**	**Thu 12/23/21**	**Thu 12/30/21**	**0 days**	**4 days**

Dependencies

Dependencies to the project include the following:

- Having clear requirements at the beginning of the project or refined prior to the development sprint they are taken into for construction.
- The development and test environments are set up and ready for the first development sprint.
- The data to be converted and migrated for the project is ready at the beginning of the project so it can be tested and reviewed throughout the course of the project.
- The award and contracting tasks are concluded in early 2020 so the project can start as close as possible to March 2, 2020.

The project schedule was organized so that information can be gathered during the requirements validation and analysis tasks not only for the requirements included in the RFP but also the standard terms can be identified. There will be a development sprint 0 iteration included in the development construction block so that the TotalVote screens can be updated with the standard terms Pennsylvania uses along with adding any additional fields critical to the system. The data conversion process will start prior to the development tasks so that the Pennsylvania data can be used in initializing the system. It is generally preferred by our clients to see their own data in the TotalVote system instead of mocked up voter records.

Resources
The primary resources for the project impact the critical path of the project. The developers are a critical element of the project's schedule. Sprint development cycles will utilize the developers' available capacity during each sprint. The BPro Product Manager will assist prior to and during the sprint planning meetings to level the requirements against the developers' time and expertise so that each development sprint will deliver a set of requirements allowing the project team to meet the project target date.

Success Factors
For this project to be successful, the following needs to be met:

- Project completes prior to 12/31/2021.
- Project is completed within the agreed upon budget (including approved change requests).
- Project delivers the requirements of the RFP which are determined to be included in the scope of the project.
- PA DOS is satisfied with the delivered system.
- Certain major risks do not materialize.
- If risks occur, they are well managed.

Assumptions
Assumptions of BPro:

- Users will be available to test during the time they agree to.
- Training facility and logistics will be the responsibility of the PA DOS.
- Funding for the project has been secured by PA DOS.
- Project scope will not change once DOS PM signs off on the scope and acceptance criteria of the requirements.
- Project will follow an Agile Scrum development process for the configuration, development, and customization of the software.
- This project will have the full support of DOS's PM, project sponsor, stakeholders, and project team.
- The purpose of this project will be communicated within DOS and to County Election Administrators prior to deployment.
- Statewide shapefiles will be provided for use with the TotalAddress functionality.

Assumptions of DOS:

- The TotalVote Software and System will be able to replace the existing SURE system.
- The schedule will be accomplished as stated in the approved schedule.
- Minor adjustments to Project Scope and functional requirements will be allowed that don't delay project implementation or success in order to replicate and accommodate critical business functions of the existing election system.

2. Project Status

Project status reports summarize key project status and performance measures for the past week. It also reports on the status of deliverables, action items, and project milestones. Project Status reports are compiled weekly and distributed to the core Project Team the day prior to the weekly Project Status meeting.

Depending on project activities and progress, the PA DOS Project Manager has the option to change the frequency of the Project Status Report.

Project Status Meetings
The weekly status meeting will consist of the core project team and additional project resources as needed. Project status meetings may be held via web conferencing if not all team members are on site to meet in person.

The project status meeting should review the weekly status report, give specifics on any new risks or issues resolved or unresolved that occurred since the last status meeting; as well as, go over project activities scheduled for the next week. It is also a time to discuss project milestones, project deliverables, and the project schedule itself.

Sample Project Status Report

PA DOS TotalVote Project

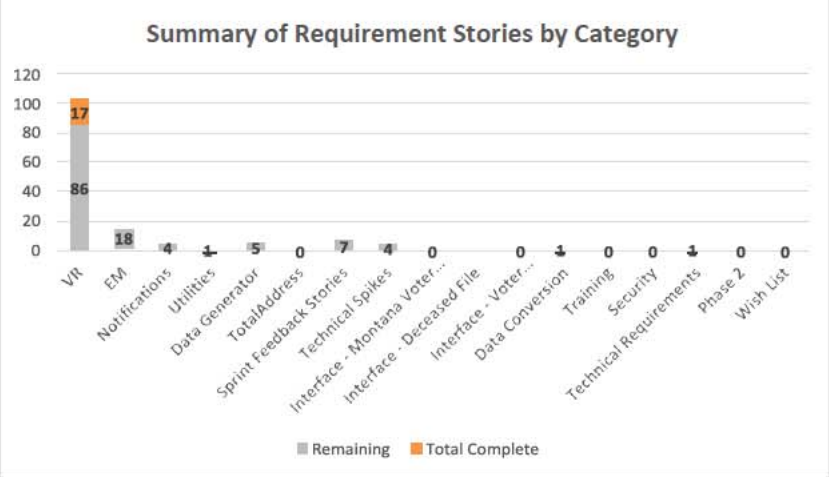
Weekly Status Report

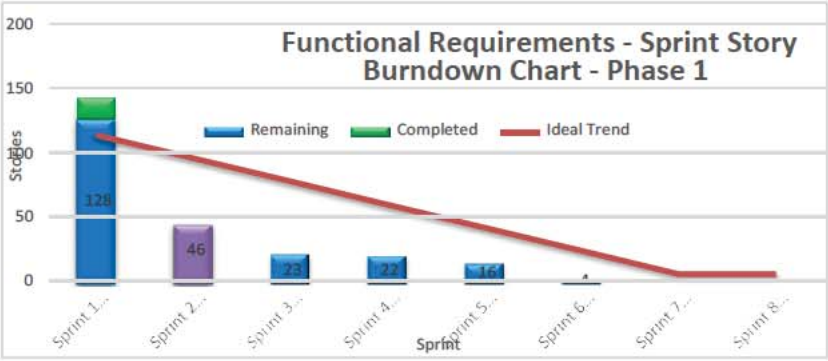
Status Report Date:				
Submitted By:	Kari Stulken, BPro Project Manager			
Work Accomplished During This Period				
• Accomplishments listed •				
Work Planned for Next Period				
• Items listed •				
Deliverables				
Del #	**Deliverable Name**	**Current Status**	**Target Date**	**Notes**
A.1	Finalized Implementation Plan	Active	03/13/2020	•
C.1	Finalized Requirement Documents	Active	04/15/2020	•
C.2	Requirements Traceability Matrix	Active	04/01/2020	•
Unresolved Issues				
Issue	**Urgency (High, Medium, Low)**	**Responsible**	**Decision/Action**	

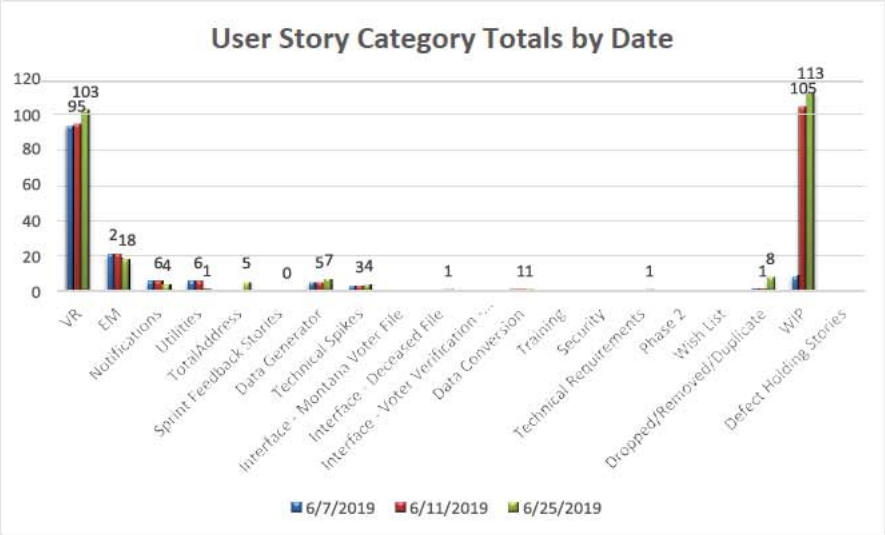
Action Items			
Action Item	**Assigned**	**Assigned Date**	**Status**	**Comments**

Sprint and User Story Statistics

The following charts show a snapshot of user story statistics as of this report date. As additional requirements are added to the project in the form of user stories, these statistics will evolve. After user stories are reviewed for acceptance, the statistics will be updated to reflect any modifications.







3. Requirements Management Plan

Requirements Management Process

The deliverables of the project are defined in the project's contract and will govern the project.

The PA DOS TotalVote system is not a custom developed application built from the ground-up. It is a configuration of BPro's TotalVote application to meet the requirements defined in the PA DOS SURE RFP. In accordance with this goal, the requirements analysis will be based mostly on the analysis of the baseline TotalVote application functionality and what is required to be

configured or adapted per the RFP and the laws and requirements of the Commonwealth of Pennsylvania to implement TotalVote as a replacement of SURE.

The following steps define the methodology that will be used for the PA DOS TotalVote system requirements analysis:

1. BPro will use the requirements summary from the RFP as the baseline of all requirements along with the User Stories derived from those requirement sets and provided by PA DOS.
2. The DOS Functional and Technical Requirements and User Stories will serve as the starting point to populate work items in BPro's Team Foundation Server (TFS). Software modules will be built using an Agile Scrum approach. Information on what requirements are met "out of the box" and those that need to be configured or changed will also be in TFS. BPro and the DOS Product Owner will update TFS to ensure that the work items are updated with acceptance criteria by working with the PA DOS Product Owner and the BPro Development Team.
3. Sprint Grooming, Sprint Planning, and Sprint Review sessions will be scheduled with the PA DOS Project Team to go through each work item to build, clarify, or verify acceptance criteria for the RFP requirements.
4. The project will use DOS Use Cases, requirements, and user stories provided for review and discussion with the PA DOS SMEs for clarification and elaboration.
5. BPro SMEs will work with the PS DOS SMEs as follows:
   a. Validate if the work item as listed is valid and correct.
   b. Elaborate the work item, if needed.
   c. Demonstrate how the requirement is being met in the baseline TotalVote application.
6. Record in TFS any work item or task that needs to be addressed.

The BPro Team will execute the following plan for requirements development for the PA DOS TotalVote Project:

1. Identify SMEs and team members that will participate in the Scrum sessions from both PA DOS and BPro Scrum Teams.
2. Establish a high-level schedule for sessions as well as the best method for conducting these sessions: in-person, online, etc. The high-level schedule will be tracked as part of the overall project schedule and the detailed meetings will be setup actively on an ongoing basis in consultation with the PA DOS Project Manager and PA DOS Product Owner.
3. Use the RFP functional and technical documents and user stories as the baseline requirements.
4. Conduct gap analysis sessions for each functional and technical module with PA DOS SMEs to elaborate, refine, and capture the gap requirements.
5. Establish the final requirements for the functional and technical deliverables in TFS for development tracking and traceability.
6. Perform Sprint meeting activities to finalize work items' acceptance criteria for each software module deliverable.
7. The approved work items will be placed in the product backlog of TFS based on priority.

8. The approved work items will be taken into development sprints based upon team capacity, necessary sequence, and priority order.
9. Work items will be managed within TFS from backlog through sprint development, testing, and delivery to the Product Owner for acceptance.

The approved requirements listing may be amended with mutual consent via a contract amendment or other established change control procedures as approved by the PA DOS PM and accepted by BPro.

All requirements and their status will be captured in the project's BPro TFS**.** Items may be "deferred" (to be done later) or "dropped" (requirement not needed anymore). In addition to this, there may be an "enhancement" which is a new requirement that is over and above the scope of work as outlined in the approved set of requirements. These will require a change request.

TFS Work Items will be reviewed during each Sprint process periodically with the Product Owner. During these reviews, the direction for the "Deferred" or "Dropped" requirements, and "Enhancements" will be determined. Decisions for prioritization will be provided by PA DOS PM and the effort estimates and pricing along with the feasibility of delivering them within the desired timeframe will be provide by BPro. Once there is agreement and change control process is executed, the requirement will be put on a delivery schedule.

Deferred Requirements

Any requirement may be "deferred" which means it can be moved to a later phase or time in the project. If any requirement in the original scope of the project is deferred, PA DOS PM and BPro PM will review the constraints and reasons for deferring and determine a mutually acceptable timeframe for delivering the requirement based on the business priority and the effort involved.

BPro will determine if moving the requirement to a later sprint or phase of the project will cost more effort and additional cost to deliver these items and provide revised estimates to the PA DOS PM. If the revised estimates are approved, PA DOS will need to pay only for the effort that is over and above the original estimate. This amount can be adjusted against the credit value of dropped requirements. The requirement will be worked after mutual agreement and change control procedures are executed.

Dropped Requirements

Any requirement may also be "dropped," which means that the PA DOS Product Owner determines that the requirement is no longer needed.

- If a requirement is "dropped", BPro will evaluate the balance of the allocated dollar value left on the requirement and consider that as a credit.

- If the credit value of dropped requirements is not used – then its residual value will be zero. BPro will not owe PA DOS any refunds or monies in lieu of the unused credit value for any "Dropped" or "Deferred" requirements.

Enhancements

An "Enhancement" is a new requirement that is over and above the scope of work initially defined for the project as per the approved original requirements set.

- BPro will provide effort estimates for enhancements.
- BPro will work on enhancements approved by the PA DOS Product Owner on a case by case basis.
- An enhancement can only be worked on once it is approved by the PA DOS PM via the change control process.

Roles and Responsibilities

The roles involved in the requirements management process include the following:

Role	Name	Organization	Responsibilities
Product Owner	TBD	PA DOS	• Responsible for bridging the gap between the development team and the stakeholders. • Ensures the Development Team understands what needs to be build and when. • Collaborates with development team on a regular basis. • Manages the product backlog. • Gathers input and feedback from stakeholders. • Defines acceptance criteria for each product backlog item. • Ensure the acceptance criteria is met through testing of each delivered user story. • Prioritizes the work items in the product backlog. • Acts as key participant in sprint-related meetings by explaining items, their scope, and the value it holds.
Scrum Master	Kari Stulken	BPro	• Responsible for facilitating the Development Team and the Product Owner to work on the day-to-day development activities.

			• Acts as an Agile Coach for both the Development Team and the Product Owner. • Facilitates and organizes all scrum events. • Removes impediments that impact the team's productivity. • Safeguards the Scrum Team from outside interference and distraction so the team can remain focused on delivering the best quality and value at the end of each sprint. • Serves as the servant leader of the Scrum Team. • Enable the team make process improvements so they can complete their sprint goals.
PA DOS Business Analyst	TBD	PA DOS	• Provides support to the Product Owner. • Not a key role in the sprint meetings but a supporting role.
Development Team	BPro Development Team	BPro	• Responsible for delivering the sprint goal at the end of each sprint. • Self-organized and cross-functional. • Selects the user stories from the prioritized sprint backlog to take into each sprint.
Business Analyst	Dakota Bixler	BPro	• Member of the development team in sprint meetings. • Provides assistance to the reporting tasks of the meeting. • Reports estimates for tasks.
Product Manager	Kevin Kumpf	BPro	• Provide estimates for tasks. • Member of the development team. • Provides support for the development team by attending requirements and other supporting meetings.

Requirements Traceability Matrix (RTM)

The Requirements Matrix will track the project requirements found in the request for proposal (RFP). The requirements will be stored in BPro's Team Foundation Server (TFS) project for scheduling, tracking, monitoring, and reporting purposes.

For each requirement, the following information will be tracked:

a. Requirement Area
b. Requirement Number (as assigned in the Source document)

c. Requirement Title - A short title (for conversation labeling)
d. The full text of the requirement
e. Multiple activities to process the decisions towards final acceptance
    a. Date
    b. Clarification
    c. Verification/Validation
    d. Group
    e. TFS ID (will be assigned as the requirement is entered into Team Foundation Server)
f. Response Code "Whether"
    a. F = Fully Met (Requirement will be fully and completely met.)
    b. N = Not Met (Requirement will not be met.)
    c. P = Partially Met (Requirement will be partially met. Please indicate in the comments field an explanation as to which part is met and which part is not.)

4. Risk Management Plan

Risk Management Process
This project presents many areas of risk and Risk Management will be critical for Scope Management, Quality Management, and Schedule Management. Risks can be mitigated through documenting. Proposed plans can be made to avoid impact of the risk, managed to reduce impact or likelihood of impact, or realized when impact is unavoidable and simply monitored.

Risk Mitigation is the ultimate goal of the PA DOS ensuring that risks do not impact the project, project team, or quality of the delivery.

BPro will confer with the PA DOS project team to define and recognize the risks of the project which are events that if they occurred would impact the success of the project. During risk discussions, the team will develop strategies to either prevent the risk from occurring or reduce the impact if the risk should occur.

Risk items are documented in the Risk Register. A preliminary Risk Register developed by the BPro Team is shown below. The BPro Project Manager will revisit the status of risk items at each project status meeting with the intent of covering:

a. Current status of the risk
b. Current impressions on whether indicators of the risk occurring have been observed, and whether a change to projected Impact or Probability is merited
c. Whether any adjustments in the proposed strategy are needed

R#	Title Description	Factors	Strategies	Notes	Indicators	Probability	Impact	Last Updated
1	Maintaining Day-to-Day Operations while Implementing Managing business process change; transitioning from the old to the new without impairing the ability for the PA DOS staff to carry out day-to-day duties	Resources changed Processes	Review upcoming work. Review Schedule with resource assignments		Missed meetings, missed training, late response to delivered software	Med	Low	10/30/2019
2	Managing Expectations Managing stakeholder's expectations as the project changes	Availability of key personnel	Keep all affected persons knowledgeable of the current state of the project with the same vision. Issues Log, Status Reports		Failed deliverables. Voiced dissatisfaction. Expectations not being expressed by stakeholders.	Med	Med	10/30/2019
3	Scope Management Maintaining Scope and Cost; BPro expects to pursue this project as a partnership with PA DOS.		Focus on the RFP Requirements		Expectations of deliverables outside the RFP Requirements	High	Med	10/30/2019

	Scope and associated cost must be continually monitored against the overall baselines and controlled for a successful project.							

Roles and Responsibilities

The roles and responsibilities table defines the lead, support, and other project members who are responsible for risk management activities throughout the project life cycle.

Role	Organization	Responsibilities
Project Manager	BPro	• Compile and approve the Risk Management Plan. • Defines the risk management approach. • Participates in the risk management process. • Takes ownership of risk mitigation, planning, and execution.
Risk Officer	PA DOS	• Leads the risk management effort. • Sponsors risk identification activities. • Facilitates communication throughout the execution of the risk management process. • Ensures the Risk Register is maintained and that the statuses assigned to risks and risk activities are current. • Provides the Project Manager with recommendations and status regarding risk actions.
Executive Sponsor	PA DOS	• The Agency executive who provides the financial resources and business authority for the project. • Provides input to risk mitigation strategies.
Project Sponsor	PA DOS	• Acts as the business manager responsible for ensuring that the needs and accomplishments within the business area are widely known and understood. • Ensures that the design of the system meets both the functional and non-functional business goals. • Provides input to risk mitigation strategies.

Rules and Procedures
The procedure which will be used to manage risk is outlined in this section:

- **Identify the Risk:** Brainstorm with the project team possible risks for the project and record the risks identified in the risk register.
- **Analyze the Risk:** Determine and record in the risk register how likely each risk is to happen.
- **Prioritize the Risk:** Categorize the risks in the risk register to be high, medium, or low.
- **Assign an Owner to the Risk:** Determine and record the assignment in the risk register on the person which is responsible for the risk, identify when it is occurring, and will lead the work towards resolving the risk if it should occur.
- **Respond to the Risk:** Create a plan to mitigate each major risk identified including in the strategy some preventative or contingency plan.
- **Monitor the Risk:** The person listed in the risk register as responsible for the risk needs to track progress towards resolving the risk.

Risk Impact Analysis Approach
A probability and impact matrix will be utilized to map the probability of each risk occurrence and its impact on the project objectives in the event that risk occurs. Individual project risks are assigned a priority level based on the combination of their assessed impact and probability. BPro PM will work with the PA DOS PM to determine the preferred method to calculate the risk probability and impact values.

Risk Owners
The risk owner is the person responsible for monitoring the risks and for selecting and implementing an appropriate risk response strategy. The risk owner will be identified for each risk found in the risk register.

Risk Appetite
Risk appetite is the degree of uncertainty an organization or individual is willing to accept in anticipation of a reward. In the case of the PA DOS TotalVote project, this item will be defined at the beginning of the project during Project Initiation phase.

Tools
The Risk Register for this project is the primary log for risks, their risk score (Likelihood of impact * Effect of Impact), and strategies to manage those risks.

5. Issue Management Plan

Issues Management Approach
Issues management is the process of identifying and resolving issues experienced within the life of the project. Since issues can arise with no warning, the PA DOS TotalVote project needs to have an approach identified to handle these unexpected matters that can either negatively or positively impact the project.

Issues may take the form of problems, gaps, inconsistencies, or conflicts. Issues will be recorded and tracked in the Issues Log.

The issues log will record the issue and responsibility assignment so the issue can be tracked as soon as it is identified through resolution. The resolution will be recorded for future reference and project learning.

Decisions are also marked in the Issues Log for understanding and acknowledgement of decisions that have been made that affect the direction of the project.

Impediments are considered to be temporary issues that are preventing work from progressing forward. When a work task cannot move forward before something else is accomplished or corrected, that is an impediment. Documenting these kinds of issues serves to present clear understanding to the team that this issue is impacting progress of the project.

The BPro Project Manager will revisit the status of the Issues Log at each project meeting with the intent of:

e. Updating current status of any identified issues
f. Following up on action items previously assigned
g. Developing new action items as needed
h. Adding new issues as needed

Issues: Roles and Responsibilities
The BPro PM will be responsible for keeping the issues log updated. The PA DOS PM will assist in identifying and assigning a responsible person to track the issue through to resolution.

Issues: Tools
An Issues Log records concerns and unknowns of the project. The Issues Log is a list maintained in the project status report and is regularly reviewed at project meetings. The Issues Log template which will be used in the project status report is as follows:

Issue ID#	Issue Title/Description	Report Date / Resolved Date	Status (Active, Closed)	Action Plan

6. Change Control Management Plan

The components of change management include:

- Scope Planning and Baseline
- Scope Definition and Verification
- Change Control Process
- Change Control Documents

Change and scope management are critical components of project management.

The Change management plan is based on the following goals:

- To monitor the needs of the various stakeholders of the project.
- To incorporate requirements or needs that may have been missed or not anticipated at project start.
- To assess new requirements or needs for change including effort, resource, time, and budget impacts.
- To evaluate the impact of the change and determine whether the changes are critical to the success of the project and if they need to be undertaken.
- Manage each change request from initiation through to closure.
- Process change requests based upon the direction the Project Sponsor sees is needed.
- Communicate the impact of changes to appropriate project staff.
- Allow small changes to be managed with a minimum of overhead.

Change Management Process

There are several types of changes which may be requested and considered for the PA DOS TotalVote Project. Depending on the extent and type of proposed changes, changes to project documentation and the communication of these changes will be required to include any approved changes into the project plan and ensure all stakeholders are notified.

Three categories of change may occur and are managed within the project:

- Major Change
    - This change would trigger the need for Executive/CCB Board approval.
    - Any change that alters the overall budget, scope, or process such that agreements in the Contract must be amended.
    - Have material impact +/- 10% on timeline or cost.
    - Has the potential to substantially increase risk or impacts the ultimate security of the system.
- Process Change
    - This would be a substantial change in agreed upon process.
    - These are logged by the PA DOS Project Manager with the sign off by the BPro Project Manager without approval from CCB.
- Minor Change
    - This type of change is managed by native Agile processes such as grooming, sprint planning, Product Owner review, etc.
    - Changes to user stories for functional or technical requirements within scope or that shift scope/budget below the CCB criteria.
    - Minor changes are handled in the Team Foundation Server (TFS) workflow.
    - Approval and acceptance of these minor changes to user stories or additional user stories are part of the natural TFS Agile flow.

Types of changes include:

- Scheduling Changes: changes which will impact the approved project schedule. These changes may require modifications to the schedule depending on the significance of the impact. Re-baselining the project should trigger the change request process.
- Budget Changes: changes which will impact the approved project budget. These changes may require requesting additional funding, releasing funding which would no longer be required, or adding to project or management reserves. If these require changes to the cost baseline, they should be considered major in nature.
- Scope Changes: changes which are necessary and impact the project's scope which may be the result of unforeseen requirements which were not initially planned for. These changes may also impact budget and schedule. These changes may require revision to WBS, project scope statement, and other project documentation as necessary. If there are changes which causes the project scope to shift, delivery time to shift, or the cost to change, this is considered a major change.

Roles and Responsibilities
The following are the roles and responsibilities for all change management efforts related to the PA DOS TotalVote Project:

Project Sponsor:
- Approve all changes to budget/funding allocations
- Approve all changes to schedule baseline
- Approve any change in project scope

Project Director:
- Chair the Change Control Board (CCB)
- Approve all changes to budget/funding allocations
- Approve all changes to schedule baseline
- Approve any change in project scope

Project Managers:
- Receive and log all change requests from project stakeholders assisting them with the completion of the form as necessary
- Conduct preliminary risk, cost, schedule, scope analysis of change prior to CCB
- Seek clarification from change requestors on any open issues or concerns
- Make documentation revisions/edits as necessary for all approved changes
- Participate in CCB
- Ensure any approved change is communicated to the project team and stakeholders
- Ensure that changes are captured in the project documentation where necessary

Project Team/Stakeholders:
- Submit all major change requests on change request form or work with PM to complete the form
- Provide all applicable information and detail on change request forms

- Be prepared to address questions regarding any submitted change requests
- Provide feedback as necessary on impact of proposed changes

Change Control Board

The Change Control Board (CCB) is the approval authority for all proposed change requests that impact the overall Scope, Schedule, or Cost having impact on the Contract. The purpose of the CCB is to review all change requests, determine their impacts on the project risk, scope, cost, and schedule, and to approve or deny substantial changes that impact contractual agreements. Project changes within the functionality will be handled by standard Agile process (see below). For changes impacting the Contract, the change will be submitted by either the Contractor or DOS Project Manager and reviewed and approved by the CCB.

The CCB will be composed of the following project team members:

Name	Position	CCB Role
TBD	PA DOS Project Sponsor	CCB Member
TBD	PA DOS Program Manager	CCB Member
TBD	PA DOS Project Manager	CCB Chair
Brandon Campea	BPro President	CCB Member

As change requests are submitted to either the Contract or PA DOS Project Manager by the project team/stakeholders, the receiving PM will log the requests in the change log and notify and review with the other PM. The CCB will review all change requests that impact the Contract. For a change request to be approved, all CCB members must vote in favor. In the event more information is needed for a particular change request, the request will be deferred and sent back to the requestor for more information or clarification.

Rules and Procedures

The seven rules of change management:

- People drive change
- Communication is a two-way street
- Today's world is digital; strategize should be digital-based
- Data fuels success
- Mature change strategy wins
- Change requires leaders
- Project team needs to be open to change

The Change Control Process for the PA DOS TotalVote Project will follow the below defined procedure. The PA DOS project manager has overall responsibility for executing the change management process for each change request.

1. Identify the need for a change (Stakeholders) – Change requestor will submit a completed change request form to the project manager.

2. Log change in the change request register (Project Manager) – The project manager will keep a log of all submitted change requests throughout the project's lifecycle.
3. Evaluate the change (Project Manager, Team, Requestor) – The project manager will conduct a preliminary analysis on the impact of the change to risk, cost, schedule, and scope and seek clarification from team members and the change requestor.
4. Submit change request to CCB (Project Manager) and Request the CCB convene – The project manager will submit the change request, as well as the preliminary analysis, to the CCB for review.
5. Participate in and obtain decision on change request (CCB) – The CCB will discuss the proposed change and decide whether or not it will be approved based on all submitted information.
6. Implement change (Project Manager) – If a change is approved by the CCB, the project manager will update and re-baseline project documentation as necessary.

The project manager must ensure that any approved changes are communicated to the project stakeholders. Additionally, as changes are approved, the project manager must ensure that the changes are captured in the project documentation where necessary. These document updates must then be communicated to the project team and stakeholders as well.

Once a change order is approved, it will be incorporated into the contract via an amendment or other procedure mandated by the PA DOS's procurement office.

Change Impact Analysis Approach

The change impact analysis approach is the method that is used to identify relevant stakeholders in the change management process as well as the risks and benefits that the change management initiative provides to them. This approach will allow the project team to develop a sound change management strategy. The key element is for the project team to collect direct feedback and fully engage the project's stakeholders during the change management process.

The change impact analysis approach has three aspects:

1. Understand the possible implications of making the change.
2. Identify all aspects of the project (code, files, documents, etc.) that might need to be modified to incorporate the change.
3. Identify tasks required to implement the change.

Steps typically used in the change impact analysis process:

1. Identify the sequence in which the tasks need to be performed.
2. Determine whether the change is on the project's critical path.
3. Estimate the impact of the proposed change on the project's schedule and cost.
4. Evaluate the change's priority.
5. Report the impact analysis results to the appropriate project members for use in approving or rejecting the change request.

Change Management: Tools
BPro will use the PA DOS's change control template, if available, or provide its own standard change order document for review.

7. Communications Management Plan

The following objects will be used to facilitate management of communication throughout the project.

Communications Management Process
Communications management involves the processes required to ensure timely generation, collection, storage, distribution, and disposition of project information. These processes include:

- Communications Planning – determining the information needs of the project stakeholders.
- Information Distribution – making this information available in a timely manner.
- Performance Reporting – collecting and reporting on project performance through status reports and forecasting.
- Coordination Between Stakeholders – managing communications to satisfy the requirements of, and resolve issues with, project stakeholders.
- All of these processes interact with one another throughout the life of the project.

Communication artifacts need to be accessible to project team members after the event occurs and between scheduled distributions, both for reference and as a historical repository. Copies of all communication documents that are produced or received by either DOS or BPro are stored in a central repository site.

Communication Management: Roles and Responsibilities
This list is a partial list of documenting only high-level responsibilities.

Role	Organization	Responsibilities
Project Manager	PA DOS	• Control and communicate changes for DOS team members • Generate project governance documents • Generate status reports • Generate project and financial report • Approve deliverables from BPro • Maintain Risk Register and manage or escalate risks
Business Analyst	PA DOS	• Document high level requirements • Gather research on alternative solutions • Take meeting notes • Maintain project documentation site

Project Manager	BPro	• Assist with developing Communication Management Plan • Assist with developing Communication Matrix • Generate weekly Status Reports • Generate TFS Backlog and work item reports • Communicate changes in key Contractor team members • Document lessons learned
Product Owner	PA DOS	• Functional Expert/ System Owner • Possesses the product vision that prioritizes work items for sprint cycles • Approve functional changes • Approve final deliverable meets requirements (through use of SME and other testing) • Test and facilitate PA DOS approval of functional user stories after each development sprint • Provide written feedback from testing of sprint review delivered stories • Test and approve technical user stories throughout the project • Support Counties and State Agencies in testing and signing off on accepting deliverables

Reporting Tools and Techniques

Different media forms will be used on the PA DOS TotalVote project for conveying information and for communicating between project team members and project stakeholders. Face-to-face communication is the most effective but is not always feasible because some stakeholders are separated geographically.

The various media to be utilized on this project:

- E-mail – E-mail will be used for normal day-to-day communication and dissemination of information. E-mail will be the media of choice for distributing documents between project team members and stakeholders. It will also be used to schedule meetings and for maintaining project calendars.
- Collaboration Tools – project work plan and schedule will be stored on DOS's Project SharePoint site.
- Web Conferencing Software and Telephone – WebEx (or similar product) and conference calls will be utilized on a regular basis to conduct meetings and on an as-needed basis. If not scheduled on a regular basis, notification of such calls should be made at least two working days in advance of the call, where possible.
- Printed Documents – Project documents will be prepared using the Microsoft Office suite. This includes status reports, meeting agendas, site documentation, presentations,

project plans, budget reports, and other project documents as may be required. In order to reduce the size of documents for electronic distribution or to ensure that a "snapshot" document is not inadvertently edited, documents may also be prepared in pdf format.

- Meetings – With the exception of informal or standup meetings, agendas will be prepared and followed for all status meetings. For status meetings and other more formal sessions, minutes should be taken, reviewed, and approved.

Meeting Types and Frequency

Communication	Communication	Purpose		Frequency	Audience	Format and Distribution	Responsibility
Kickoff Meeting	Introduce the project team and the project. Review project objectives and management approach.	Once	Project Team Stakeholders	Meeting with minutes taken		BPro PM DOS PM	
Project Status Report and Meeting	Summary of key project status and performance measures for the past week including the status of deliverables, action items, and milestones. Review status of the project with DOS including existing or new issues and risks. Prioritize and agree on a strategy to mitigate the issues and/or risks.	Weekly – with option to change depending on project activities.	Project Team	Meeting with minutes taken. Agenda based on project status report.		DOS PM provide status report. BPro PM will contribute any updates they deem necessary or as requested.	
Sprint Product Backlog Grooming Meeting	Initially to load the project and then as needed, generally once per sprint. Product Backlog is reviewed for completeness of user story definition.	On Initiate and as needed during the Sprint cycles.	Product Owner Project Team	Work items are staged in TFS by priority. Incomplete A report will be generated prior to each meeting on the proposed list of product backlog items to be discussed during the meeting.		BPro Scrum Master/PM	

Communication	Communication	Purpose		Frequency	Audience	Format and Distribution	Responsibility
Sprint Planning Meeting	This meeting loads the sprints with work items from the backlog. Any Work Items that need to be refined are identified and assigned. Scrum Team agrees to what can be accomplished during that Sprint.	Every 3 weeks to load the start of a Sprint.	Product Owner Project Team	Review of highest priority items in the Product Backlog. User stories taken on for the sprint will be assigned to the sprint.		BPro Scrum Master/PM	
Sprint Review Meeting	BPro team will present what it accomplished during the sprint.	Every 3 weeks to mark the end of a Sprint.	Product Owner Project Team	BPro PM provides meeting agenda. DOS PM prepares Sprint Review meeting summary of feedback. DOS Product Owner provides documented acceptance of demonstrated software items.		BPro Scrum Master/PM	
Scrum Team Standup	Round table of Project Participants: What did you accomplish yesterday? What do you plan to accomplish today? Do you have any roadblocks?	Two days a week during development construction and customization	BPro Development Scrum Team	Using Agile Scrum rules, meeting minutes are not distributed.		BPro Scrum Master/PM	

Communication	Communication	Purpose		Frequency	Audience	Format and Distribution	Responsibility
		portions of project.					
Urgent Project Concerns	Explain time-sensitive issues that have an immediate impact on the project and/or effect a majority of the project team members include possible impact to project assignments and expectations.	As needed	Project Team	Verbal report in a meeting; or email, delivered to project stakeholders and team members and included in weekly status reports.		DOS PM BPro PM Project Sponsor	
Requirements Clarification	Clarification of requirements that impact design, development, or implementation of the PA DOS TotalVote project.	As needed	Project Team	Email, possibly phone conversations, and meetings.		DOS BA	
Sprint or Phase Retrospective	Review performance for a completed project phase.	At conclusion of selected project milestones	BPro Scrum Team	Project metrics distributed beforehand. Summary notes provided to Development Scrum Team.		BPro PM	

8. Quality Management Plan

Quality Management Process
Quality Management will be executed through the inherent Agile Process of product delivery and acceptance. All deliverables must be tested and accepted by the PA DOS.

Delivery of integrated functionality will occur in sprint review testing sessions and formally in the testing events outlined in the Testing Plan.

Prior to any go live, several quality acceptance gates should occur:

- Review of user stories in during the sprint review
- Review of full system in user acceptance testing to ensure gaps are fully identified
- Acceptance of the security measures
    - Security scans on code and environment show no high-level concerns
    - Security standards are met
- Load Testing
    - The ability of the system to support all types of users is verified by PA DOS
- Legal review by PA DOS to ensure PA statutes are satisfied by product

Quality Management: Roles and Responsibilities
The PA Product Owner is responsible for accepting User Story deliverables a test environment.

Role	Organization	Responsibilities
Product Owner	PA DOS	• Provides the quality expectations for the PA DOS TotalVote project.
Project Manager	BPro	• Delivers the PA DOS TotalVote project.
Project Manager	PA DOS	• Inspects the PA DOS TotalVote deliverables.
Technical Lead	BPro	• Responsible for the project assurance tasks.

Quality Management: Tools
The tools used will include testing software, PA security standards, and the formal testing events of the project.

Testing and Promotion Process
Quality control and testing procedures shall be driven by requirements and design and shall adhere to detailed test plans. BPro uses TFS for issue and project tracking. All requirements, including their functionality and design, are tracked in TFS for the development staff. After development work is complete, testing is carried out by both development staff and a business analyst (BA). This testing includes individual requirement testing, unit tests, and system tests. Upon the success of all testing, the software is ready for release to the PA DOS staff for their

sprint review testing. If issues are identified by either the PA DOS Product Owner, BPro will log the issues and the development team will fix them. After issues have been fixed, they can be re-tested through the sprint review process.

Details of the formal testing events of the project will be provided in ***Testing Plan.***

Release Management
Types of releases are categorized as follows:

- **Major Release:** Introduces new functionality to the TotalVote software. These are usually numbered before the decimal point. For example, a major release will be numbered 1.0.
- **Minor Release:** A significant improvement to an existing system, many times packaging together several fixes. These are usually numbered after the decimal point of the major release. For example, a minor release to version 2 will be numbered 2.1.
- **Emergency Release:** As the name implies, this is an unplanned fix to a certain function which simply solves a symptom by allowing the developers to fix the problem. These are usually numbered using the standard for minor releases.

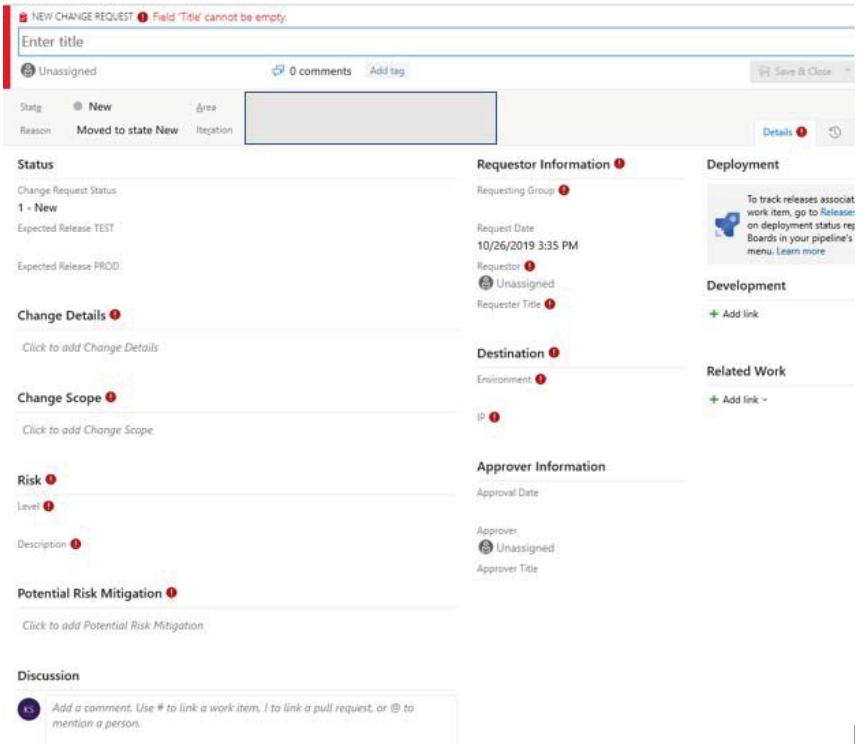
Release Numbering Standard
For release management, BPro will use the following numbering system:

- [Major Version].[Minor Version].[Last 2 Digits of Year + Day of Year]. [Build number for that day]

Example: 1.3.19098.1

Release Management Planning
Prior to releases of software for unscheduled full releases, upgrades, or hot fixes, a change order form will be submitted by BPro to PA DOS. The change order form is used whenever a function is changed or new functionality is planned to be introduced. This form is approved by those named to the Change Control Board or the PA DOS Product Owner prior to the release.

The change order form created in TFS will be used to submit the request.

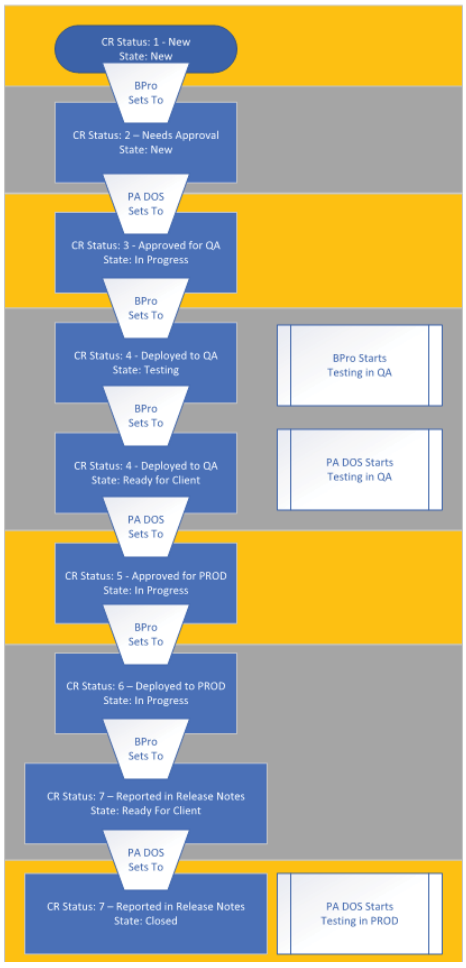


The change order form acts as the release plan template. The purpose is to present and record the following details regarding a release plan:

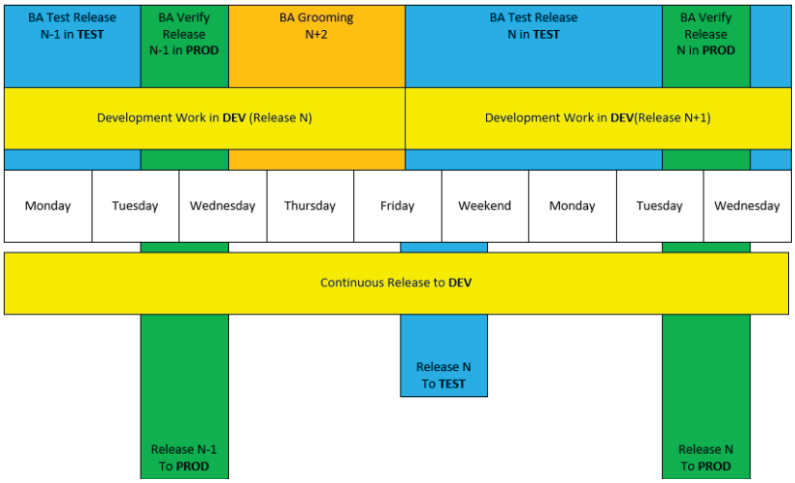
1. Requesting Group. SOS or BPro are the options.
2. Requestor and Requestor Title. This is the owner and title of the request. This is who will update the plan and the details on a periodic timeline.
3. Request Date. When the change order was submitted.
4. Destination. Options are Prod and QA.
5. Change request status. The status of the plan (New, Needs Approval, Approved for QA, Deployed to QA, Approved for PROD, Deployed in PROD, Reported in Release Notes, Canceled).
6. Expected Release TEST.
7. Expected Release PROD.
8. Change Details. Describes the change to be included.
9. Change Scope. Describes the scope of the change.
10. Risk: Level. The risk level (High, Medium or Low). A High risk means that if the implementation is unsuccessful, the organization will be impacted immensely.

11. Risk: Description. Description of the risk. Every change includes risks and a release plan must address these, otherwise they may be overlooked.
12. Potential Risk Mitigation. Description of the potential plan to handle or monitor the risk.
13. Approver Date.
14. Approver and Approver Title. The owner of the release program (generally the Product Owner). Any change to the release must be submitted, reviewed, approved, and documented.

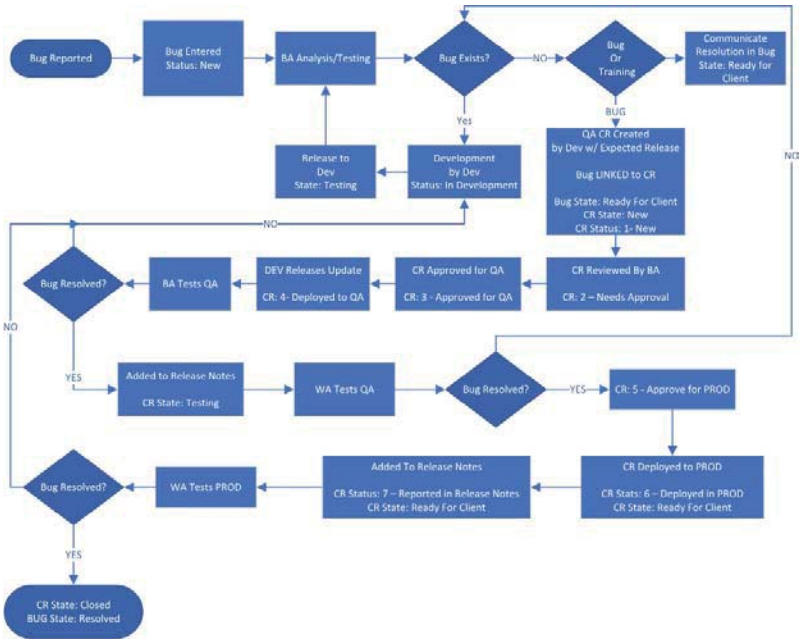
CR Ticketing Status Workflow



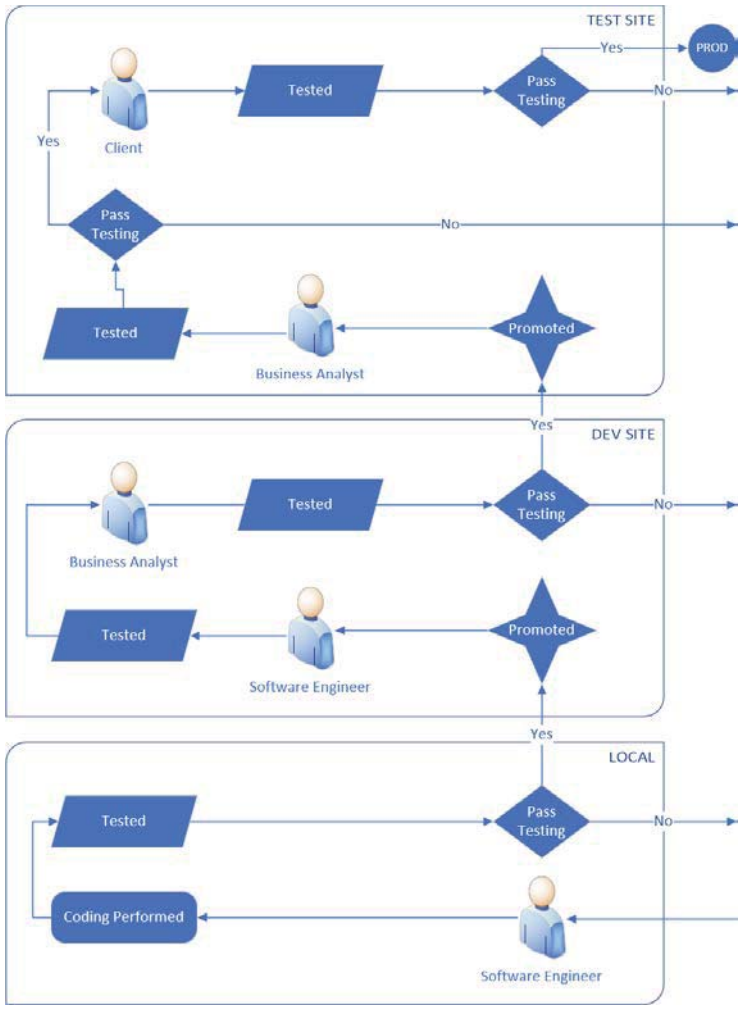
Example Release Flow



Bug Resolution Process Flow – Vote WA example



BPro Testing Promotions Process



User Acceptance Process

All deliverables will follow the approval processes as per the Contract. The following processes are offered as guidelines to prevent delays in finalizing deliverables.

a. Document Deliverables:
    i. BPro will present the Deliverable Document to the PA DOS PM as per the project schedule.

ii. Once PA DOS PM reviews a deliverable and provides feedback, within 10 working days BPro updates and submits a revised deliverable for approval.
iii. If issues are still outstanding, within 10 days BPro will conduct a collaborative session with the PA DOS team to finalize the deliverable and get approval.

b. Design documents: Same process as Document Deliverables above with addition of a step for BPro to conduct a walkthrough with the designated PA DOS team.
c. Prototypes and software releases:
    i. BPro will conduct a demonstration of the prototype/release as per the defined schedule.
    ii. Requirements will be updated to a status of successfully demonstrated.

PA DOS Team will have three business days from the date the release is available in the test environment to test functionality and to provide final approval.

Reviewers and Approvers

PA DOS PM can determine the appropriate personnel in preparation to receive the deliverable and process it in a timely manner to meet the agreed upon time windows for acceptance.

Responsibilities for Each of the Above

Quality Management Tasks	Responsible Role	Organization
Quality Management Process	Project Manager	PA DOS BPro
Tools	Project Manager	PA DOS BPro
Quality Standards	Technical Lead	PA DOS BPro
Testing and Promotion Process	Product Manager	BPro
User Acceptance Process	Product Owner Project Manager	PA DOS

Expected Deliverables

The expected deliverables of this project were outlined in the RFP:

- Implementation Planning
    - Finalized Implementation Plan Approved by DOS
- Implementation of the Solution
    - Requirements Package
    - Configuration Confirmation Report for all agreed to environment reviewed and approved by DOS
    - Detailed Solution and Interface Design Document and Interface Delivery Specification

    - Fully Configured solution and interfaces reviewed and accepted by DOS
    - Test Plan and Test Scenarios
    - Final Implementation Report
- Data Conversion and Validation
    - Data Conversion and Validation Plan Approved by DOS
    - Data Conversion Schedule
    - Final Conversion Test Results
    - Final Data Conversion Report
- Training
    - Finalized Training Plan
    - Training Documentation
    - County User Training Session(s)
    - DOS User Training Session(s)
- Exit from Hosting
    - Hosting Transition Plan
    - Test Plan
    - Test Results
    - Final Hosting Migration Results Report
- Outgoing Transition
    - Outgoing Transition Plan Reviewed and Accepted by DOS
    - Final Report Showing the Successful Completion of Turnover Activities

9. Time Management Plan

Time Management Process
The Time Management Plan will control the changes to the schedule once it has been baselined. The baseline schedule will reflect the agreed upon schedule of the project after refinement.

Once baselined, any changes to the schedule that are created by new tasks (Scope Change) or a change in scheduled delivery (Schedule Change) will be reflected in the ongoing schedule and the impact tracked and reported.

Some events that should trigger Schedule Review are:

a. Changes to Critical Path dates
b. Changes to Milestone Deliverable dates
c. Changes to Dates involving coordination of meetings with the Project Team

The PA DOS TotalVote Project Schedule will be maintained in Microsoft (MS) Project by the BPro Project Manager. The MS Project file and the mirrored .pdf version will be made accessible to the PA DOS Project Manager on the central project document repository.

The Schedule will be reviewed with the PA DOS project team for updates at minimum during the designated project status meetings and more often as necessary.

If slippage is found to be occurring in the project schedule, the Project Managers will discuss the situation during the project status meeting (or special meeting) to document the incident, discuss strategies to resolve, and make assignments to carry out the action plan. The action plan will then be monitored until resolved.

Time Management: Roles and Responsibilities

Role	Organization	Responsibilities
Project Manager	PA DOS BPro	• Monitor tasks to make sure they are completed within the agreed upon time. • Timebox meetings and other discussions. • Monitor the project's workplan. • Update the project's workplan on regular basis. • Flag project schedule concerns if they arise.
Development Team	BPro	• Manage the number of stories taken into a sprint to align with delivery of modules. • Ask clarifying questions to ensure each requirement is understood clearly.
Scrum Master	BPro	• Facilitate meetings in manner which promotes collaboration and open communication between PA DOS and BPro Development Team.

Time Management: Tools and Techniques

Tools used in this project for time management will be mostly Microsoft Project, Excel, and Word documents. The .pdf version of documents will be made available as appropriate.

Project documents will be stored in a central repository using versioning control standards.

Action plans will be discussed for all issues and risks.

TFS will include tasks for each user story, technical requirement, issue, or bug so that a project member can be assigned to the task. The task's progress tracked through TFS.

Time Management: Work Plan

The PA DOS TotalVote project's work plan originate as a Microsoft Project document with .pdf versions available to those which need to view the plan outside of Microsoft Project.

The workplan will be housed in a central repository.

The workplan will be reviewed by the Project Managers and Project Sponsor on a weekly basis. The Project Managers will be responsible for keeping the workplan up to date.

B. IT Service Management. Offeror(s) shall describe its service management methodology its uses to deliver service to its customers. Identify the standards upon which its service management methodology is based. IT Service management shall include strategic approach directed by policies and incorporated in processes and supporting procedures that are performed to plan, deliver, operate, control, and improve IT services offered to customers. Offeror shall describe tools used for service management to include any integration of automated tools. Offeror shall include as part of its proposal any service management plan(s) which will be utilized to deliver, operate, control, and improve the services as described in this RFP. The Offeror's service management methodology is subject to the review and approval by the DOS. Any required timelines will be mutually agreed upon between the Offeror and the DOS.

Offeror Response

IT service management is characterized by adopting a process approach towards management, focusing on customer needs and IT services for customers rather than IT systems, and stressing continual improvement. BPro embraces IT service management through its fully configurable TotalVote systems and its Agile-based development approach. BPro's focus on customer needs is demonstrated in the TotalVote systems available around the country today and the continual customer relationships BPro has developed since its first election technology was used in 2008.

C. Status Report. An initial weekly progress report covering activities, problems and recommendations will be required as part of this project to monitor project activities. As the project progresses, the report timeline can be adjusted to accommodate a mutually agreed upon timeline. This report should be concentrated on the work plan the Offeror developed in its proposal, as amended or approved by the Issuing Office. The status report format and design will be subject to DOS review and approval. The timeline to deliver the status report will be mutually agreed upon by the Offeror and the DOS.

Offeror Response

BPro has included a copy of a weekly status report in the Project Management Plan and the format can be adjusted to meet the needs of the project.

D. Annual Reports. Annual reports shall be provided to the Department each calendar year to document, update, or modify operational or technical details. The Offeror shall work with the Department to develop and implment the report template and information contained within the reprots. Each plan delivered by the Offeror shall be subject to DOS review, modification, acceptance and approval. DOS review and approval of the Offeror's plans shall not act as a waiver of, nor in any way effect, the Offeror's

obligations hereunder. The timeline to deliver annual reports will be mutually agreed upon between the Offeror and the DOS. Reports shall be provided in the following areas:

a. Facility specification sheets for the primary and disaster-recovery data centers; and
b. Technical architecture design of the solution
c. continuity plan;
d. security plan;
e. disaster recovery plan;

Offeror Response

BPro will develop an Annual Report format and timeline with DOS input and final approval.

E. Service Level Agreement (SLA) Report. A monthly report provided to the Commonwealth within five (5) business days of month's end. The final format and design of the SLA report will be subject to review and approval by the DOS. The reporting timelines will be mutally agreed upon between the Offeror and the DOS. The report shall provide statistical data to track compliance with the SLAs as described in **Appendix H, Service Level Agreements Vendor Hosted.**

BPro will work with DOS to develop the format of an SLA Report and deliver the report within five (5) business days of month's end.

F. Problem Identification Report. An "as required" report, identifying problem areas. The report should describe the problem and its impact on the overall project and on each affected task. It should list possible courses of action with advantages and disadvantages of each, and include Offeror recommendations with supporting rationale.The format and design of this report shall be subject to DOS review and approval. The timeline to deliver this report will be mutally agreed upon between the Offeror and the DOS.

Offeror Response

BPro will work with DOS to develop a Problem Identification Report format and timeline.

XIII. Objections and Additions to Standard Contract Terms and Conditions. The Offeror will identify which, if any of the, service level agreements, non-commonwealth hosting terms, and terms and conditions contained in the Buyer Attachments section that it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions. The Offeror shall clearly identify any additions, modifications, or edits to the RFP documents with red-lined versions of documentation to easily identify changes. The Offeror's failure to make a submission under this paragraph will result in its waiving its

right to do so later, but the Issuing Office may consider late objections and requests for additions if to do so, in the Issuing Office's sole discretion, would be in the best interest of the Commonwealth. The Issuing Office may, in its sole discretion, accept or reject any requested changes to the standard contract terms and conditions. The Offeror shall not request changes to the other provisions of the RFP, nor shall the Offeror request to completely substitute its own terms and conditions for this RFP. All terms and conditions must appear in one integrated contract. The Issuing Office will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any proposal.

Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, on the basis of the terms and conditions set out in the Terms and Conditions contained in the Buyer Attachement section. The Issuing Office will reject any proposal that is conditioned on the negotiation of service level agreements, non-commonwealth hosting terms and the terms and conditions set out in the Terms and Conditions contained in the Buyer Attachment section or to other provisions of the RFP.

Offeror Response

BPro has carefully reviewed the service level agreements, non-commonwealth hosting terms, and terms and conditions in this RFP and requests to negotiate the following:

Service Level Agreements

BPro has fully reviewed Appendix H. If selected, BPro will commit to developing mutually agreeable Service Level Agreements with DOS.

Terms and Conditions

4. EXTENSION OF CONTRACT TERM.

The Commonwealth reserves the right, upon notice to the Contractor, to extend the term of the Contract for up to three (3) months upon the same terms and conditions.

27. CHANGES.

(a) At any time during the performance of the Contract, the Commonwealth or the Contractor may request a change to the Contract. Contractor will make reasonable efforts to investigate the impact of the change request on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commonwealth is the requestor of the change, the Contractor will inform the Commonwealth of any charges for investigating the change request prior to incurring such charges. If the Commonwealth and the Contractor agree on the results of the investigation and any necessary changes to the Contract, the parties must complete and execute a change order to modify the Contract and implement the change. The change order will be evidenced by a writing in accordance with the Commonwealth's change order procedures. No work may begin on the change order until the Contractor has received the executed change order. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall perform the Services; and

either party may elect to have the matter treated as a dispute between the parties under Section 30, Contract Controversies. During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts.

31. CONFIDENTIALITY, PRIVACY AND COMPLIANCE.

(a) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

- Prepare and submit an un-redacted version of the appropriate document;
- Prepare and submit a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret. The Contractor shall use a redaction program that ensures the information is permanently and irreversibly redacted; and
- Prepare and submit a signed written statement that identifies confidential or proprietary information or trade secrets and that states:
  - (1) the attached material contains confidential or proprietary information or trade secrets;
  - (2) the Contractor is submitting the material in both redacted and un-redacted format, if possible, in accordance with 65 P.S. § 67.707(b); and
  - (3) the Contractor is requesting that the material be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

64. LIQUIDATED DAMAGES.

(a) By accepting this Contract, the Contractor agrees to the delivery and acceptance requirements of this Contract. If a due date is not met, the delay will interfere with the Commonwealth's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the Contractor is the material cause. The Commonwealth and the Contractor therefore agree that in the event of any such delay, the amount of damage shall be the amount set forth in this section, unless otherwise indicated in the Contract, and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty. Such liquidated damages are in lieu of all other damages arising from such delay.

(b) The amount of liquidated damages shall be as set out in the Solicitation. If not amount is set out in the Solicitation, the amount of liquidated damages for failure to meet a due date shall be three-tenths of a percent (.3%) of the price of the deliverable for each calendar day following the scheduled completion date. If the price of the deliverable associated with the missed due date is not identified, liquidated damages shall apply to the total value of the Contract. Liquidated damages shall be assessed each calendar day until the date on which the Contractor meets the requirements for the deliverable associated with the due date, up to a maximum of 30 days. If indicated in the Contract, the Contractor may recoup all or some of the

amount of liquidated damages assessed if the Contractor meets the final project completion date set out in the Contract.

(c) If, at the end of the 30-day period specified in subsection (b) above, the Contractor still has not met the requirements for the deliverable associated with the due date, then the Commonwealth, at no additional expense and at its option, may either:

(i) Immediately terminate the Contract in accordance with Subsection 28(c) and with no opportunity to cure; or

(ii) Order the Contractor to continue with no decrease in effort until the work is completed in accordance with the Contract and accepted by the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, any liquidated damages will also continue until the work is completed.

70. RIGHT-TO-KNOW LAW.

(d) If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within seven (7) days of receiving the written notification, a written statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

(h) The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts, however, the Contractor shall indemnify the Commonwealth for any legal expenses incurred by the Commonwealth as a result of such a challenge and shall hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth, regardless of the outcome of such legal challenge. As between the parties, the Contractor agrees to waive all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.

Exhibit B

PERFORMANCE AUDIT REPORT

Pennsylvania Department of State

Statewide Uniform Registry of Electors

December 2019

Commonwealth of Pennsylvania
Department of the Auditor General

Eugene A. DePasquale • Auditor General

This page left blank intentionally

Commonwealth of Pennsylvania
Department of the Auditor General
Harrisburg, PA 17120-0018
Facebook: Pennsylvania Auditor General
Twitter: @PAAuditorGen
www.PaAuditor.gov

EUGENE A. DEPASQUALE
AUDITOR GENERAL

December 13, 2019

The Honorable Tom Wolf
Governor
Commonwealth of Pennsylvania
Room 225 Main Capitol Building
Harrisburg, PA 17120

Dear Governor Wolf:

This report contains the results of the Department of the Auditor General's (DAG) performance audit of the Statewide Uniform Registry of Electors (SURE) administered by the Department of State (DOS). This audit was conducted pursuant to the Interagency Agreement (agreement) entered into by and between DOS and DAG, effective May 15, 2018, and under the authority of Sections 402 and 403 of The Fiscal Code, 72 P.S. §§ 402 and 403.

This audit covered the period January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date, and focused on audit objectives, which were agreed upon and formalized in the agreement, as follows:

1. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law.
2. Evaluation of the process for input and maintenance of voter registration records.
3. Review of security protocols of the SURE system.
4. Review of the efficiency and accuracy of the SURE system.
5. Review of the internal controls, methodology for internal audits and internal audits review process.
6. Review of the external controls, methodology for external audits and external audits review process.
7. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance.
8. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.

Further, this audit was conducted in accordance with applicable *Government Auditing Standards*, issued by the Comptroller General of the United States, except for certain applicable requirements that were not followed. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.[1] Significant scope limitations caused by a lack of cooperation and a failure to provide the necessary information by DOS, the Pennsylvania Department of Transportation (PennDOT), and four county election offices (counties), substantially impacted our ability to obtain sufficient appropriate evidence to fully achieve all audit objectives as described below and within *Finding 1*.

DOS' denial of access to critical documents and excessive redaction of documentation resulted in DAG being unable to fully achieve three of the eight audit objectives. Specifically, DAG was unable to accomplish the following: (1) Objective 1, the accuracy of the records maintained in SURE; (2) Objective 3, the review of security protocols of the SURE system; and (3) Objective 6, review of the external controls, methodology for external audits and external audits review process. This sustained refusal to cooperate with our information requests was done without DOS providing any plausible justification for their noncooperation. Accordingly, DAG was unable to establish with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines. See additional explanation in *Finding 1*.

As part of determining the accuracy of the voter registration records in SURE, we originally designed our tests to allow us to project the accuracy of the records over the entire population of 8,567,700 voters as of October 9, 2018 through the use of statistical sampling. We randomly selected 196 out of the 8,567,700 voters and requested source documents to verify the accuracy of the related voter data within SURE. While we found the records were accurate for the 58 voter records that we were able to test, we were unable to form any conclusions as to the accuracy of the entire population of voter records maintained in SURE since we could not test 138 or 70 percent of the records we sampled due to source documentation not being made available. The reasons that source documentation was not available for these records included DOS not providing adequate record retention requirements and guidance to the counties, counties not responding to our requests for source documentation, PennDOT's refusal to provide access to Motor Voter source documents, and DOS not maintaining online application source documents. Because of this, we could not conclude on our statistical sample and therefore, we could not project our results and ultimately conclude on the overall accuracy of the voter registration information maintained in the SURE system.

---

[1]U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Please see the following summary of key standards: (1) Paragraphs 6.56 through 6.72 relate to standards related to obtaining sufficient appropriate evidence; (2) Paragraphs 6.23 through 6.27 relate to standards for evaluating the effectiveness of information system controls; and (3) Paragraph 6.36 relates to review of previous audits and attestation engagements.

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures and believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See *Findings 2 through 7* for our results. Overall, we provide 50 recommendations to strengthen DOS' policies, management controls, and the accuracy of the voter registration records in SURE, and to close gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system. It is imperative for DOS to implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records. Additionally, it is imperative that DOS continue with its plans to develop and implement a replacement system to ensure the voter registration records are secure and accurate. DOS should also update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

Based on data analysis that we were able to perform, despite the substantial scope limitations noted above, we identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from SURE. We found that voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in SURE. Specifically, voter registration applications remain in pending status for long periods of time- indefinitely in some cases, and although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records. Additionally, incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Finally, during the conduct of our procedures, we identified potential areas of improvement related to computer security, information technology general controls, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information due to security concerns over the Commonwealth's critical elections infrastructure. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

We are very discouraged by management's response to our draft findings. We were quite surprised that DOS' response indicates that it strongly disagrees with many of our findings and mischaracterizes information that was provided, or not provided to us in many instances, during the course of our audit. With its attempt to refute our findings, DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records, and our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further review. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis strongly suggests otherwise. Also, while DOS requested

this audit, management does not seem to grasp that we cannot properly conclude and satisfy the audit objectives in accordance with generally accepted *Government Auditing Standards* without obtaining sufficient appropriate evidence, which they refused to provide to us.

In closing, despite the substantial limitations imposed by DOS, we believe we have provided DOS with recommendations that, if appropriately implemented, will improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records. We hope that, despite its written disagreements, DOS seriously considers all of the management control weaknesses identified and works conscientiously with the counties to address all of the potential voter registration inaccuracies noted in the SURE voter registration records. We will follow up at the appropriate time to determine whether and to what extent all recommendations have been implemented.

Sincerely,

Eugene A. DePasquale
Auditor General

TABLE OF CONTENTS

Executive Summary 1

Introduction and Background 8

Finding One: **As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested** 16

Recommendations 25

Finding Two: **Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system** 27

Recommendations 36

Finding Three: **The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records** 38

Recommendations 43

Finding Four: **Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system** 46

Recommendations 59

Finding Five: **Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy** 60

Recommendations 65

TABLE OF CONTENTS (continued)

Finding Six: A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system 67

Recommendations 74

Finding Seven: The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention 75

Recommendations 78

Agency's Response and Auditor's Conclusions 80

Appendix A – *Objectives, Scope, and Methodology* 134

Appendix B – *Interagency Agreement Between the Department of State and the Department of the Auditor General* 150

Appendix C – *Voter Registration Process* 157

Appendix D – *The lack of oversight that allowed non-citizens the ability to register to vote at PennDOT's photo license centers, even after indicating they are not a citizen, was addressed during the audit period* 161

Appendix E – *Voter Registration by County* 165

Appendix F – *HAVA Funds Received by Pennsylvania* 168

Appendix G – *Description of Data Used in the Audit* 172

Appendix H – *SURE Survey* 173

Appendix I – *Distribution List* 183

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

Executive Summary

This audit report presents the results of a performance audit of the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). This audit was conducted pursuant to an Interagency Agreement (agreement) entered into by and between DOS and the Department of the Auditor General (DAG) on May 15, 2018.[2] The agreement specified eight audit objectives related to SURE and required the final report to be delivered by January 31, 2019. Additionally, the agreement specified that the audit time period would begin on January 1, 2016 and go through the end of our audit procedures.[3] Throughout the execution of this audit however, the auditors experienced scope limitations (addressed in *Finding 1* below) due to a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure of those parties to provide DAG the necessary information needed to satisfy certain audit objectives. These delays resulted in the need to amend the agreement multiple times to extend the report release date as explained in *Appendix B*. In spite of these extensions, we were unable to fulfill all the requirements to conduct the audit in accordance with applicable *Government Auditing Standards* as described by the modified *Government Auditing Standards* compliance statement in the letter within this report and discussed further in *Finding 1*.

Despite these limitations, we believe that this report's seven findings and 50 recommendations as well as the comments and recommendations we have separately provided DOS within our confidential communication related to security protocols, information technology general controls, and interface controls will assist DOS, if appropriately implemented to improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records.

Regrettably, we were surprised and disappointed that DOS' response contained in this report indicates that it strongly disagrees with many of our findings and mischaracterizes the information that was provided or not provided to us during the course of our audit. We address management's disagreements and mischaracterizations in the *Auditors' Conclusion* section of this report. We are concerned, however, with its attempt to refute our findings. DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records, and our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further review. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis strongly suggests otherwise. We hope that despite these written disagreements DOS seriously considers all of the management control

[2] See *Appendix B* for a copy of the agreement.
[3] Additional information on the audit scope, as well as the audit objectives and methodology can be found in *Appendix A*.

weaknesses identified and works conscientiously with the counties to address all of the potential voter registration inaccuracies noted in the SURE voter registration records prior to migrating this data into the new replacement system.

Our findings are summarized below.

Finding 1 – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS failed to comply with the agreement's provision requiring that they cooperate with DAG's requests related to the audit. This failure impeded DAG's ability to timely conclude the audit and resulted in significant scope limitations that affected our ability to achieve audit objectives 1, 3, and 6. As a result, DAG was unable to determine with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines.

During the audit, DOS management denied us access to significant key documents/information related to the security and operation of the SURE system and for some documents that were provided, the entire documents were redacted, making the documentation unusable as evidence.[4] Without these critical documents, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards,* which require auditors to evaluate the effectiveness of IT controls and review previous audits and assessments significant within the context of our audit objectives. Without access to the external security assessment reports, we were unable to determine what information the assessments contained, and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6). We were also unable to determine if any security weaknesses were noted in the assessments or whether corrective actions had been implemented.

Additionally, due to the lack of cooperation from certain counties, PennDOT, and the system design of online voter registration applications, we were unable to perform adequate tests to determine the accuracy of the voter record data in SURE (Objective 1). We are, therefore, unable to form any conclusions as to the accuracy of the entire population of voter registration records maintained in SURE.

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures, including some related to objectives 1, 3, and 6, and have discussed our

[4] After approximately nine months of requesting copies of certain reports, we were provided with hundreds, if not thousands of pages that were blacked out from top to bottom other than the report cover pages.

results in *Findings 2 through 7*. Within this finding, we offer six recommendations related to future audits of SURE or its replacement and the need for respective parties to cooperate with auditors.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

We requested SURE electronic files of all currently registered voters and the history of all of the changes made to voter records during the period January 1, 2016, to the present. We also requested copies of the Full Voter Export List for each county, which are available to the public through DOS' website. It took over three months for DOS to provide these electronic files. These files contained voter registration records for 8,567,700 registered voters as of October 9, 2018. Using these files, we performed data analysis to evaluate the information within SURE for reasonableness.

As a result of our data analysis, we identified potential inaccuracies, including:

- 24,408 cases where the same driver's license number was listed in more than one voter record.
- 13,913 potential duplicate cases.
- 6,876 potential date of birth (DOB) inaccuracies.
- 2,230 potential DOB and/or registration date inaccuracies.
- 2,991 records of potentially deceased voters.

Due to audit time constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS will need to work with the counties to follow up and address all these situations in order to investigate and correct the voter records as appropriate.

Based on the results of our data analysis, along with reviewing DOS regulations and guidance, and on-site visits to seven counties where we observed staff processing new voter registration applications (applications) to check for duplicate records, we found the process ineffective for identifying duplicate records and removing voter records of deceased voters. We also identified other weaknesses increasing the risk of inaccurate records regarding the processing of applications and subsequent list maintenance, which are addressed separately in *Findings 4 and 5*.

We offer 10 recommendations to DOS to work with the counties to investigate these situations of potential duplicates, deceased voters, and inaccuracies and correct the voter records as appropriate; create automated processes to prevent duplicate and invalid information from being

recorded in the SURE system and/or the replacement system for SURE; and to evaluate the guidance provided to the counties regarding duplicates to ensure that it is adequate.

Finding 3 – The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

As described in *Finding 1,* DOS refused to provide us access to significant key documents related to the security, information technology (IT) controls, and operation of the SURE system. As a result, we were unable to satisfy our audit objective to review the security protocols of the SURE system and conduct our audit in accordance with applicable *Government Auditing Standards.*[5]

Based on the limited information that DOS management did provide to us or through review of other available information, we were able to identify gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system and supporting architecture. We found that the governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls. Additionally, DOS management's vendor oversight practices need to be improved. DOS management could not provide System and Organization Control (SOC) reports for its key vendors or evidence that it reviewed the SOC reports and assessed whether controls at the service organizations were appropriately designed and operating effectively.

Further, we found that DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties for the appropriate use of the IT equipment provided by DOS. It also fails to include the additional responsibilities for security if the county chooses to connect county-owned equipment to the SURE system and a corresponding form to request and approve such deviation.

We offer one recommendation to the Secretary of the Commonwealth to consider creating an oversight body for the SURE system. We also offer 11 additional recommendations to DOS management to develop a governance structure that will provide clear lines of authority in the operation, maintenance, and security of the SURE system; continue with plans to replace the SURE system; implement additional security guidelines; monitor vendors through a documented process; and update the *SURE Equipment Use Policy*.

[5] U.S. Government Accountability Office. Government Auditing Standards. 2011 Revision.

Finding 4 – Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

We found that the SURE system and supporting processes and controls are not effective to ensure that the voter registration information is accurate. We identified several reasons why inaccuracies occur and grouped them into two areas: (1) weaknesses within the application process, and (2) weaknesses regarding the maintenance of voter registration records within the SURE system.

Regarding weaknesses within the application processes, we found that no review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry. Automated edit checks and other features to prevent or detect inaccuracies are also not sufficiently incorporated into the SURE system. Additionally, we found that applications can remain in pending status for long time periods and in some cases indefinitely. Based on data analysis, as of October 9, 2018, there were 91,495 applications in pending status, including 23,206 that had been placed in pending status prior to the beginning of our audit period on January 1, 2016.

For weaknesses regarding the maintenance of voter registration records within the SURE system, we found that insufficient analysis by counties has resulted in inaccurate voter record data, despite the performance of list maintenance activities by the counties. Our analysis also identified 96,830 voters who potentially should be classified as inactive and an additional 65,533 records of inactive voters whose voter records potentially should have been canceled. Additionally, DOS does not fully utilize the list maintenance feature it pays for as a member of the Electronic Registration Information Center (ERIC).

We offer eight recommendations to improve application processing controls and the accuracy of the voter registration data.

Finding 5 – Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

In addition to the inadequate or nonexistent automated checks in the SURE system for allowing duplicate voter records, preventing adding a voter with a driver's license already associated with a voter record, and recording of obviously inaccurate birthdates and/or voter registration dates (addressed in *Finding 2*), we found features that were missing or inadequate which could further reduce or prevent errors. Specifically, we found that the SURE system does not prevent applications with a non-Pennsylvania residential address from being approved. The SURE system also lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing. Additionally, the SURE system lacks a "Read Only" feature to prevent key fields with permanent data such as a date of birth, Social Security number, or driver's license number

from being changed. Finally, the SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

We were also informed of two additional areas needing improvement related to the PennDOT Motor Voter process and the reporting capabilities within the SURE system. We found that some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote. Through discussions with DOS management and input from county officials, we also found that the ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

We offer five recommendations to DOS that include incorporating several information technology enhancements into its design of the replacement SURE system and consider the feasibility of making some or all of these enhancements into the current SURE system. Additionally, DOS should consider working with PennDOT to revise the Motor Voter process to obtain all required voter registration information from individuals requesting to update their voter registration address.

Finding 6 – A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

We selected a random statistical sample of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018. Our intent was to review source documents to confirm the accuracy of the information in SURE in the 196 voter records and thus conclude as to the accuracy of the entire voter population. Due to lack of cooperation and the unavailability of 138 of the 196 records selected (or 70 percent), we could not conclude on the accuracy of the entire voter population. Of the 196 voters selected, 84 of the voters' most recent application/change to their registration was made using a paper application. We were only able to test and verify the accuracy for 58 of these 84 paper applications. Of the remaining 26 applications, 14 could not be tested because 12 counties acknowledged that they were unable to locate the source documents needed to test each record for accuracy, and four counties did not respond to our requests to provide source documents for the other 12.

One factor for the unavailability of the applications is due to the lack of a clear records retention policy issued to the counties by DOS. Without clear guidance from DOS, we found that the counties have differing stances on how long an application must be kept. A clear record retention policy from DOS and a requirement to scan all applications into SURE would help ensure uniformity among counties, ensure complete records, provide a SURE user with the ability to answer questions if/when they arise from either voters or county staff, and allow for documents to be audited, as necessary.

We also found that DOS does not maintain copies, nor does it require the counties to maintain copies, of applications submitted via the online application process. This accounted for 19 of our 196 selected voters. Finally, for the remaining 93 applications processed through the Motor Voter system, PennDOT refused to provide us access to Motor Voter source documents.

We offer five recommendations to DOS to develop an audit trail for registration applications that are submitted online and via hard copy, develop a records retention policy to help ensure consistency of records retention amongst all the counties, and update the SURE regulations to ensure that they are in accordance with the newly developed records retention policy.

Finding 7 – The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

We found that DOS generally provided meaningful assistance and guidance to the counties regarding SURE voter registration and list maintenance. DOS provides guidance to the counties related to the SURE system through job aids, which provide step-by-step instructions on how to complete various tasks associated with the processing of a voter registration application. Additionally, DOS also makes hands-on training available to the counties upon request. The counties and DOS also have access to the SURE Help Desk for assistance, as needed.

We believe, however, that the guidance provided by DOS did not sufficiently address all critical areas. The critical areas not adequately addressed include: job aids need to be updated to reflect recommended improvements regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls, no guidance was provided to the counties regarding the length of time that applications remain in pending status and whether pending applications past that timeframe should be denied, and no clear guidance was provided to the counties regarding a record retention policy for voter record source documents. Additionally, we found that the job aids did not consistently contain uniform issue or revision dates in order to maintain version control and prevent confusion.

We offer four recommendations to DOS to continue to offer hands-on training on the SURE system; update the applicable job aids to reflect changes in processes; include an issue date on all job aids distributed to the counties and create an indexed list of job aids listing the most current version; and provide guidance to the counties regarding the maximum length of time that an application can remain in pending status.

Introduction and Background

This report presents the results of our performance audit of the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). The performance audit was conducted under the authority of Sections 402 and 403 of The Fiscal Code and pursuant to the Interagency Agreement entered into by and between the Pennsylvania Department of the Auditor General and DOS.[6] Our performance audit had eight objectives and covered the period of January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date. Refer to *Appendix A* of this report for a detailed description of the audit objectives, scope, and methodology.

In the following sections we will discuss:

- Threats to Pennsylvania elections
- The election-related responsibilities of DOS and county election offices
- The implementation of SURE
- The Commonwealth's voter registration process
- The voter record maintenance process
- The status of Pennsylvania's voting systems
- DOS plans to replace the SURE system

Threats to Pennsylvania Elections

An accurate voter registration system and effective paper record voting machine system are critical in the current environment where a significant threat of hacking election records exists. In September 2017, the *New York Times* reported that earlier that month, the United States Department of Homeland Security had informed 21 states that their election systems had been ". . . targeted by hacking efforts possibly connected to Russia" during the 2016 Presidential election. The *New York Times* listed Pennsylvania as one of the states that informed the Associated Press that they had been targeted.[7]

In May 2018, the United States Senate Intelligence Committee (Intelligence Committee) released an unclassified summary of its investigation into the matter, confirming that cyber actors affiliated with the Russian government scanned state systems extensively throughout the 2016 election cycle. These cyber actors made numerous attempts to access several state election systems and, in a small number of cases, actually accessed voter registration databases. The

[6] 72 P.S. §§ 402 and 403. See *Appendix B* for a copy of the Interagency Agreement.
[7] <https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html> (accessed September 11, 2019).

investigation also found that at least 21 states potentially had their election systems targeted in some fashion while other states reported suspicious or malicious behavior.[8]

The targeting of state voter registration systems was confirmed by the Mueller Report, released in April 2019. This report found that officers of the Russian military intelligence agency used cyber hacking techniques during the 2016 presidential election to attack state boards of elections, secretaries of state, and county governments involved in the administration of elections, as well as individuals who worked for those entities.[9]

The Mueller report noted for example, that the Illinois state Board of Elections reported that hackers had succeeded in breaching its voter systems by sending malicious code to the state's website in order to run commands and gain access to the database containing the information for millions of registered voters.[10] The Mueller report also noted that Florida county election administration officials were targeted through spear-phishing emails that allowed the intruders to gain access to the network of at least one Florida county government.[11]

In July 2019, the Senate Select Committee on Intelligence reported that additional information was obtained in late 2018 that evidenced the U.S. election infrastructure of all 50 states, which includes voter registration databases, had been scanned by foreign agents in attempts to understand the networks and identify vulnerabilities within the systems at both state and local levels.[12] These events demonstrate the need for ensuring the security of Pennsylvania's voting systems against cybersecurity attacks which are increasing in both quantity and sophistication. Improving voting systems will simultaneously endeavor to maintain the utmost integrity in Pennsylvania election results.

The Election-Related Responsibilities of DOS and County Election Offices

DOS' Bureau of Election Security and Technology (BEST) oversees the functions of SURE, election security and technology initiatives, certification of equipment, and technology and data

[8] U.S. Senate Intelligence Committee, *Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations*, dated May 8, 2018. <https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated> (accessed February 27, 2019).
[9] U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, March 2019, page 50 <https://www.justice.gov/storage/report.pdf> (accessed April 22, 2019).
[10] Ibid.
[11] Id. at page 51.
[12] *Report of the Select Committee on Intelligence, United State Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, pages 3-12, <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf> (accessed August 1, 2019).

innovation. BEST is also responsible for working with federal, state, and local partners to maintain and enhance the security of Pennsylvania's elections infrastructure.[13]
DOS' Bureau of Election Services and Notaries (BEN) oversees the functions of the Division of Election Services and Voter Registration. BEN is responsible for areas such as serving voters, candidates, counties, and other stakeholders on matters relating to election administration and voter registration.

DOS also oversees elections in conjunction with the county elections and/or voter registration office(s) in each of Pennsylvania's 67 counties. Staffing for these county election offices (county) range from 1 to 100 full-time employees, as well as some part-time/temporary employees as needed. County election/voter registration staff report to the County Commissioners/County Executive and are responsible for conducting elections and performing related tasks, including, but not limited to:

- Completing all tasks related to voter registration, including processing voter registration applications; performing procedures to update and monitor the accuracy of voter registration records, typically and hereafter referred to as *list maintenance*; and certifying voter registration statistics to DOS prior to each election
- Processing county level candidates' petitions for inclusion on the ballot
- Designing/printing the ballots
- Purchasing voting machines[14]
- Programming voting machines
- Printing poll books
- Hiring and organizing poll workers
- Finding/securing polling locations
- Certifying the election results to DOS

It is important to note that while DOS oversees Pennsylvania's elections and maintains the SURE system, the voter registration records are owned by the individual counties. If a voter moves from one county to another, any paper documents associated with that voter are transferred to the new county. DOS does not have ownership over the records, nor does it have the authority to edit records, cancel a record, or move a voter from active to inactive status.

The Implementation of SURE

The Help America Vote Act of 2002 (HAVA) was enacted to improve voting systems and voter access throughout the nation. HAVA created mandatory minimum standards related to key areas of election administration that every state must follow, one of which was to implement a

[13] For purposes of this report, we refer to BEST collectively as DOS.
[14] The counties have the authority and mandate to purchase voting machines; however, they may only purchase machines that have been certified by the federal government and by Pennsylvania's Secretary of State.

computerized statewide voter registration list to serve as the single system for storing and managing the official list of registered voters.[15] While DOS has had authority over elections in Pennsylvania since the early 1900s, it was charged with maintaining the SURE system shortly after HAVA's enactment.[16] SURE, which was implemented in Pennsylvania as a result of Act 3 of 2002, is the platform that supports the critical functions of the Commonwealth's election system, including voter registration, voter list maintenance, precinct data, and the production of poll books.[17] SURE was designed to ensure the accuracy and integrity of the Commonwealth's voter registration records maintained by the election authorities in each of the 67 counties.

SURE is maintained by DOS and utilized by each of the counties. DOS must ensure that the counties fulfill their statutory responsibilities, but DOS must be careful not to infringe upon functions reserved for the counties (as discussed above, the counties own the voter registration records, not DOS). For example, the counties have the authority to process voter registration applications, make changes to a voter's record, or cancel a voter's registration; however, HAVA requires DOS to ensure that the voter registration records are accurate and are updated regularly. This includes "file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote."[18] Accordingly, HAVA places the responsibility on DOS to ensure that SURE data is accurate but at the same time, DOS has no ability to force the counties to comply.

The Commonwealth's Voter Registration Process

Any individual who wants to vote in an election in Pennsylvania is required to register to vote no later than 30 days prior to the election. The National Voter Registration Act (NVRA) requires that:

- Each State shall designate agencies for the registration of voters in elections for *Federal office*.
- Each State shall designate as voter registration agencies:
  - all offices in the State that provide public assistance
  - all offices in the State that provide State-funded programs primarily engaged in providing services to persons with disabilities.[19]

[15] 52 U.S.C. § 21083(a)(1).
[16] As part of the SURE system, DOS also created the SURE Portal (Portal). The Portal allows the user to view but not edit or cancel a voter's record. The Portal is used by county staff, especially during periods of high activity, and by the BEST staff to answer telephone calls from voters requesting their status (registered or not), their party affiliation, or the location of their polling place.
[17] 25 Pa.C.S. § 1222.
[18] 52 U.S.C. § 21083(a)(2).
[19] 52 U.S.C. § 20506(a). For the purposes of voter registration, as required by the NVRA, the offices in Pennsylvania that have been identified as those that "provide public assistance" are: Women, Infant and Children Nutrition Clinics; County Assistance Offices; Clerk of Orphans' Courts, Children and Youth Agencies; Area Agencies on Aging; Para-Transit providers; Special Education Programs at the 14 state-owned universities; agencies

Pennsylvania, through its voter registration law, has included these requirements for all elections.[20]

The ways in which a person can register, as well as the qualifications to register, are standardized throughout Pennsylvania and are outlined in *Appendix C*. The application to register is received and processed by the county. The SURE system guides the county staff through the process; however, the number of applications received varies greatly and the manner in which a county distributes work is discretionary within each county.

Anytime an individual submits a voter registration application (application) that is able to be processed, whether it is to initially register to vote or to change their name/address/party, the applicant will be mailed a voter card that contains the voter's information and the name and location of the corresponding polling place.[21] The voter card is mailed "non-forwardable" and if it is not returned to the county within 10 days, the applicant becomes a registered voter. Once an applicant is a registered voter, they are eligible to vote in the next election. If the voter is a new voter or voting for the first time at a polling place, the voter will need to show proof of identification (see *Appendix C* for a list of acceptable forms of identification). See *Appendix E* for information on 2018 Pennsylvania voter registration statistics.

The NVRA also requires that the Pennsylvania Department of Transportation (PennDOT) provide its customers an opportunity to register to vote.[22] Commonly referred to as "Motor Voter," this process provides PennDOT customers the ability to register to vote while applying for or renewing a driver's license or photo ID at a PennDOT center. Being fully electronic since 2003, any voter registration applications obtained by PennDOT are uploaded into SURE and are electronically distributed to the applicable counties for processing. A defect detected with the Motor Voter system, which permitted non-U.S. citizens to request to register to vote, is discussed in *Appendix D*. The following table shows the number of new voter registrations and change of address edits made to SURE voter records resulting from voters' usage of PennDOT's Motor Voter system during the calendar years 2015 through 2018:

serving people with disabilities and County Mental Health/Intellectual Disabilities offices; and the armed services recruitment centers.

[20] 25 Pa.C.S. § 1325.

[21] An application should not be processed if it is missing information or if it is an exact duplicate of the information for a voter already within the system.

[22] 52 U.S.C. § 20501 *et seq.* which is also known as the Motor Voter Act.

Pennsylvania Department of State Number of Voter Registration Transactions Processed Through PennDOT's Motor Voter System by Transaction Type for Calendar Years 2015-2018				
Type of Transaction	**2015**	**2016**	**2017**	**2018**
New Registration	112,774	112,680	94,946	98,911
In-County Change of Address	295,377	321,410	369,727	346,899
Out-of-County Change of Address	91,468	92,466	111,260	106,930
Total[a/]	**499,619**	**526,556**	**575,933**	**552,740**

[a/] The numbers reported only reflect transactions that were forwarded from PennDOT to DOS that resulted in a new registration or change made to an existing registration. Therefore, these numbers do not include applications that were unable to be approved/processed, such as those with incomplete information, applications for individuals that are already registered to vote, or for those individuals that were not eligible to register to vote.
Source: Produced by the Department of the Auditor General staff based on information from the Pennsylvania Department of State's "The Administration of Voter Registration in Pennsylvania, Report to the General Assembly" for calendar years 2015-2018, dated June 2016, June 2017, June 2018, and June 2019, respectively.

The Voter Record Maintenance Process

Voter registration data is continuously maintained by the individual counties through the SURE system. In addition to ongoing maintenance, the counties conduct annual maintenance activities as prescribed by law.[23] For instance, the counties send address verification notices to voters who have been identified by the United States Postal Service as having submitted a change of address. Counties send Five-Year Notices to voters who have not voted in the past five years or made any contact with the county. If the voter fails to respond to the mailing, they are marked as inactive. Once a voter is marked as inactive, the voter will remain in that status until they vote or update their information. An inactive voter can still cast a ballot at their polling location, but must sign an affidavit confirming their address. Once the affidavit is signed, the voter is able to vote and will be moved back to active status in SURE as part of a post-election process. If the voter fails to vote in the next two consecutive general elections for federal office (four or more years after being moved to inactive status), the county should cancel the voter's registration.

In addition to cancelling a voter's registration due to inactivity, a county should cancel a voter's registration if the county receives a written request from the voter to have their voter registration cancelled or is notified that the voter died or moved out of state. The following table summarizes the number of active and inactive voters whose registrations were cancelled and the reason for cancellation in the calendar years 2015-2018:

[23] 52 U.S.C. § 21083(a)(2) and 25 Pa.C.S. § 1901(b)(1)(i).

Pennsylvania Department of State Number of Active and Inactive Voters Cancelled by Reason for Calendar Years 2015-2018						
Calendar Year and Voter Status	Cancelled at Voter's Request	Cancelled due to Voter's Death	County Confirmed Change of Address[a/]	PennDOT Confirmed Change of Address	Voter Removal Programs[b/]	Total
2015 Active	1,280	91,951	20,405	86,476	5,955	206,067
2015 Inactive	351	13,321	5,713	10,473	156,107	185,965
2016 Active	1,605	76,987	100,956	90,565	3,935	274,048
2016 Inactive	374	11,799	23,328	11,253	83,515	130,269
2017 Active	1,859	93,649	21,963	101,984	3,979	223,434
2017 Inactive	251	10,264	3,761	8,018	233,517	255,811
2018 Active	2,311	79,178	50,602	95,332	3,458	230,881
2018 Inactive	516	12,246	12,019	10,916	113,576	149,273

[a/] Includes if the county visited the address on record to confirm the voter no longer lives there.
[b/] Cancelled because no response was received after various mailings.
Source: Produced by the Department of the Auditor General staff based on information from the Pennsylvania Department of State's "The Administration of Voter Registration in Pennsylvania, 2018 Report to the General Assembly" dated June 2019.

The Status of Pennsylvania's Voting Systems

HAVA not only requires that each state has a general registry for voter registration, it also placed mandates on the states regarding voting systems. While HAVA was a funded mandate (see *Appendix F* for federal money received by Pennsylvania, by year) from the federal government, the money has waned in the past several years. Technology however, continues to evolve, and the HAVA-compliant voting machines purchased over a decade ago are reaching or have already reached, the end of their useful life. In April 2018, DOS informed all counties that they must select a voter-verifiable, paper record voting system no later than December 2019, but ideally they should have one in place for the November 2019 election.[24] At the time of this mandate, the voting systems in use in 50 of the 67 counties in Pennsylvania did not have the ability to record votes with a hard-copy record and, therefore, were not in line with the new mandate from DOS. DOS received $14.15 million in August 2018.[25] This money has been used to assist the counties in replacing their voting systems, however, this amounts to only approximately 10 percent of the estimated total statewide cost of $150 million.[26] In October 2019, an election reform bill was

[24] <https://www.governor.pa.gov/governor-wolf-statement-directive-new-voting-machines-paper-record/> (accessed May 16, 2019).
[25] This $14.15 million consisted of 95 percent federal funding and a 5 percent state match.
[26] County Commissioners Association of Pennsylvania, *Election Equipment and Voting Systems*, <https://www.pacounties.org/GR/Documents/1-ElectionEquipmentPriorities2019.pdf> (accessed May 16, 2019).

signed into law by Governor Wolf that included $90 million to assist the counties with purchasing new voting systems.[27]

All voting systems to be used in Pennsylvania must be certified by both the federal Election Assistance Commission and the Secretary of the Commonwealth.[28] As of June 13, 2019, DOS (via the Secretary) certified seven new voting systems for use in Pennsylvania.[29]

DOS Plans to Replace the SURE System

As noted above, the SURE system in place today was initially implemented and rolled out beginning in 2003, making it over 15 years old. DOS management stated that they are starting the process to obtain and implement a new SURE system. DOS is currently working with the Office of Administration, Office for Information Technology to develop a request for proposal to replace the SURE system.

[27] *See* Act 77 of 2019, enacted October 31, 2019 (Immediately effective with exceptions).
[28] 25 P.S. § 3031.5.
[29] <https://www.media.pa.gov/Pages/State-Details.aspx?newsid=342> (accessed September 23, 2019).

Finding 1 – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

In November 2017, the Pennsylvania Senate's State Government Committee considered legislation that would require the Pennsylvania Department of the Auditor General (DAG) to audit the Pennsylvania Department of State's (DOS) Statewide Uniform Registry of Electors (SURE). Various members of our state legislature voiced concerns regarding the security of Pennsylvania's voting systems after several national media outlets reported allegations of foreign actors hacking multiple states' voter registration databases.[30]

DOS contacted DAG to discuss the pending legislation, and after various meetings between DAG, DOS, the Pennsylvania Governor's Office of Administration, Office for Information Technology (OA/OIT), and the Senate State Government Committee, it was agreed that DOS and DAG would enter into an Interagency Agreement (agreement) to conduct an audit which would accomplish the goals set forth in the proposed legislation. The agreement tasked DAG to audit the SURE system and outlined specific audit objectives to be performed that satisfied the interests of all parties involved.[31]

As the audit progressed, however, DOS failed to comply with the agreement's provision requiring that they cooperate with DAG's requests related to the audit. In addition to language in the agreement, Pennsylvania law requires DOS to cooperate with the DAG.[32] This failure impeded DAG's ability to timely conclude the audit and, as outlined in the table below, resulted in significant scope limitations that affected DAG's ability to achieve audit objectives 1, 3, and 6.

[30] More recently, there has been concerning news of hacking the databases of all 50 states and federal officials have noted major concerns about Pennsylvania's system. https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html and https://www.nytimes.com/2019/07/26/us/politics/states-voting-systems.html (accessed August 12, 2019).

[31] See *Appendix B* for a copy of the original agreement.

[32] Please note that Section 502 (relating to Cooperative duties) of the Administrative Code of 1929 provides as follows: "[w]henever, in this act, **power is vested in a department**, board, or commission, to inspect, examine, secure data or information, or to procure assistance, from any other department, board, or commission, **a duty** is hereby imposed upon the department, board, or commission, upon which demand is made, to render such power effective." (Emphasis added.) *See* 71 P.S. § 182 (Adm. Code § 502). This section of the Administrative Code clearly requires that whenever an administrative agency (DAG) has a power to secure an audit as provided in statute, any other agency (DOS or the Pennsylvania Department of Transportation) requested to provide such documents has the duty to be cooperative.

Objective Number	Objective	Able to Achieve Audit Objective	Detail Found in Finding Number
1	Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law.	No (See Scope Limitation B below)	2, 4, 5, 6
2	Evaluation of the process for input and maintenance of voter registration records.	Yes	4
3	Review of security protocols of the SURE system.	No (See Scope Limitation A below)	1, 3 [a/]
4	Review of the efficiency and accuracy of the SURE system.	Yes	5
5	Review of the internal controls, methodology for internal audits and internal audits review process.	Yes	4
6	Review of the external controls, methodology for external audits and external audits review process.	No (See Scope Limitation A below)	1 [a/]
7	Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance.	Yes	7
8	Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.	N/A[b/]	No Finding[b/]

[a/] - Due to its sensitive nature, we summarized the scope limitation in these findings, but included relevant detailed information in a separate confidential communication to DOS.

[b/] - While no other areas were added to the audit objectives and we do not have any findings or recommendations outside those related to the first seven objectives, see *Appendix D* regarding an issue that occurred during the audit period but was corrected prior to the beginning of the audit. The issue concerns the lack of oversight that allowed non-citizens the ability to register to vote at the Pennsylvania Department of Transportation's (PennDOT) photo license centers even after indicating they are not a citizen. We did not test for citizenship as part of this audit because citizenship information is not maintained in the SURE system, however, we did obtain from DOS certain information they were willing to provide regarding steps taken to address this issue. Other information regarding management's investigation and analysis of the situation was not provided. See further details in *Appendix D*.

After the agreement between DOS and DAG was executed on May 21, 2018, DAG promptly issued a standard engagement letter on May 22, 2018 to begin the audit. The engagement letter stated that DAG would release its final report on or before January 31, 2019, which was the date provided for in the agreement. Due to a lack of cooperation from DOS, PennDOT, and certain county election offices (counties), as well as a failure to provide the necessary information needed to satisfy the audit objectives, it became evident that DAG would not be able to perform the audit in accordance with certain applicable standards in *Government Auditing Standards*, which is issued by the U.S. Government Accountability Office. The standards in question included obtaining sufficient appropriate evidence, evaluating the design and operating

effectiveness of information technology (IT) controls, and reviewing previous audits and attestation engagements significant within the context of the audit objectives.[33] In February 2019, the original agreement was amended, and the date for final audit report release was extended to July 31, 2019. Due to a continued lack of cooperation from DOS in terms of providing requested information, this date was further postponed to September 27, 2019.[34]

The agreement included responsibilities of both DOS and DAG. The first responsibility listed for DOS was to **"cooperate with the Auditor General's requests involving the proposed audit"**; however, as discussed throughout the report, DOS did not provide us with responses to all of our requests. Instead of terminating the engagement due to lack of cooperation, which was justifiable under the terms of the agreement, in an effort to salvage an audit of paramount importance intended to enlighten Pennsylvania's electorate on the issue of election security and reliability, DAG issued a modified *Government Auditing Standards* compliance statement for this audit to account for the significant scope limitations that resulted from DOS' refusal to provide access to documentation and data required to complete the audit.

As a direct result of this sustained refusal to cooperate with our data requests without plausible justifications, DAG was unable to establish with any degree of reasonable assurance that the SURE system is secure and that Pennsylvania voter registration records are complete, accurate, and in compliance with applicable laws, regulations, and related guidelines. These weaknesses, despite the full performance of DAG under the terms of the agreement, combined with the recent increased threats from cyber intrusion, leaves serious questions and concerns regarding Pennsylvania's voter registration system and records.

The following sections describe in greater detail the various scope limitations, how each affected our abilities to satisfy the audit objectives, and the uncooperative nature of DOS, PennDOT, and certain counties throughout the audit.

[33] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to evaluating the effectiveness of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.
[34] Subsequently, DOS requested a further extension for the final audit report to be released by November 29, 2019.

DOS-Imposed Scope Limitations Impacting Audit Objective Achievement

Scope Limitation A

We attempted to document a complete understanding of the complex IT security landscape supporting the SURE system and evaluate the design and operating effectiveness of IT controls using a four-pronged approach:

1. Document the IT system landscape of the SURE system and its supporting infrastructure.

2. Document governance over cybersecurity using the National Institute of Standards and Technology Framework and review security assessments previously performed by outside entities.[35]

3. Document and test IT General Controls as defined by the US General Accountability Office, *Standards for Internal Controls in the Federal Government* (Green Book).[36]

4. Interview and survey county election offices and county IT staff.

During the audit, DOS management denied us access to significant key documents/information related to the security and operation of the SURE system and, for some documents that were provided, redacted information to the extent that the documentation was not usable as evidence. The following list identifies the key documents/information that were not provided (items 1, 2, and 5) or were heavily redacted (items 3 and 4):

1. Contents of external security assessment reports issued by the United States Department of Homeland Security (Homeland Security), as well as reports issued by private firms contracted to assess security.[37]

[35] The National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity,* consists of five steps: (1) Identify critical physical and software assets, threats, vulnerabilities, and risks; (2) Protect the system and infrastructure to ensure its security and resilience; (3) Detect the occurrence of a cybersecurity event in the system and infrastructure; (4) Respond to and contain a detected cybersecurity incident; and (5) Recover and restore system data, capabilities, and services impacted by a cybersecurity incident. See <https://www.nist.gov/cyberframework> (accessed June 11, 2019).

[36] We attempted to compare the policies, procedures, and practices over the SURE system to the IT General Control best practices described in Principle 11 of the S*tandards for Internal Controls in the Federal Government* (Green Book), issued September 2014. The Pennsylvania Governor's Office adopted these federal standards for all Commonwealth agencies within Management Directive 325.12, effective July 1, 2015.

[37] We confirmed with audit agencies in other states that their auditors are provided access to security assessment reports issued by private firms and at least one other state has received security assessment reports issued by Homeland Security.

2. Systems and Organization Control reports detailing the security practices in place at outside vendors key to the security and operation of the SURE system.[38]

3. Detailed information on system configuration and implementation of cybersecurity policies.

4. The formal results and corrective action plans from the 2018 test of the emergency recovery system.

5. Documentation of significant IT controls and system interfaces.

In lieu of these key documents, DOS instead provided us with an affidavit from the Chief Information Security Officer of the Employment, Banking, and Revenue Delivery Center of OA/OIT stating that IT security controls were in place. This affidavit however, does not provide sufficient, or even appropriate, audit evidence as a basis for conclusions.

Without these critical documents listed above, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards*, which requires auditors to evaluate the effectiveness of IT controls and review previous audits and assessments significant within the context of our audit objectives.[39] DOS's refusal to provide these documents resulted in our inability to provide a conclusion regarding the security of the SURE system. It is important to note that DOS originally requested this performance audit and agreed to the audit objectives, as well as for DAG to conduct the audit in accordance with *Government Auditing Standards*; therefore, its refusal to provide the documents is of great concern.

Additionally, as a result of not being provided access to the contents of the external security assessment reports, we were not able to determine what these assessments included and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6). We were also unable to determine if any security weaknesses were noted in the assessments or whether corrective actions have been implemented. Further, until our audit revealed that DOS had failed to enact a policy for marking, handling, sharing, and storing Election Infrastructure (EI) information, DOS was unaware of the vital importance of having such a policy.[40] This is deeply concerning because the absence of such a

[38] Systems and Organization Control (SOC) reports are reports on a service organization's controls by an independent auditor.
[39] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.23 through 6.27.
[40] Department of State, *Policy on Election System Security Measures*, Version 1.1, issued April 23, 2019, which establishes DOS policy regarding the identification, marking, handling, storage, and protection of Election Infrastructure Information, was issued after our audit cutoff date of April 16, 2019 for information submissions so that the report could be prepared.

critical policy dealing with EI information is indicative of systems that lack adequate controls or uniformity of protocols.

It is also important to note that DOS had initially agreed to provide us with access to these security assessments on July 9, 2018, but on the very day that such reports were to be provided to DAG, DOS advised us that we were not permitted to view the reports due to "policy." We requested a copy of the DOS policy restricting access to these reports and were not provided the policy until late April 2019, over nine months later. The effective date of the policy that DOS eventually provided to us restricting access to these and other documents dealing with the SURE system was April 23, 2019, many months after we had been refused access to such records and many months after we had requested a copy of DOS' policy. If the security assessment reports were as sensitive as claimed by DOS, we are concerned that DOS had no policy in place dealing with such critical information until April of 2019.

Further, while DOS refused to permit DAG the ability to review these documents, in October 2018, we were provided with a list of **20** persons who had access to these reports. This list not only included one contractor who was not a Commonwealth employee, but it was unclear why the remaining **19** DOS and OA/OIT employees needed such access.[41] Finally, DOS repeatedly advised us that the security assessments were not to be provided because Homeland Security had designated election infrastructure as "critical infrastructure" which prevented DOS from releasing the reports to DAG. Despite repeated requests over six months for a statement in support of this contention, DOS claimed that they were unable to obtain such a statement from Homeland Security. During the course of our audit, we were able to determine that these types of reports are provided to auditors in another state and as noted below, Homeland Security did not have concerns about DOS sharing the reports with DAG.

In a letter dated August 17, 2018, DOS' Chief Counsel denied DAG's request to review the security assessment reports on the SURE system issued by Homeland Security and other outside entities citing that pursuant to the USA Patriot Act, Homeland Security designated election systems as part of critical infrastructure as defined under the Critical Infrastructure Information Act of 2002 (CIIA).[42] It was the opinion of DOS' Office of Chief Counsel that the outside security assessment reports were protected critical infrastructure information (PCII) and could only be accessed by those with an absolute "need to know" in order to perform homeland security duties.[43] The Auditor General traveled to Washington, D.C. to meet with representatives from Homeland Security who stated, however, that sharing the reports was left up to the discretion of each particular state.

---

[41] While the contractor is not an employee, he is a contractor who performs critical functions in the SURE system. While the contractor's duties are necessary for the operation and security of the SURE system, see *Finding 3* for our concerns about governance over the SURE system.

[42] *See* 42 U.S.C. § 5195c(e), 6 U.S.C. §§ 131-134, respectively.

[43] Yet, it was not clear whether all 19 DOS and OA/OIT employees actually needed access to the reports. Later in the audit, DOS represented that certain employees' access to these reports was revoked after our audit request made DOS question why the access had been granted.

We considered review of the security reports and access to sensitive security information to be so crucial to our audit objectives, that we offered to review the reports and sensitive information in a secure setting with DOS supervision. Our offers to provide these additional security measures were refused repeatedly by DOS. Without access to the reports we could not determine the following:

- If all of the servers and supporting infrastructure used in the SURE system were included in the security testing.
- If the external security assessors were provided unrestricted access and performed their work in accordance with standards.
- If all relevant controls were tested.
- If exceptions were noted.
- If appropriate corrective actions were implemented.

Without an independent assessment of these reports and any corrective actions taken by DOS in response to these reports, the public has no assurance that DOS is taking proper steps to secure the SURE system. We cannot, with any degree of certainty, have confidence in the security of the SURE system because we were not permitted to review the reports or the other documents/information we requested. Our offers to review reports and documents/information in strictly controlled settings make DOS' refusals to cooperate that much more difficult to defend.

Scope Limitation B

As part of our audit procedures, we selected a random, statistical sample of 196 voters from the total population of 8,567,700 voters registered as of October 9, 2018, with the intention of reviewing source documents to confirm the accuracy of the voter record information in SURE and to confirm that a signature was on file for the voters indicating that they had affirmed that they were legally qualified to vote (Objective 1).[44] Source documents include the voter registration applications or information provided by the individuals to update their voter record. Of the 196 voters in the sample, we were unable to verify the accuracy of information for 138 voters, or over 70 percent of the sample. Depending on the source of the voter's application, we found that:

- DOS maintained no source documentation for the 19 voter records reviewed that were created through online applications.

- PennDOT did not provide access to source documentation for the 93 voters who registered to vote through the Motor Voter process.

[44] Statistical sampling means to select a limited number of items from the population on a systematic or random basis, review/test those items, and then draw a conclusion about the entire population based on the results of the items selected for testing with a statistically measurable degree of confidence considering the accepted percent rate of tolerable error. Our statistical sample of 196 voters was determined based on a confidence level of 98 percent and a tolerable error rate of 2 percent.

- Four counties did not respond to our request for 12 paper applications.

- Twelve counties confirmed they did not have paper applications on file to support 14 paper applications.

Due to the lack of cooperation from certain counties, PennDOT (regarding information from the Motor Voter system), and the system design of online applications, we were unable to perform adequate tests to determine the accuracy of the voter record data in SURE. We are therefore unable to form any conclusions as to the accuracy of the entire population of voter registration records maintained in SURE. Inaccurate voter records could ultimately lead to ineligible individuals being able to vote in elections or one individual being able to vote multiple times. An accurate and effective voter registration system, as well as public confidence in such a system, is critical in the current environment where a significant threat of hacking election records and results exists. See *Findings 2 and 6* for further details.

Overall

The aforementioned scope limitations encountered during the audit contributed to our conclusion that the SURE data used in this audit has significant limitations.

The uncooperative nature of DOS, PennDOT, and certain counties throughout the audit.

Contributing further to the significant scope limitations, we found that DOS was not only uncooperative, which was inconsistent with our agreement and state law, it was untimely in providing us the information we needed in order to satisfy our audit objectives.[45] As quoted previously, the agreement required DOS to cooperate with DAG's requests related to this audit. Specifically, DAG's audit engagement letter stated that DOS shall provide us with requested information or documentation within three working days of the request, which is a standard business practice. It was further communicated to DOS that if this pre-established timeframe was insufficient and DOS would need additional time to prepare its response, DAG would approve a reasonable extension if requested.

We submitted 66 individual official requests for information to DOS throughout the audit. We received 11 responses within the pre-established three-day timeframe. The information for the other 55 however, was either never provided or not received by the due date and, with one exception, DOS never requested an extension. This equates to DOS being untimely for more than **83 percent of information requests** on the audit that they requested. Regarding items that DOS never provided, there were 11 such instances that information was not provided even after several months of our repeated attempts to obtain the information. Despite this unresponsiveness,

[45] *See* 71 P.S. § 182 (Adm. Code § 502).

we continued to send reminders to DOS regarding the outstanding requests for information and emphasized the importance of receiving the documentation requested. As seen in the following table, it took DOS weeks, or in some cases months, to respond to certain requests after numerous appeals from us.

DOS Delays in Responding to Audit Information Requests	
Length of Time that DOS was Late in Responding to Information Requests [a/]	**Number of Requests**
Never provided [b/]	11
61-94 days late	2
31-60 days late	7
15 – 30 days late	13
4 -14 days late	12
1-3 days late	10
Total	**55**

[a/] - Timeframes are based on calendar days.
[b/] - We received no information for nine requests and only received a portion of the information for two requests.

The information provided by DOS 94 days late was the voter registration records for the population of registered voters in SURE. DOS was aware that this information, which took over three months to provide, was absolutely critical to us for performing data analysis as part of our audit procedures. Additionally, as previously mentioned, PennDOT did not provide source documentation for the 93 voters in our sample that registered to vote through the Motor Voter process, and four counties did not respond to our request for 12 paper applications. Delays and uncooperativeness of this magnitude were not only inconsistent with our agreement and state law but had a detrimental effect on our ability to perform our audit procedures and satisfy the audit objectives.

As a result of repeated delays (several extending for many months), non-responses, and refusals to provide information responsive to our official requests, the agreed upon audit report release date had to be extended and DAG was forced to establish a cutoff date of April 16, 2019 for information submissions in order to ensure that sufficient time would be allotted to prepare the report.

Conclusion

Despite experiencing these difficult impediments throughout the audit, we were able to complete many audit procedures, including some related to audit objectives 1, 3 and 6, and report our results and recommendations in *Findings 2 through 7*, accordingly. Based on our interviews with DOS, OA/OIT, and county management executives; data analysis; on-site interviews and

observation of procedures at seven counties; written surveys of Pennsylvania's 67 counties; and other audit procedures as explained throughout our report; we report the following findings:

- Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system. (see *Finding 2*)

- The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records. (see *Finding 3*)

- Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system. (see *Finding 4*)

- Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy. (see *Finding 5*)

- A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system. (see *Finding 6*)

- The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention. (see *Finding 7*)

We believe that it is imperative that DOS management take steps to implement the recommendations that we were able to include in this report, albeit based on DAG's significantly restricted ability to perform standard auditing practices, to ensure the completeness, accuracy, and auditability of the voter registration data recorded in the SURE system.

Recommendations for Finding 1

We recommend for future audits that DOS:

1. Arrange for independent audits of all parts of the SURE system, supporting architecture, and connected systems using a comprehensive framework of security standards, which includes tests of IT general controls, tests of cybersecurity controls, vulnerability

assessments, and penetration testing. These audits should be performed annually and build on security assessments already performed.

2. Cooperate with auditors by providing them with full, confidential access to all information and documents, to comply with state law and to allow the auditors to satisfy the audit objectives, especially when requesting a particular audit to be performed by a fellow public agency charged with doing audits.

3. Provide appropriate and sufficient supporting evidence to back up its assertions that disclosure of certain materials to an auditing agency is legally impossible.

4. Encourage counties, PennDOT, and other related agencies involved in voter registration to cooperate with future audits.

5. Provide specific policies and direction from federal authorities supporting DOS' position in the event that it believes that it cannot provide information pursuant to security concerns.

6. Provide the results of audits recommended above to those charged with governance of the SURE system.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

As part of audit procedures to address the accuracy of the voter registration information contained in the Statewide Uniform Registry of Electors (SURE), on July 10, 2018 we requested electronic files of all currently registered voters and the history of all of the changes made to voter records, such as changes to a voter's name or address that were recorded during the period January 1, 2016 through present. We also requested copies of each county's Pennsylvania Full Voter Export List from the SURE system available to the public through the Department of State (DOS) website.[46] It took three months for DOS to provide the electronic files. The files contained voter registration records for 8,567,700 registered voters as of October 9, 2018.[47]

Using these files we performed the following:

- Selected a statistical sample of voter records to determine whether the information contained in SURE agreed with the information contained on the voter registration application (application). (see *Finding 6* for results and conclusions)

- Data analysis to evaluate the information within SURE for reasonableness. (see below)

Data Analysis[48]

To perform data analysis, we utilized software that allowed us to sort, classify, match, and validate information (data fields) within SURE to look for potential errors or inaccuracies within the fields.[49] Once identified, in certain instances, we also attempted through data analysis to

[46] As provided by 25 Pa.C.S. § 1404(b)(1) (relating to Public Information Lists), as well as the SURE Regulations at 4 Pa. Code § 184.14(b) (relating to Public Information Lists), DOS will provide the Full Voter Export List to requestors. This version of the Public Information List is a full export of all voters in the county and contains the following fields: voter ID number, name, sex, date of birth, date registered, status (e.g., active or inactive), date status last changed, party, residential address, mailing address, polling place, date last voted, all districts in which the voter votes (e.g., congressional, legislative, school district, etc.), voter history, and date the voter's record was last changed.

[47] See *Finding 1* for discussion regarding delays by DOS and scope limitations to the audit.

[48] In spite of the limitations with regard to completeness and accuracy of the information in SURE (See *Findings 1, 2, and 6*), we conducted additional data analysis and found that the voter table agreed with published reports and that the overwhelming majority of records in SURE were consistent throughout the various tables within the system. As a result, this data is considered reliable with significant limitations. See *Appendix A* for more information.

[49] The software we used included Excel and ACL. ACL data analytics is a data extraction and analysis software used for audit, fraud detection, and risk management. By sampling large data sets, ACL data analytics software is used to find irregularities or patterns in data records that could indicate control weaknesses or fraud.

assess the possible causes for the errors or inaccuracies. Weaknesses in the controls with regard to processing applications and subsequent list maintenance are separately addressed in *Finding 4*.

The following summarizes the results of our data analysis:

- **24,408 cases** – The same driver's license (DL) number listed in more than one voter record:
  - **18,536 potential duplicate cases** – A voter may have two or more records.
  - **5,872 potential cases** – Two or more voter records have the same DL number.
- **13,913 potential duplicate cases** – The same first name, last name, and date of birth (DOB) and/or last four digits of Social Security number (SSN) are shared by more than one voter record.
- **6,876 potential DOB inaccuracies** – The DOBs equate to voters being 100 years of age or older.
- **2,230 potential DOB and/or registration date inaccuracies** – The DOBs listed are after the registration date.
- **2,991 records of potentially deceased voters** – The same first name, last name, and DOB and/or last four digits of SSN match the Pennsylvania Department of Health (DOH) deceased files.

Throughout the remainder of this finding, we describe the results of our data analysis. Due to audit time constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS will need to work with the counties to follow up and address all these situations in order to investigate and correct the voter records as appropriate.

24,408 Cases – The same DL number listed in more than one voter record.

Of the approximately 8.6 million voter records, 7,938,806 records contained DL numbers, which should be unique to only one person.[50] We analyzed data to determine if the same DL number appeared in more than one voter record and found 24,408 cases as noted below:

[50] A DL number is not required to register to vote.

Voter Registration Records with the Same DL Numbers as of October 9, 2018		
Number of Cases the Same DL Number is Listed in More than One Record[a/]	**Total Number of Records Involved**	**Personal Elements**
7,540	15,100	Same DL Number, First Name, and Last Name
10,329	20,715	Same DL Number and First Name only
667	1,336	Same DL Number and Last Name only
18,536	**37,151**	**Total Number of Potential Duplicate Cases**
5,872	11,768	Same DL Number, Different First and Last Name
24,408	**48,919**	**Total Records with Duplicate DL Number**

[a/] 24,305, or over 99 percent, of the total cases with potential duplicate records, were pairs of records. The remaining 103 instances consisted of three records containing the same DL number.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As shown in the table above, we evaluated the information based on what personal elements were the same and summarized accordingly. More than 18,500 cases were found where the two records that matched the same DL number also matched either the first name, last name, or both. We consider these cases to be voters that potentially have two or more records within SURE (potential duplicate records). We will discuss the possible reasons that this occurred in the next section of this finding. Having two or more records could potentially allow a voter to vote more than once in an election.[51]

We also identified in the above table 5,872 cases, involving 11,768 records that had the same DL numbers but different first and last names. Although it is possible that a few of these cases relate to the same individual with more than one voter record, it is much more likely that these results indicate that a typographical error occurred when the DL number was entered into SURE. See *Finding 4* for weaknesses related to data entry errors and *Finding 5* for lack of edit checks.

13,913 Potential Duplicate Cases – The same first name, last name, and DOB and/or last four digits of SSN are shared by more than one voter record.

In addition to our analysis of DL numbers, we analyzed the remaining 8,518,781 records in SURE that either had no DL number recorded or had a unique DL number recorded and were not reported as duplicates above. We identified an additional 13,913 cases where two or more

[51] Voting more than once in an election is against the law and considered a felony offense of the third degree. *See* 25 P.S. § 3535 (relating to Repeat voting at elections).

records shared first name, last name, and one or more other personal elements as summarized in the following table:

Voter Registration Records with Other Duplicated Information as of October 9, 2018		
Number of Cases with Three or More of the Same Personal Elements[a/]	**Total Number of Records Involved**	**Personal Elements**
6,427	12,872	Same First and Last Name and DOB
7,230	14,506	Same First and Last Name and last 4 digits of SSN
256	525	Same First and Last Name, DOB, and last 4 digits of SSN
13,913	**27,903**	**Total records with other duplicated information**

[a/] - The vast majority of these cases were instances where a pair of records shared the same information; however, 68 cases (213 records in total) had three or more instances of duplicate information with up to 10 records sharing identical information for one voter. Of the 68 duplicates, 1 individual had 10 active records matching on first and last name, DOB, and last 4 digits of their SSN, while another individual had 5 active records matching on the same personal elements. The remaining 66 cases (198 records in total) consisted of sets of 3 potentially duplicate records.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Because these 13,913 cases share three or more personal elements, we consider these as potential duplicate records (i.e., an individual potentially has more than one voter record). Again, it is incumbent upon DOS to work with the counties to evaluate these potential duplicate records to determine if in fact they are duplicate records or whether some of the personal elements may have been incorrectly entered into SURE. Having two or more records could potentially allow a voter to vote more than once in an election.

Ineffective process for identifying duplicate records.

One of the steps to process an application includes making sure that the individual applying to register to vote does not already have a voter record in SURE (i.e., to avoid creating a duplicate record). DOS regulations require, at a minimum, a duplicate check using the registrant's first and last name as well as DOB.[52] If upon examining those initial criteria county staff believes that the record may be a duplicate, the regulation indicates that staff then should use other criteria to assess duplication, including:

[52] 4 Pa. Code § 183.6. (relating to Uniform procedures for the commissions relating to the process for identifying and removing duplicate records in the SURE system).

- The unique identifier.[53]
- The last four digits of a registrant's SSN.
- The DL number of the registrant.
- The signature of the registrant.[54]

To ensure compliance with the regulations, DOS creates and distributes job aids that provide step-by-step instructions on how to perform the duplicate checks. Specifically, county staff are instructed to perform two duplicate checks: (1) same last name and same DOB; and (2) same first and last name. The job aid then notes that additional duplicate checks "*can be made*" and provides instructions on how to perform those additional duplicate checks, including checks for duplicate DL numbers.

In order to understand the duplicate check process, during our on-site visits to seven counties, we observed staff processing new applications check for duplicate records. We noted that when staff entered the voter information into SURE, several records associated with a particular name might be displayed. It is then up to staff to manually determine whether the application is a duplicate of a voter record already in SURE. Once county staff determine that the applicant does not have a duplicate record, they indicate that in SURE and continue processing.

Although this process appears to be in compliance with the respective job aids and the regulations, it is not effective in ensuring that duplicate records are not being created. The SURE system does not require staff to check for duplicate DL numbers, if available, which is a unique number to an individual and should be a key element for determining whether an individual already has a voter record. Additionally, as noted in the next section, using DOB as key criteria for identifying a unique person will not work if the DOB is not correct in SURE. Further, as noted previously, this process is generally a manual one and can be labor intensive. According to county staff, during certain times of the year, such as prior to the general election, the number of applications counties receive for processing becomes voluminous. Processing a lot of applications within a short period of time, however, can lead to errors and reduce the effectiveness of the process for identifying duplicates. We also noted that the SURE system does not have any automated edit checks or a "hard stop" that prevents staff from adding a voter registration record with a DL number that is already associated with an existing voter record.

Therefore, DOS needs to re-evaluate its regulations and job aids to develop a more effective duplicate check process, especially since DOS is looking into replacing the existing SURE system (see the *Introduction and Background* section) so that the replacement system for SURE is designed to prevent or detect and correct duplicate voter records.

[53] The unique identification number consists of a nine digit number plus a two digit county identifier. The nine digit number should stay with the voter if they move to a new county, but the two digit county identifier should be updated to reflect the new county of residence.
[54] 4 Pa. Code § 183.6.

6,876 potential DOB inaccuracies – The DOBs equate to voters being 100 years of age or older.

In addition to analyzing records for potential duplicate records, we conducted data analysis regarding the reasonableness of voters' DOB. DOS informed us that inaccuracies existed regarding DOBs due to DOBs not being a required field for registering to vote at some point prior to the Help America Vote Act of 2002 (HAVA). According to both DOS and county staff, when data was migrated into the SURE system from the 67 counties' systems, a "generic" DOB was entered for voters who did not have a DOB listed.

As part of our DOB reasonableness analysis, using the 8.6 million registered voters' files, we evaluated DOBs for voters whose SURE record indicated that the voter was 100 years of age or older. The following table provides a summary of the analysis:

Voter Registration Records Indicating that the Voter was 100 Years of Age or Older as of October 9, 2018

Number of Registered Voters	Number of Potentially Deceased[a/]	Age Range
1,800	0	110 years of age or older – DOB recorded as January 1, 1800, January 1, 1900, or January 1, 1901
518	2	110 years of age or older – Other DOB recorded
4,558	134	100 through 109 years of age
6,876	**136**	**Total records indicating voter was 100 years of age or older as of October 9, 2018**

[a/] Of the 6,876 registered voters with DOB in the SURE system indicating that they were 100 years of age or older, 136 were also identified as potentially deceased (discussed later in the finding).

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations regarding completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As noted in the table above, we identified three "generic" dates (January 1, 1800, January 1, 1900, and January 1, 1901) accounting for 1,800 of the 6,876 voters (26 percent) who are potentially 100 years of age or older. As these dates are not accurate DOBs, DOS needs to work with the counties to correct these inaccuracies as well as determine whether the voters are potentially deceased (see next section).

It is also unlikely that most of the 518 records with DOBs indicating the voters are 110 years of age or older are accurate. According to the most recent United States Census Report for 2010

(census report), the number of persons 110 years old and over was just 330 nationwide.[55] Similarly, many of the 4,558 records in SURE where the DOB indicates that the voter was between 100 and 109 years old are potentially inaccurate. According to the census report there were only 2,510 Pennsylvanians over the age of 100 in 2010.[56] Therefore, our analysis demonstrates the need to research these voters' records and correct these records, if necessary.

Without accurate DOBs in SURE, county staff may fail to detect duplicate records as discussed in the prior section. Additionally, it can prevent county staff from accurately matching DOH death files with SURE records potentially allowing deceased individuals to remain on the voter rolls (see last section of this finding for more information).

2,230 Potential DOB and/or Registration Date Inaccuracies – The DOBs listed are after the registration dates.

In addition to looking at the potential age of the voter, we also compared the DOB to the registration date for reasonableness. Since an individual cannot be born after registering to vote, this comparison would indicate that the DOB or the registration date would be inaccurate, although it is also possible that both could be inaccurate. We found 2,230 voter records in which the DOB listed is after the registration date.[57]

Of the 2,230 voter records that listed DOB after the registration date, we found through data analysis that the DOB in 1,943 records, or 87 percent, was changed on the same day: December 13, 2008. Given the voter registration date was prior to the DOB, these records were changed inappropriately at that time. We also noted that some of the voter registration dates in this group were listed as prior to the year 1900, obviously errors or additional cases where staff filled in a value to facilitate the transfer of records to the SURE system. Again, DOS will need to work with the counties in order to fix the inaccuracies found.

Weaknesses and concerns regarding DOBs.

As noted in this section and the previous section, there are several thousand potential inaccurate DOBs and probably thousands that we have not detected. In order for the information to be accurate in SURE, sufficient controls must be developed to reduce the likelihood of data entry errors. *Finding 4* describes the weaknesses identified during the audit regarding data entry errors. Additionally, *Finding 5* describes the need for the SURE system or its replacement system to

[55] US Census Bureau, Centenarians: 2010, 2010 Census Special Reports, December 2012, <https://www.census.gov/prod/cen2010/reports/c2010sr-03.pdf> (accessed April 8, 2019). As noted in *Appendix A*, data from the US Census Bureau is of undetermined reliability; however, this is the best data available. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

[56] Ibid.

[57] Two of the 2,230 records were also included in the table of voters 100 years old and over.

have a "read only" feature for certain personal elements that would not typically change, such as DOB. Further, DOS should consider developing an automated process that would prevent SURE and/or its replacement system from accepting obviously inaccurate DOBs as well as questioning dates that do not make sense, such as DOB after the registration date. These types of edit checks would help reduce data entry errors.

2,991 Records of Potentially Deceased Voters – The same first name, last name, and DOB and/or last four digits of SSN match DOH death files.

DOS has developed a process through the SURE system to provide the counties with death records from DOH to help the counties identify and cancel deceased voters' records. According to instructions in the job aid (described in detail in *Finding 7*) related to processing death records, for each individual included in the death record, county staff should do a search in SURE for voter records that match on the last name and DOB. A second search is then done based on first and last name (in essence, the same process as searching for duplicate records for a new application previously discussed). County staff then manually compares the death record information to the list of voter records that were matches in the two searches performed to determine if the deceased individual has a voter record. Staff can perform additional searches of voter records to include information such as an address to assist in determining if a voter record is a match. If county staff determines that a voter's information matches a deceased individual in the death record, they are to cancel the voter's record in SURE.

To determine whether there were voter records within SURE that should have been cancelled due to deaths, we first independently requested and obtained from DOH death files from the period October 1, 2010 through October 9, 2018. [58] Next, using data analysis, we compared those files to the SURE records as of October 9, 2018, and grouped the matches based on the number of personal elements that agreed and the time period that the individual was deceased per DOH records, as shown in the below table:

[58] These data were supplied by the Bureau of Health Statistics & Registries, Pennsylvania Department of Health. The Pennsylvania Department of Heath specifically disclaims responsibility for any analyses, interpretations, or conclusions.

Analysis of Potentially Deceased Individuals as of October 9, 2018				
Number of Voters Matching Four Elements[a/]	**Number of Additional Voters Matching Three Elements[b/]**	**Total Number of Voters[c/]**	**Percentage of Total**	**Time as Registered Voter After Date of Death (As of October 9, 2018)[c/]**
131	158	289	10%	181 days to 1 year
550	489	1,039	35%	Over 1 year up to 3 years
501	440	941	31%	Over 3 years up to 5 years
391	331	722	24%	Over 5 years
1,573	**1,418**	**2,991**	**100%**	**Total**

[a/] - Includes those voter records that matched first name, last name, DOB, and last four digits of SSN.
[b/] - Includes those voter records that matched using two different sets of matching elements: first name, last name, and last 4 digits of SSN; first name, last name, and DOB.
[c/] - Due to timing and to be conservative, we did not include 1,258 voters who matched three or four elements whose date of death occurred less than 181 days prior to October 9, 2018.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system and from data received from DOH. As noted in Appendix A, we determined that the reliability of the SURE data had significant limitations in regards to completeness and accuracy and that DOH death data was data of undetermined reliability. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Based on the above results using the independent data files we received from DOH, we conducted further data analysis to verify that DOH information was in fact received by DOS for the 2,991 potentially deceased voters. Our data analysis found that DOS had received at least 2,094 of the 2,991 death notices by DOH, but the record had not been cancelled as of October 9, 2018. This appears to indicate that counties received the death notice information for at least 2,094, but determined the result to not be a match. As previously stated, this is a manual process that depends on the accuracy of the data in SURE and the judgment of the county staff performing the review. If staff are reviewing the file too quickly or a piece of personal information is inaccurately listed in the voter record (such as previously described inaccurate DOBs) and therefore does not match, they may incorrectly dismiss the deceased individual record as not being a match.

Additionally, the 897 potentially deceased voters that did not seem to have a death notice could have been caused by our data analysis procedures failing to identify the SURE DOH application record because of misspellings in SURE and/or DOH death files. On the other hand, it could also indicate that there may be a problem in how DOH death files are transmitted to DOS. The process to provide DOS, and subsequently the counties, with death records is designed so that the counties only receive new death records. This is done to avoid counties having to review duplicate records. If, however, there is an update to the record of a deceased individual, this update may not be forwarded to DOS and subsequently the counties. As a result, a deceased

voter's registration may not be cancelled.[59] It is important that DOS investigate with DOH to determine if all appropriate death information is being provided to DOS so all appropriate, updated, and corrected death information is provided to the counties for processing. Failure to timely remove a deceased voter record increases the risk that records maintained within the SURE system are not accurate and therefore, not in compliance with HAVA.

Recommendations for Finding 2

We recommend that DOS:

1. Evaluate the lists of voter registration records with the same DL numbers and potential duplicate cases provided by DAG and work with the county election offices to investigate and eliminate the specific duplicate information identified during the audit.

2. Perform additional data analysis and cleansing procedures and work with the counties to remove duplicate and incorrect data from the SURE system before migration into the replacement system for SURE.

3. Create automated processes, such as a "hard stop," to prevent the inclusion of duplicate DL numbers in the design of the replacement system for SURE.

4. Evaluate and update, as needed, the instructions provided to the counties in the SURE job aids to ensure they provide adequate guidance on how to check for duplicates in the SURE system or the replacement system for SURE.

5. After conducting the cleansing procedures outlined in Recommendation 2 in preparation for migrating to the replacement system for SURE, perform periodic data analysis to ensure that duplicate records created in error are identified and removed from SURE in a timely manner.

6. Evaluate the lists of voter records provided by DAG with a DOB listed in SURE as January 1, 1800, January 1, 1900, or January 1, 1901 and who appear to be 100 years of age or older and instruct the counties to determine the correct DOB and ensure the record is still valid and the voter is not deceased.

[59] For example, if the original death record that was sent to DOS and subsequently to a county had an incorrect birthdate listed, then the county probably would not have cancelled the voter's registration due to the non-match of the birthdate. If the birthdate was later corrected to update the DOH record, this update may not be forwarded to DOS because DOH would recognize the deceased name as one that was previously sent to DOS. The county, therefore, would not receive the updated record with the correct birthdate that would provide the match and prompt the county to cancel the deceased voter's registration.

7. Create automated processes in the replacement system for SURE to prevent the recording of obviously inaccurate DOBs and voter registration dates (e.g., voter registration dates prior to DOB).

8. Evaluate the lists of potentially deceased voters provided by DAG and instruct the counties to investigate and take appropriate action to cancel deceased voters' records in SURE.

9. Consider an additional periodic comparison of the cumulative file of deaths received from DOH to records in SURE to identify any voters that may have been missed during past reviews. DOS should consider performing the match using data analysis techniques and provide matching records to the counties for follow-up.

10. Work with DOH to ensure the process is working properly regarding forwarding death records to DOS with all relevant, appropriate, and corrected information so that counties can evaluate the information and cancel the voter registrations of deceased individuals.

Finding 3 – The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

The Statewide Uniform Registry of Electors (SURE) was established, in part, to ensure the integrity and accuracy of all registration records in the system by prohibiting unauthorized entry, modification, or deletion of registration records.[60] Protecting the SURE system to ensure the reliability of voter registrations is of utmost importance based on recent events, specifically related to Russian interference in the 2016 national election. See the *Introduction and Background* section of this audit report for further information regarding the most recent United States Senate Intelligence Committee report released in July 2019 stating that voting systems in all 50 states were probably targeted in some manner.

The Department of State (DOS) is working with the Governor's Office of Administration, Office for Information Technology (OA/OIT) to develop a Request for Proposal to replace the SURE system given that it is over 15 years old. In a July 2019 report, the Brennan Center, a think tank within the New York University School of Law, interviewed DOS leadership and learned that "voter registration system replacement is absolutely about security."[61] It is imperative that DOS continue with its plans to develop and implement a replacement system to ensure the voter registration rolls are secure.

While conducting our audit procedures related to our audit objective to evaluate security protocols of the SURE system, we intended to test both security protocols, including cybersecurity controls implemented to protect the SURE system from outside cyber-attacks, as well as test information technology general controls (ITGC).[62] As described in *Finding 1*, however, DOS refused to provide us access to significant key documents related to the security, information technology (IT) controls, and operation of the SURE system.[63] Without these critical documents, we were unable to satisfy our audit objective to review the security protocols of the

[60] 25 Pa.C.S. § 1222(a), (c)(2), (c)(4), (c)(5), and (c)(14).

[61] Brennan Center for Justice. *Defending Elections: Federal Funding Needs for State Election Security*, <https://www.brennancenter.org/sites/default/files/publications/2019_07_DefendingElections_Final.pdf> (accessed July 31, 2019).

[62] ITGC are controls that apply to all systems, components, processes, and data for a given organization or IT environment. ITGCs must be designed and operating effectively in order to support the security of the systems, as well as to ensure application controls, such as edit checks, are operating effectively.

[63] As detailed in *Finding 1*, DOS contended that they were unable to provide outside security assessments and other detailed systems documentation because their election infrastructure was determined to be "critical infrastructure" by the US Department of Homeland Security (Homeland Security). However, DOS was unable to obtain confirmation of this position from Homeland Security. Further, during the course of the audit we learned that this type of information has been provided to auditors in other states. Further, DOS contended that they could not provide the information because it was against their policy. The policy in question, however, was not issued by DOS until April 23, 2019, *after* the deadline for providing documents for use during the audit.

SURE system and conduct our audit in accordance with applicable *Government Auditing Standards,* since the standards require auditors to evaluate the design and operating effectiveness of information systems controls when those controls are significant to the audit objectives.[64]

Based on the limited information that DOS management did provide to us or through review of other available information, we were able to identify gaps between leading IT security practices and the current policies, procedures, and practices protecting the SURE system and supporting architecture. Specifically, we found:

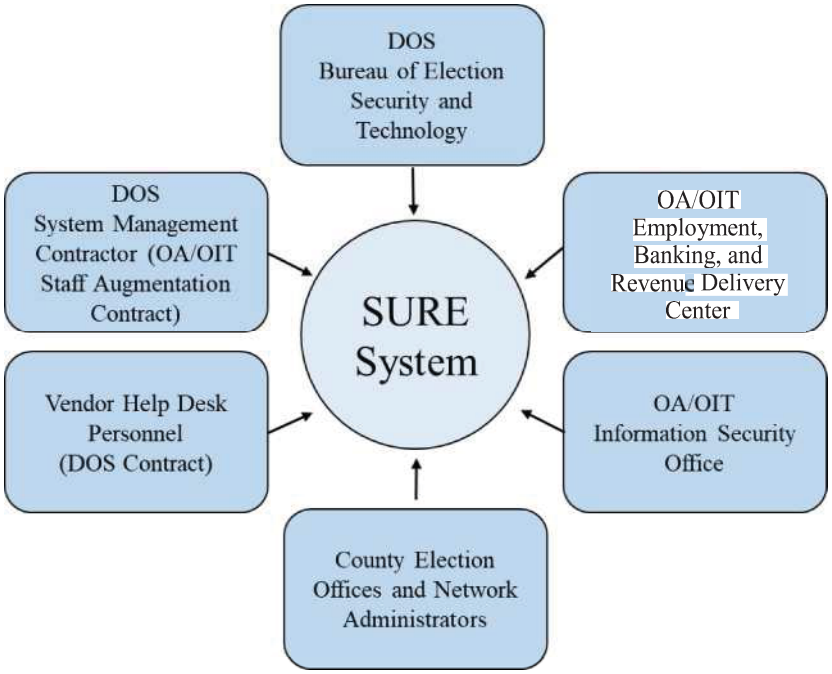
- The governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls.
- DOS management's vendor oversight practices need to be improved.
- DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties.

In addition, during our procedures we identified potential areas of improvement related to computer security, ITGCs, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

The governance structure of the SURE system and supporting architecture does not adequately define oversight and IT management in order to implement effective IT controls.

Since the implementation of the SURE system, DOS has worked with vendors, OA/OIT, and the county election offices (counties) to operate, maintain, and secure the SURE system and its supporting infrastructure. The following diagram provides an overview of the various individuals and organizations that must work together to operate, update, maintain, and secure the SURE system.

[64] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.24 states that, "When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information system controls, auditors *should* then evaluate the design and operating effectiveness of such controls." According to paragraph 215b, *Government Auditing Standards* uses the word *should* to indicate a presumptively mandatory requirement with which auditors must comply in all cases where such a requirement is relevant except in rare cases where auditors perform alternate procedures to achieve the intent of the requirement. In the case of the SURE audit, given the lack of documentation provided by DOS, no alternative procedures were possible.



Source: Produced by the Department of the Auditor General staff based on information provided by DOS management.

In April 2016, Governor Tom Wolf signed Executive Order 2016-06, assigning overall responsibility for the management and operation of IT services for all executive agencies to OA/OIT.[65] Under this Executive Order, most IT professionals in the various agencies were transferred to OA/OIT effective July 1, 2017. IT governance over the SURE system, however, has not been fully transferred to OA/OIT.

The governance structure of the individuals responsible for operation and maintenance of the SURE system includes multiple parties without defined, clear lines of authority between them. At the Commonwealth level, the Bureau of Election Security and Technology are DOS employees while most Commonwealth IT employees operating and maintaining the SURE system are OA/OIT employees. The Help Desk vendor operates under a contract with DOS, and the key IT system manager for many aspects of the SURE system is a contractor hired by DOS management through an OA/OIT staff-augmentation contract. With the counties also connected to the SURE system, the counties' systems and network administrators also have a part to play in the administration of the SURE system statewide. There is no single oversight body that coordinates all the parties and ensures an effective system of internal controls is in place that meets the needs of all stakeholders, including DOS management, the counties, OA/OIT, and registered voters of Pennsylvania.

[65] Executive Order 2016-06, *Enterprise Information Technology Governance*, dated April 18, 2016.

In addition, DOS was unable to describe or document the structure for responsibility and authority over the maintenance and operation of the SURE system and infrastructure. We requested a description of the working and reporting relationships of the various parties responsible for maintaining and securing the SURE system. DOS management was able to provide organizational charts for the technology groups in DOS and OA/OIT, and simply stated that there are no inter-organizational reporting relationships, but rather collaborative peer relationships.[66] We found this organizational structure unclear and were not provided with a document that would define authority and responsibility for these "collaborative peer relationships" described by DOS management.

The Commonwealth's standards over internal control state that management must establish an organizational structure, assign responsibility, and delegate authority in order to achieve its objectives. Additionally, the standards state the establishment of an oversight body to oversee its internal control system is foundational to effective internal controls and documentation of its internal controls systems must be adequate.[67]

Without a clearly defined governance structure and clear reporting relationships, silos of information may develop that could foster miscommunication and security gaps. It is imperative that the roles of an oversight body and IT management for maintaining and securing the SURE system be clearly defined in a governance document that provides guidance and structure to the organization. In the current high-risk environment, when outside actors have an interest in disrupting American elections and interfering with our democracy, clear lines of communication and authority are essential to timely and effectively responding to cyber threats and attacks.

DOS management's vendor oversight practices need to be improved.

DOS management relies on service organizations (vendors) for the operation and maintenance of key parts of the SURE system and its supporting infrastructure. These vendors were procured through contracts with other Commonwealth agencies, such as the Pennsylvania Department of Transportation (PennDOT) and the Governors' Office of Administration (OA), but provide services relevant to supporting the SURE system's operation and maintenance. Our procedures to review DOS's vendor management controls included requesting key vendors' System and Organization Control (SOC) reports, which are reports on a service organization's controls by an independent auditor. DOS management is required by Commonwealth policy to obtain and review vendor's SOC reports or perform other vendor monitoring when controls at the vendor

[66] DOS and OA/OIT use vendors, organizations working under an agreement with DOS or OA/OIT, to maintain and operate specific systems, as well as staff-augmentation contractors, hired to supplement Commonwealth employees, to perform similar functions as employees.

[67] The United States Government Accountability Office, *Standards for Internal Control in the Federal Government*, sections 2.01, 3.01, and 3.09. The Pennsylvania Governor's Office adopted these federal standards for all Commonwealth agencies within Management Directive 325.12, effective July 1, 2015.

are integral to the agency's system of internal controls.[68] Additionally, the Pennsylvania Department of General Services' (DGS) *IT Contracts Terms and Conditions* procurement policy requires that vendor contracts contain specific language regarding security, confidentiality, and audit provisions to aid in ensuring the security and confidentiality of the SURE system and data.

DOS management could not provide the SOC reports for service organizations or evidence that it reviewed the SOC reports and assessed whether controls at the service organizations were appropriately designed and operating effectively. In addition, DOS management could not provide evidence that they had reviewed any complementary user entity controls noted in the SOC reports and ensured that they were operating effectively at PennDOT and OA. Further, DOS management did not have the vendor contracts readily available for review and referred us to other Commonwealth agencies. Finally, DOS agreements with PennDOT did not require PennDOT's contracts with their vendors to include DGS's *IT Contract Terms and Conditions* to ensure the security of the SURE system and data.

Without adequate, documented monitoring of vendor controls and security practices, DOS management cannot be assured that the vendors are properly securing the SURE system and infrastructure.

DOS management's county-level *SURE Equipment Use Policy* fails to provide clear guidance to counties.

The *SURE Equipment Use Policy* (policy) imposes requirements on county users of the SURE system for appropriate use of the IT equipment provided by DOS management.[69] Specifically, this policy requires appropriate physical security for SURE system components located at the counties. The policy describes procedures for connecting county-owned equipment to the SURE system and prohibits the following:

- Installation of software on DOS-provided equipment.
- Use of SURE network equipment for non-SURE network traffic.
- Sharing user IDs and passwords.

[68] Management Directive 325.13, *Service Organization Controls*, establishes responsibilities for the oversight and evaluation of external parties (known as service organizations) likely to be relevant to an agency's internal controls, such as vendors that operate and maintain systems key to the SURE system. The Management Directive requires agencies to obtain and review SOC reports and/or perform other monitoring activities to understand the controls each service organization maintains, as well as how each service organization's internal controls system interacts with the agency's internal control system.

[69] During the audit, we received two versions of the *SURE Equipment Use Policy* with different dates and slightly different information, one version from a county and one version from DOS management. Further, we saw on the *SURE User ID Request Form* which must be signed by new SURE users, a reference to a policy entitled, *SURE User and Equipment Policy,* which was not provided for review.

The policy fails to include the additional responsibilities for security if the county chooses to connect county-owned equipment to the SURE system. The policy also fails to require use of a form to request and approve such deviations to track and monitor nonconformities from the preferred network architectural model or the use of county-owned equipment. Requiring the use of a form to request such changes would formalize the process for these deviations and provide a system for logging and monitoring associated risks.

DOS management did not provide us with the most recent (updated in 2012) version of the policy. We were unable to determine whether new users were provided the most recent version and whether county network administrators, who are responsible for maintaining the SURE system architecture but who might not be given SURE user IDs, are required to review and sign the policy. Further, the policy was referenced on the *SURE User ID Request Form* under another name, the *SURE User and Equipment Policy*, which may cause confusion among users. Finally, there is no master list of all SURE system policies applicable to the counties and their IT vendors which clearly specifies the most recent approved versions for each policy.

It is important that DOS management provide clear guidance to counties on the use, maintenance, and configuration of equipment connected to the SURE system, and it is vital that the SURE IT management team (DOS, OA/OIT, contractors, and vendors) continue to implement leading security practices, such as those specified in the recent *Best Practices for Securing Election Systems* document issued by the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS-CISA).[70] Without adequate security over the system, the voter registration rolls may be vulnerable to fraud, manipulation, deletion, and extraction by malicious actors who intend to disrupt elections across Pennsylvania. Ensuring leading practices are implemented and consistently documented will help to ensure the integrity of the voter rolls and facilitate efficient and fair elections.

Recommendations for Finding 3

We recommend that the Secretary of the Commonwealth:

1. Consider creating an oversight body to regularly meet about the SURE system consisting of members with SURE system knowledge, relevant expertise, and the appropriate independence needed to fulfill such oversight duties. The Secretary should consider appointing members that represent all key stakeholders of the SURE system including the counties and OA/OIT.

[70] <https://www.us-cert.gov/ncas/tips/ST19-002> (accessed May 23, 3019).

We recommend that DOS management:

2. Coordinate with OA/OIT to develop a governance structure that will provide clear lines of authority in operation, maintenance, and security of the SURE system and its supporting infrastructure. This control structure should address all parties with access to and/or responsibility for the SURE system and its supporting infrastructure and should be formalized in a governance document that is formally adopted by DOS and OA/OIT.

3. Continue with plans to replace the SURE system with a more up-to-date system that includes current leading security features.

4. Implement, along with OA/OIT, the security guidelines issued by DHS-CISA in May 2019, *Best Practices for Securing Election Systems*.

5. Ensure agreements with other agencies include requirements that vendors comply with all Commonwealth security policies and that the agencies update vendor contracts to include the most recent DGS *IT Contracts Terms and Conditions* for security, confidentiality, and audit provisions.

6. Monitor vendors through a documented process that complies with Management Directive 325.13, *Service Organization Controls*, including documented reviews of SOC reports.

7. Collaborate with PennDOT and OA/OIT to identify key contacts at each agency and delivery center who would provide oversight and evaluation of each service organization's internal controls. Specific consideration should be given to the following:

    a. Timely reviewing SOC reports and documenting the assessment of the review.

    b. Reviewing SOC reports for noted exceptions that may affect DOS processes and following up with the vendor's corrective action plans.

    c. Reviewing SOC reports' complementary user entity controls to ensure those controls are in place and operating effectively at agencies and/or applicable sub-service organizations.

    d. Ensuring SOC report results are communicated to all affected agencies and escalation procedures exist when the report(s) includes control objective exceptions, testing deviations, or a qualified opinion.

8. Update the *SURE Equipment Use Policy* to address the risk of counties connecting county-owned equipment to the SURE system or deviating from the preferred architectural model.

9. Consider instituting the use of a form for counties to request and receive approval from DOS for deviations from the approved network architectural model or the use of county-owned equipment.

10. Ensure that all county users, including county administrators and vendors, review and sign an updated version of the *SURE Equipment Use Policy*.

11. Correct the reference to the *SURE User and Equipment Policy* on the *SURE User ID Request Form* to eliminate confusion as to policy requirements applicable to county users of the SURE system.

12. Create a master list of all SURE system policies applicable to the counties and their IT vendors, which clearly specifies the most recent approved versions for each policy.

Finding 4 – Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

The Help America Vote Act (HAVA) outlines minimum standards for the accuracy of voter registration records and requires states including Pennsylvania, to perform list maintenance on a regular basis to remove ineligible voters and voters who have not: (1) responded to a notice; and (2) have not voted in two consecutive general elections for Federal office.[71]

Pursuant to HAVA, each State acting through its chief state election official (for Pennsylvania this is the Department of State (DOS)), must:

> Implement a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the state.[72]

DOS' implementation and use of the Statewide Uniform Registry of Electors (SURE) system, as discussed throughout this report, is intended to fulfill this requirement. Based on our audit procedures covering the period January 1, 2016 through April 16, 2019, it appears that DOS and county election offices (counties) generally utilize the SURE system as designed. The counties perform list maintenance on voter records in order to attempt to comply with federal and state laws. We found, however, that the SURE system and supporting processes and controls (collectively Pennsylvania's voter registration process) are not effective to ensure that voter registration information is accurate. Based on federal and state law, accuracy with regard to voter registration information includes the following:

- Only eligible voters are registered to vote.
- All information fields within voters' records agree with information provided on the application form.
- All applications are timely processed to ensure information is current.
- Each voter has one unique record.

---

[71] *See* 52 U.S.C. § 21083, including Subsection (a) "Computerized statewide voter registration list requirements" and Subsection (a)(4) "Minimum standard for accuracy of State voter registration records."
A notice is correspondence mailed by a county election office to a voter requesting the voter to confirm their address. A notice is mailed due to either the individual not voting for five consecutive years or information the Department of State obtains from the United States Postal Service regarding a potential change of address for the voter. For the purpose of this audit, a "voter" is a person who is registered to vote in Pennsylvania. It does not indicate that the person has voted in an election.

[72] 52 U.S.C. § 21083(a)(1)(A).

- Each voter is assigned the correct voting status, e.g., *active versus inactive*.[73]
- All ineligible voters are removed from the registration rolls in a timely manner.

Inaccuracies presented in *Finding 2*, as well as information discussed later in this finding, demonstrate that Pennsylvania's voter registration process does not adequately ensure that the voter registration information within the SURE system is accurate.

Based on our audit procedures, we identified several reasons why inaccuracies occur within Pennsylvania's voter registration process. This finding categorizes reasons into the following two areas, noting where each reason is discussed within the report after each listed item:

- Weaknesses within the voter registration application (application) process.
- Weaknesses regarding the maintenance of voter registration records (list maintenance) within the SURE system.

Weaknesses within the application process

- No review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry. (See below)
- Automated edit checks and other features that would prevent or detect inaccuracies are not sufficiently incorporated into the SURE system. (See *Findings 2 & 5*)
- The process to search for duplicate records is predominately a manual process and is inadequate. (See *Finding 2*)
- County staff added a generic date of birth (DOB) (e.g., January 1, 1900) in the SURE system for thousands of voters when the counties migrated their data into the SURE system upon implementation between 2003 and 2005 and never corrected those dates. (See *Finding 2*)
- Applications remain in pending status for long time periods, indefinitely in some cases. (See below)
- The source documents for some voter record information have not been maintained by the counties due to a lack of clear record retention guidance. (See *Finding 6*)

Weaknesses regarding the maintenance of voter registration records within the SURE system

- Although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records. (See below)

[73] A voter in active status can vote after signing the poll book at their polling place. A voter is to be placed in inactive status if they have not voted nor had any communication with the county election office in at least five years. An inactive voter is still able to vote but will need to sign an affidavit to confirm their continued eligibility at their polling place before casting their ballot.

- Voters who should be classified as inactive or whose records should be cancelled according to state law remain in an incorrect status within the SURE system. (See below)
- The process to search for deceased voters is predominately a manual process and is inadequate. (See *Finding 2*)
- DOS does not fully utilize the list maintenance feature it pays for as a member of the Electronic Registration Information Center (ERIC).[74] (See below)

The following sections describe the weaknesses within the application process and the maintenance of voter registration records within SURE that are not presented in other findings.

Weaknesses within the application process

As part of our audit procedures, we visited seven counties to gain an understanding of how the counties process applications in SURE, including procedures for applications received electronically and for applications received in paper format. Our analysis included the procedures for both new applications and updates to voter records.

For paper applications, county staff manually enter all of the application information into SURE. Applications electronically received, either online or through the Pennsylvania Department of Transportation (PennDOT) Motor Voter system, require less manual input from staff. While there are times when county staff may need to make edits to the information, such as moving data to the correct field, generally speaking, the data entry part is completed by the applicant.[75] County staff only need to review to ensure that the required information is present, conduct duplicate voter record checks (discussed in *Finding 2*), and assign the voter to the correct precinct.

Whether the applicant submits an application in paper format or electronically through DOS' website as part of the application process, the SURE system requires county staff to run a mandated HAVA check prior to completing the registration process.[76] The HAVA check compares the applicant's information supplied on the application to either the information maintained by PennDOT or the U.S. Social Security Administration. These comparisons are only performed if the individual has provided either a Pennsylvania driver's license (DL) or Pennsylvania identification (ID) number and/or the last four digits of their Social Security number (SSN).[77] Providing this information on the application is not mandatory. If the

[74] ERIC is a non-profit corporation governed by a board of directors made up of member-states, including Pennsylvania. https://ericstates.org/who-we-are/ (accessed August 12, 2019).
[75] An example of an edit that may be required is if the house number is located in the field for the street name rather than the field for the house number.
[76] 52 U.S.C. § 21083(a)(5) "Verification of voter registration information."
[77] The HAVA check includes: checking the applicant's first two characters of last name in conjunction with the PennDOT DL or ID number and DOB, if the applicant supplied their DL or ID number. If the applicant supplied the last four digits of their SSN, the check includes: checking the applicant's last name, first name, middle initial, last

information provided on the application matches the HAVA check results, the registration is automatically approved. If any of the information provided on the application does not match and the county staff confirms that in the case of paper copy applications that there was not a data entry error, the application is placed in pending status (discussed later in this finding). At this point, a HAVA non-match letter is generated through SURE that the county mails to the applicant requesting clarification of the information provided.

No review is required to ensure that data on the application form is being accurately entered into SURE either at the time of data entry or on a routine basis after data entry.

Based on our audit procedures, neither DOS nor the SURE system itself require counties to have a second person, whether a colleague or supervisor, to double-check the accuracy of data entry performed so that typographical errors can be immediately corrected at the time the applications are processed. According to our survey results, at least 35 of the 65 counties that responded have two or fewer people in the elections office, which could make a required second person or supervisory review process difficult.[78] We understand that during peak processing times it may not be practical for counties to double-check data entry accuracy for application processing; however, this does not negate the risk that data entry errors will likely occur. Efforts should be made to mitigate this risk by routinely reviewing the data entry information as frequently as possible to detect and correct typographical errors.

Based on our discussion with DOS management, we also found that DOS does not provide guidance to counties regarding reviews of data entry information to ensure accuracy. Based on responses from the survey however, we found that some counties have implemented their own rules for reviewing data entered into SURE for applications. As part of the survey, we asked county directors if they reviewed work performed in SURE by county staff to help ensure accuracy of voter records.[79] Only 35 of the 64 counties (less than 55 percent) that responded to this particular question indicated that they review work performed by county staff in SURE. The responses regarding the frequency of reviews conducted included comments such as, "as needed," "as time allows," "monthly," "weekly," and "daily." One county indicated that its staff performs a weekly review of voter information to determine if there are any records with duplicate DL numbers, names, DOB, and addresses. In addition, the same county indicated that a monthly review is performed to determine if any records are missing party affiliation or precinct designation.

four digits of the SSN, and DOB. An applicant can indicate on their application that they do not have a DL, ID or SSN. As with all first time voters, the applicant must show one form of approved identification (see list in *Appendix C*) when voting for the first time.

[78] The information is based upon responses from the counties in the county survey performed as part of our audit procedures. See *Appendix H* for a copy of the survey sent to the counties.

[79] A total of 65 of the 67 counties provided responses to our questions either during the on-site interviews or by returning the survey; however, not all of the counties responded to every question in the survey.

Due to staff limitations in some counties, it may not be feasible for every county to conduct weekly checks; however, routine reviews and data analysis would help to identify missing and inaccurate data as well as ensure the accuracy of the voter records maintained in SURE. See *Finding 2* for details on our data analysis results that indicates thousands of potentially inaccurate voter records exist.

In addition to the counties performing periodic reviews of voter information, it would be beneficial for DOS to analyze voter information data on a statewide basis for accuracy and reasonableness. When inaccurate data is entered into SURE, other procedures designed to keep the SURE system accurate, such as the duplicate check, cannot work effectively because exact matches are less likely. Therefore, DOS and counties should be performing periodic analyses of the voter information data for missing and/or inaccurate data.

In addition to DOS and counties performing internal reviews of the data in SURE, another available option is for DOS to contract with a third-party vendor to review the data and perform an analysis. Such an analysis would be similar to that performed during our audit procedures to identify potentially inaccurate or missing data in voter records for DOS and/or counties to investigate and resolve.

Applications remain in pending status for long time periods, indefinitely in some cases.

Applications (both initial applications and applications to update existing voter record information such as name, address, political party) received by the counties that are missing required data, such as personal information, party selection, or a signature, are placed into a pending status in SURE. DOS management stated that counties are to follow-up with the applicant and request the missing information in order for the application to be processed. Additionally, if the HAVA check portion of the voter registration process results in a non-match, the application is placed into pending status while awaiting follow-up with the applicant.

According to DOS management, there is currently no criteria established requiring counties to follow-up or reject an application that remains in pending status after a certain amount of time has elapsed (this issue is further discussed in *Finding 7*). Based on data analysis, as of October 9, 2018, there were 91,495 applications in pending status, including applications from all 67 counties.[80] The following table provides a summary of the applications in pending status as of October 9, 2018, based on the age of the pending record:

[80] According to interviews with both DOS and county staff, work to clear applications from pending status occurs up through each election, which in this case was November 6, 2018. County staff therefore had approximately one month from October 9, 2018 through November 6, 2018, to further process the applications and potentially remove some from pending status.

Applications in Pending Status[81] As of October 9, 2018		
Number of Months/Years the Application had been in Pending Status	**Number of Applications**	**Percent**
0 to 30 days	25,022	27.35%
31 to 180 days	7,958	8.70%
181 to 365 days	3,738	4.09%
12 to 24 months	12,639	13.81%
24 to 33 months	18,932	20.69%
Subtotal: Number of applications placed in pending status during our audit period (January 1, 2016 forward)	**68,289**	**74.64%**
33 months to 4 years	4,498	4.92%
4 to 6 years	3,396	3.71%
6 to 8 years	3,526	3.85%
8 to 10 years	4,235	4.63%
More than 10 years	7,551	8.25%
Subtotal: Number of applications placed in pending status prior to the beginning of our audit period (January 1, 2016)	**23,206**	**25.36%**
Total	**91,495**	**100.00%**

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

As reflected in the above table, a record can remain in pending status indefinitely. More than 7,500 applications have been in pending status for more than 10 years. DOS management stated that they have asked counties to review pending applications and reject them, if appropriate. Based on the number of pending applications, it does not appear that counties have made the cancellation of older pending applications a priority.

Further, it appears that many of the applicants with records in pending status have submitted subsequent applications (either a new request to register to vote or to update their existing voter record information) which would potentially make the prior pending application moot. We found 16,000 pending records that matched a subsequent application filed by the same voter.

Based on additional analysis performed, we determined that almost 95 percent of the 68,289 applications placed into pending status during our audit period, or 64,587, were awaiting a response from the applicant in order to further process the application while approximately 5 percent required action by the county to complete processing.

[81] A list of these records has been provided to DOS to allow them to instruct the county election staff to review the records and make a determination as to whether they should be processed further or rejected.

Of the 64,587 applications that were awaiting a response from the applicant, 16,206 were pending while awaiting a response from the applicant who was sent a HAVA non-match letter. DOS management stated that there is no legal basis under federal or state law to reject or delay the processing of a voter registration application based solely on a HAVA non-match. Therefore, for these 16,206 applications, county election staff is responsible for making a determination as to whether there are grounds for rejection or if the applications should be processed for approval.

When an individual's application is placed in pending status due to the applicant not providing all required information, they are sent a letter explaining the deficiency and requesting the missing information. When an individual's application is placed in pending status because it requires action by the county to continue processing, it is possible that the applicant may be unaware that their registration has not been approved, and therefore is not eligible to vote. We believe that the number of applications in pending status would be drastically reduced if guidelines existed requiring counties to: (1) take action within a certain time period on applications that require further review or processing by the county, and (2) reject incomplete applications if the applicant does not respond to the county's inquiry within a certain timeframe. If an application must be rejected, a notice would be mailed to the applicant. This would help to ensure that the applicant is notified that they have not been registered and therefore are unable to vote. Once rejected, an individual has the ability, if they so choose, to again register to vote, which would start the process again. We believe, and DOS management agreed, that it is better for an individual to have their registration rejected than to have it remain in indefinite pending status. DOS should work with its legal office to determine whether the above-suggested guidelines can be implemented.

Weaknesses regarding the maintenance of voter registration records within the SURE system

Pennsylvania voter registration laws require the maintenance of a database containing records for all registered voters. It also requires that the database permit the sending of notices regarding death, change of address, or other information affecting the qualifications of an applicant or registration of a registered voter, and identify duplicate voter registrations on a county and statewide basis.[82] State law also requires the removal of voters and use of National Change of Address (NCOA) on a periodic basis, but not less than once every calendar year, to identify registered voters who may have changed addresses.[83] These requirements are to help ensure that voter records for individuals who are no longer eligible to vote are cancelled in a timely manner and that voter records are properly updated for those voters who have moved to a new county.

[82] Pennsylvania Voter Registration Law (PVRL) – 25 Pa.C.S. §§ 1201(3) and 1222(c). See also 25 Pa.C.S. § 1901(b) "Voter removal program."
[83] Ibid. at 25 Pa.C.S. § 1901(b).

Federal and state election law governs the election cycle in Pennsylvania.[84] Each county must complete specific tasks, such as completing list maintenance activities no later than 90 days prior to the general election in order to comply with these laws. List maintenance of the computerized list must be performed on a regular basis and must be conducted in a manner that ensures that:

- The name of each registered voter appears in the computerized list.
- Only voters who are not registered or who are not eligible to vote are removed from the computerized list.
- Duplicate names are eliminated from the computerized list.[85]

As noted in the *Introduction and Background* section, elections in Pennsylvania are a function of local elections offices. DOS, however, also has certain authority over the state's elections. The counties own the voter registration records, but federal law placed the requirement to create and maintain the SURE system with DOS. DOS must ensure that voter registration records are accurate and are updated regularly. As a result, DOS provides oversight to the counties to ensure that they complete all required tasks in accordance with the governing law, but DOS does not have any authority over the counties, which are governed by county commissioners or a county executive. There is a delicate balance between DOS and the counties. DOS needs the counties to do what they are statutorily required to do, but lacks the power to mandate compliance or to simply do the required work itself.

The following sections describe the weaknesses we found related to the maintenance of voter registration records.

Although list maintenance activities are performed by counties, insufficient analysis and monitoring has resulted in inaccurate data in the voter records.

During our review of DOS reports, analysis of SURE data, and testing performed on voter records, we saw evidence that counties had performed required list maintenance activities on voter records.[86] The annual report presented by DOS to the Pennsylvania General Assembly includes information, by county, of the number of voters affected by list maintenance activities. DOS also provided us with examples of emails between the Help Desk and DOS staff regarding county progress in conducting list maintenance, such as the number of voter records given to a

[84] Help America Vote Act (HAVA) – 52 U.S.C. § 21083(a)-(b); PVRL – 25 Pa.C.S. §§ 1201(3), 1222(c), and 1901(b)(1)(i).

[85] 52 U.S.C. § 21083, Subsection (a)(2) "Computerized list maintenance" and Subsection (B) "Conduct." Pennsylvania election law assigns the responsibility of maintaining voter records to the county election offices.

[86] List maintenance activities are prescribed by law and are performed by counties to help ensure that the voter rolls remain up to date and accurate. Such activities include an annual change of address mailing and a five year mailing to voters who have not voted in two federal general elections. *See* 25 Pa.C.S. § 1901(c) and (d).

county to follow up regarding the NCOA process and how many of those voters were sent correspondence, confirming follow-up was performed.[87]

Additionally, we analyzed the data in the application table from the SURE system to look for indications that counties performed list maintenance activities as required by federal and state law.[88] The results of our testing indicated that all 67 counties had updated voter records for list maintenance activities and, therefore, had performed some type of list maintenance during the audit period January 1, 2016 through October 9, 2018. Based on information contained in the SURE system, there were indications that all 67 counties had updated records for change of address, deceased individuals, and inactive voters. Virtually all counties' data had indications of list maintenance activities in each of 2016, 2017, and through October 9, 2018.[89] There are limitations in the data received from the SURE system that prevent a high level of assurance in the data analysis results; however, the data appeared to corroborate DOS management's statement that all counties performed required list maintenance activities annually during our audit period.[90]

Additionally, as part of our audit procedures, we visited seven counties between July 11, 2018 and September 11, 2018. The NCOA mailings (a required list maintenance activity) are typically conducted during the summer when the counties are between election cycles. During our visits we observed counties processing responses to the NCOA mailings, which further verifies that they conducted the NCOA process.

While the above scenarios appeared to corroborate DOS management's assertion that all counties perform the required list maintenance, the effectiveness of the list maintenance activities is largely based on the accuracy of the existing voter records. As explained in *Finding 2*, insufficient analysis is being performed to identify duplicate voters during the application process and to identify all deceased voters on the voter rolls. Issues also exist with the accuracy of voter records, including missing or incorrect birthdates, duplicate records, and potentially deceased voters that remain on the voter rolls. As the list maintenance process is dependent upon

[87] The NCOA includes mailing a notice to each voter that was identified as having possibly moved in the last year. The data is provided to DOS by ERIC.

[88] The application table contains the history of all additions and changes made to voter registration records since the implementation of the SURE system in 2003 through 2005. Each change to a voter registration record is captured as a record in the application table. *See* 52 U.S.C. § 21083(a)(2) "Computerized list maintenance" and 25 Pa.C.S. § 1901(b) "Voter removal program."

[89] The application table data for one small county that contained only four list maintenance records in 2017 contained no list maintenance records in 2016. We deemed the level of list maintenance activity reasonable for that small county. The data also included no indication of list maintenance performed by one other county during approximately the first nine months of 2018 (January 1, 2018 through October 9, 2018, the date our data was extracted by DOS), but there was still time for that county to complete its list maintenance activities by the end of calendar 2018.

[90] We determined that the reliability of this data had significant limitations regarding completeness and accuracy as noted in *Appendix A*. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

accurate voter record data in order to identify individuals, until the inaccurate voter record information is corrected, the list maintenance activities will only be marginally effective.

DOS management stated that it regularly monitors the work performed by counties; however, it does not have standard operating procedures formalizing the monitoring conducted, nor does it monitor whether the work by the counties is adequately performed.[91] DOS management stated that there are multiple DOS staff members who regularly receive emails from the Help Desk that update them on the status of work performed in SURE by each county. DOS management provided us with examples that included daily automated emails indicating if list maintenance processes have been completed, what counties have certified their voter registration statistics, and what counties have started/completed printing their poll books for an election. There are no written procedures, however, to document the frequency and which staff members are ultimately responsible for monitoring the various types of work performed by the counties. Additionally, DOS staff does not maintain a centralized document to track the status of work performed by each county. As a result of DOS staff not maintaining a centralized document, DOS is unable to document the work done to track the status of the counties' work in order to determine if there are any county election offices that need to be notified/reminded of required work necessary to meet established deadlines or confirm that all required tasks have been completed by each county. Therefore, we could not confirm that DOS regularly monitored each county for required tasks.

It is imperative that standard operating procedures be formalized to ensure that there is clear direction on when and what monitoring is to be performed of the counties, as well as who at DOS is responsible for performing the monitoring. Both DOS and counties must work together to ensure that all processes are completed in a timely manner so that all eligible persons who have applied to register to vote are allowed to vote.

Voters who should be classified as inactive or whose records should be cancelled according to state law remain in an incorrect status within the SURE system.

State law requires that voters without any activity for five years be placed in inactive status.[92] In order to test that all counties were performing list maintenance activities to identify inactive voters, we performed data analysis to look for voters who should have been changed to inactive status based on the required criteria. We identified 96,830 active registered voters who had no activity in the past five years (e.g., they did not vote, did not change their address, did not change

[91] Examples of county work that DOS monitors includes ensuring applications are being processed, list maintenance is being performed, poll books are printed timely prior to an election, and that voter registration statistics are certified.

[92] As defined in **Pennsylvania Voter Registration** Law (PVRL) (Act 3 of 2002), 25 Pa.C.S. § 1901(c), registered voters are to be identified as inactive when they have not responded to a mailed notice from the county based on information received by either DOS or the county that a registered voter has moved. Additionally, the law indicates that registered voters should be identified as inactive when they have not responded to a mailed notice from the county when they have not voted within the last five years.

political party, etc.). These voter records likely should have been placed into inactive status by counties when performing required list maintenance procedures unless there was some form of communication between the county and voter that was not included in the data we analyzed. As reported in the following table, almost 44 percent of the total 96,830 stale, but still active, voter records were voters registered in Allegheny County:[93]

Active Registered Voters as of October 9, 2018 with no Activity During the Period October 9, 2013 through October 9, 2018 (Five Years with no Activity) by County		
County[a/]	**Number of Voters**	**Percentage of Total Voters**
Allegheny	42,437	43.83%
Cumberland	13,215	13.65%
Luzerne	7,395	7.64%
Northumberland	6,164	6.36%
Philadelphia	6,280	6.48%
48 counties	21,339	22.04%
Total	**96,830**	**100.00%**

[a/] - Our analysis did not find any stale voters in 14 of the 67 Pennsylvania counties.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Further, we used the "date last voted" field, in part, for this analysis. As noted in Appendix A, this field is of undetermined reliability. Although these determinations may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

The law also requires that voters who have already been placed into inactive status and who fail to vote in the following two federal general elections should have their voter record cancelled.[94] Using our data analysis procedures, we found that 17 of the 67 counties had a total of 65,533 records of inactive registered voters who had not voted since the 2008 federal general election and therefore should have been cancelled, but remained registered in inactive status as of October 9, 2018. The following table provides detail regarding the four counties that account for 60 percent of these inactive registered voters and the amount of voters from the remaining 13 counties:

[93] For purposes of this finding, we consider a stale voter record to be voters that we identified as being in active status in spite of meeting the criteria to be moved to inactive status.
[94] PVRL (Act 3 of 2002), 25 Pa.C.S. § 1901(d)(1)(ii)(B).

Registered Voters who had been Inactive from 2003 through 2008 and who had Not Voted since the 2008 Federal Election but who had Not Been Cancelled as of October 9, 2018, by County		
County	**Voters**	**Percentage of Total Voters**
York	13,520	20.63%
Erie	9,873	15.07%
Allegheny	9,098	13.88%
Westmoreland	7,404	11.30%
13 other counties	25,638	39.12%
Total	**65,533**	**100.00%**

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the SURE system. We determined that the reliability of this data had significant limitations in regards to completeness and accuracy as noted in Appendix A. Further, we used the "date last voted" field for this analysis. As noted in Appendix A, this field is of undetermined reliability. Although these determinations may affect the precision of the numbers we present, there is sufficient evidence in total to support our findings and conclusions.

Possible reasons for the counties' failure to move stale voters who meet the applicable criteria to inactive status or to cancel inactive voters' records could vary from simple oversight to not being able to complete list maintenance activities due to several special elections.[95] We did not conduct interviews with representatives from each county, and therefore did not determine the actual reasons. In failing to properly classify active voters as inactive and subsequently removing inactive voters from the voter rolls after the established time periods, counties are not complying with state law and are increasing the risk of fraudulent voting. In addition, since current controls to identify and remove deceased voters' records (discussed in *Finding 2*) appear to not be functioning in all cases, removal of inactive voters' records becomes more important as a safeguard against deceased individuals' voting records remaining active. In addition to these concerns, inaccurate voter rolls could also affect other voting related aspects, such as the size of an election district, which should not contain more than 1,200 registered voters, and the amount of funding for elections, including funding for voting machines, which is based on the number of eligible voters by county.[96]

As discussed throughout the finding, inaccurate information associated with a voter's record can inhibit a county's ability to keep their rolls up to date. As previously mentioned, list maintenance depends on the ability to match information provided for individuals to voter registration records. If information in a voter registration record is inaccurate, county election staff may erroneously disregard the information as not being a match to an existing voter record, which allows

[95] A special election is scheduled by the General Assembly in order to fill a vacancy due to the current elected official no longer being able to hold office such as due to death or retirement. Pursuant to the National Voter Registration Act (NVRA), 52 U.S.C. § 20507(c)(2)(A), and the PVRL (Act 3 of 2002), 25 Pa.C.S. § 1901(b)(4), a voter's record cannot be cancelled due to list maintenance within 90 days of an election.

[96] Pennsylvania Election Code Act of June 3, 1937, P.L. 1333, No. 320 Article V, § 502 "Court to Create New Election." *See* 25 P.S. § 2702, as amended. https://www.legis.state.pa.us/WU01/LI/LI/US/PDF/1937/0/0320..PDF (accessed June 7, 2019). Letter from DOS to the U.S. Election Assistance Commission with their narrative of how they will distribute the HAVA money. https://www.eac.gov/havadocuments/PA_narrative_Budget.pdf (accessed June 10, 2019).

duplicate voters to be included in the voter rolls. Inaccurate information can also result in a failure to cancel an ineligible voter's record, such as a voter who has died. Beyond the fact that the law requires that the voter rolls be maintained to include accurate information, accurate, up-to-date voter rolls are helpful to the voters by minimizing disruption at the polling places due to inaccurate information in the poll books.

DOS does not fully utilize the list maintenance feature it pays for as a member of ERIC.

As previously described, it is critical that accurate voter records be maintained. Organizations such as ERIC have been established to help improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens.[97] From the launch of ERIC in 2012 through the end of 2017, ERIC helped its member states identify 8.4 million inaccurate voter records.[98] ERIC provides its member states with reports on voters who have moved in-state or out-of-state, voters who have died, voters with duplicate registrations in the same state, and individuals who are potentially eligible to vote but are not registered. According to DOS management, however, it only uses ERIC to obtain information for list maintenance purposes regarding change of address and is not utilizing available information such as death notices and cross-state matches.[99] We inquired of DOS management as to why they are not fully utilizing all of the features available through ERIC. DOS management responded that they "have plans to incorporate them into production prior to the November 2019 election." This is despite the fact that DOS has paid for but not utilized some of the information available to ERIC members since it first joined in 2015.[100]

Conclusion

Issues with the input of voter record data and the lack of fully performing list maintenance has resulted in inaccurate information being maintained in SURE. Additionally, by not updating voters' information and not removing ineligible voters from the voter rolls, counties are not complying with required state and federal laws. Finally, DOS is not utilizing benefits that it is paying for as a member of ERIC to aid counties with list maintenance procedures.

[97] ERIC 2017 Annual Report. https://ericstates.org/wp-content/uploads/2019/01/FINAL_ERIC_2017_Annual_Report.pdf (accessed March 25, 2019).
[98] Ibid. Pennsylvania, through DOS is one of 26 states, plus the District of Columbia that is a member of ERIC.
[99] Cross-state matches involve matching Pennsylvania voter records to out-of-state voter registration commissions and Department of Motor Vehicle records that indicate updated information.
[100] According to ERIC's web-site, each member pays a one-time membership fee of $25,000 and an annual fee. https://ericstates.org/wp-content/uploads/2019/01/ERIC_Bylaws_2018-11-30.pdf (accessed August 5, 2019).

Recommendations for Finding 4

We recommend that DOS:

1. Emphasize to the counties the vital need and importance of having a second person review the data entered into SURE to reduce data entry errors and increase the accuracy of voter records.

2. Consider supplementing the data analysis that we recommend DOS perform in *Finding 2* (Recommendation 2), by contracting with a third-party vendor to periodically perform analysis on the data in SURE to identify potentially inaccurate or missing data for DOS and/or counties to investigate and resolve.

3. Request that its designated legal counsel make a determination as to whether DOS can: (1) direct the counties to review their pending applications and reject them; and (2) establish a time period for requiring counties to process, or reject if applicable, all applications placed into pending status.

4. Instruct the counties to review the applications in pending status to determine if another application for the person has been approved which would then lead the county to reject the initial application currently in pending status.

5. Develop detailed written procedures, including detailed processes to be performed and by whom, regarding DOS monitoring the activities of the counties to ensure required processes are completed properly and timely.

6. Instruct the counties that have not been updating the status of voters from active to inactive, for those voters who meet the criteria of an inactive voter, to perform list maintenance and update voters' status as necessary. This instruction should include a deadline to be established by DOS. Additionally, formally remind all counties of the importance of why they need to perform this type of list maintenance.

7. Instruct the counties that have not been cancelling the records of the inactive voters who meet the criteria for cancellation to perform list maintenance and update voters' status as necessary. This instruction should include a deadline to be established by DOS. Additionally, formally remind all counties of the importance of why they need to perform this type of list maintenance.

8. Move forward with plans to utilize all information available from ERIC to assist in improving the accuracy of voter registration records.

Finding 5 – Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Accurate voter information within voter registration systems is critical for two important reasons: (1) to ensure that only the voter registration applications (application) of individuals eligible to vote are approved and (2) only eligible voters are casting votes in elections. Because the Statewide Uniform Registry of Electors (SURE) system has been in place for more than 15 years, Pennsylvania Department of State (DOS) management stated that it has engaged the SURE Advisory Board to start discussing a replacement system. Additionally, DOS has started to develop the requirements and a timeline for the request for proposal process to replace the current SURE system. According to DOS management, the replacement system will be customized to meet the specific needs of Pennsylvania. As a result, the audit objectives included reviewing efficiencies of the SURE system that DOS should consider in the design of the replacement system to improve the processing of applications and improve accuracy.

As discussed in *Finding 4*, DOS does not require supervisors at county election offices (counties) to verify the accuracy of the application information manually entered into SURE by county staff. According to the survey we conducted, we found that less than 55 percent of the counties that responded to the survey perform any procedures to verify whether the application data was entered accurately.[101] In addition to manually verifying data entry accuracy, there are several information system input controls that could be utilized to increase the accuracy of the information entered into SURE. For example, edit checks for reasonableness, validity, and completeness tests can be programmed into the system to ensure certain data entry mistakes are detected/flagged by the system upon entry, which could then be immediately corrected by county staff at the time of data entry.[102]

Through our data analysis, we found instances where edit checks were lacking or non-existent. The following issues were previously discussed in *Finding 2*:

- The automated check for duplicate voter records within the SURE system at the time of application approval is inadequate.

[101] As part of our audit procedures, we sent a survey to all 67 Pennsylvania counties. 65 of the 67 counties provided responses to our questions either during on-site interviews or by returning the survey, however not all of the counties responded to every question in the survey. See *Appendix H* for a copy of the survey.

[102] An edit check is a type of data validation routine built into a system that is designed to ensure data input into the system meets certain criteria prior to being accepted into the database. There are a number of validation types that can be used to check the data being entered such as spell checks, presence checks (checks to make sure data is present in all required fields), or length checks (checks to make sure data is not too long or too short). Edit checks that could be used on voter application data could be a validation routine ensuring the voter will be at least 18 years of age by the date of the next election and ensuring the date of birth field includes only numbers and not letters.

- There are no automated edit checks in the SURE system that prevent adding a voter registration record with a driver's license (DL) number that is already associated with a voter record.
- There are no automated processes in the SURE system to prevent the recording of obviously inaccurate birthdates and/or voter registration dates, e.g., voter registration dates prior to date of birth (DOB).

We also found features that were missing or inadequate within the SURE system which could reduce or prevent errors. Specifically, we found:

- The SURE system does not prevent applications with non-Pennsylvania residential addresses from being approved.
- The SURE system lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing.
- The SURE system lacks a "Read Only" feature for voter information that should not be edited without additional supervisory review and approval.
- The SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

In addition to these features, we were informed of two areas related to the Pennsylvania Department of Transportation (PennDOT) Motor Voter process and the reporting capabilities within the SURE system that need improvement:

1) Some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote.
2) The ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

It is clear that the SURE system itself needs to be improved, and there is a need for the counties to strengthen their oversight of the SURE system transactions and the accuracy of the data. DOS should conduct periodic reviews of the data to identify errors, inaccuracies, and omissions and instruct the appropriate counties to fix the identified issues. Incorrect data within SURE could lead to an individual being able to vote more than once in an election or for eligible voters to encounter difficulties, such as not being included in the poll books.[103]

The following sections describe these missing or inadequate features and areas that can be improved.

[103] 25 P.S. § 3535 (Repeat voting at elections).

Features that were missing or inadequate within the SURE system which could reduce or prevent errors

The SURE system does not prevent applications with non-Pennsylvania residential addresses from being approved.

County election staff (staff) are able to enter a voter's "residence address" in SURE that includes zip codes and states that are outside of Pennsylvania. The SURE system provides fields for both a "residence address" which should be in Pennsylvania because residency is a requirement for voting, and a "mailing address" which may differ from the individual's residence and does not have to be within Pennsylvania (e.g., address for a Pennsylvania student attending an out-of-state college). The SURE system does not issue a warning message that would prompt staff to review and either reject the application or correct the inaccuracy.

As part of our data analysis, we found that of the 8,567,700 eligible voters as of October 9, 2018, the residence address in SURE for 27 voters' records contained a state other than Pennsylvania, and in some cases a zip code outside of Pennsylvania. Using auditor judgement we further researched 13 of the 27 voters using Google Maps and found that for nine of 13 records, the streets, cities, and zip codes in the residence addresses of these records appeared to be within Pennsylvania; however, the state was incorrectly entered as a state outside of Pennsylvania. Therefore, the voter appeared to be eligible to vote from review of the record. Two of the 13 records were entered in SURE as Taneytown, Maryland and the address in Google Maps verified that the address was in Taneytown, Maryland. Two of the 13 records were entered in SURE as Tallahassee, Florida, and the residence street address was blank. Therefore, for four of the 13 records, (two in Maryland and two in Florida) it appears that the voters should not have been eligible to vote based on the information in SURE. Implementing a data validation edit check to ensure the residence address is within Pennsylvania could prevent data entry errors and inaccurate records. It could also help to prevent applications for ineligible voters from being approved.

The SURE system lacks geographical mapping assistance which would reduce inefficiencies and potential inaccuracies by preventing applications from being sent to the wrong county for processing.

According to DOS and county management, the SURE system does not have the capability to utilize a geographic information system (GIS) which provides mapping assistance. The GIS could be used to identify and verify information such as the county of residence, based on the zip code entered by the applicant. This technology could prevent applications from being sent to the wrong county for processing.

During our visits to seven counties, we were informed that if an applicant lists an incorrect county when electronically completing an application or when utilizing the voter registration services offered at PennDOT's photo license centers, the application will be sent to the wrong

county for processing. Once a county receives an application (either electronically or on paper) from an individual that does not reside in that county, staff may need to conduct research in order to forward the application on to the correct county. This process is inefficient and potentially delays the processing of the application.

The SURE system lacks a "Read Only" feature for voter information that should not be edited without additional supervisory review and approval.

It may be necessary at times to edit information in a voter's record, such as a change of address or last name. There is certain personal information, however, that generally does not change, such as DOB, DL number, and Social Security number (SSN). Therefore, the information included in those fields should be made "Read Only" in the SURE system, with the ability to edit such information reserved for a higher level and only after careful review. This should be coupled with proper documentation of who made the change and why.

Currently all fields, including DOB, DL number, or SSN in SURE can be edited by county staff. DOS management and Help Desk staff stated that Help Desk staff also have the ability to make changes to a county's voter records once the county electronically gives permission and provides the Help Desk staff with access for remote control of their computer. Based on our data analysis, we found instances where it appears that DOBs had been changed to a date after the registration date. For example, the DOB in one voter record was changed on April 18, 2018 from July 4, 1952 to July 4, 2016. This is clearly an error. Implementation of "Read Only" fields would preclude staff from inadvertently editing information that should not change.

The SURE system does not have controls in place to ensure that voter registrations are not improperly cancelled within 90 days of an election.

Although performing list maintenance is required by law, counties may not cancel a voter's registration within 90 days of an election due to list maintenance activities.[104] A voter may cancel their own registration at any time, but a county may not take action to remove a voter from the active rolls based on list maintenance activities so close to an election. This helps to ensure that a voter has time to receive the notification of cancellation and take action to re-activate their voting registration in time to cast a ballot on Election Day.

Our data analysis, however, indicated that counties had cancelled voter registrations within 90 days of the 2016 federal election using cancellation codes which may indicate the voters registrations were cancelled in violation of the law. We found 155 voter registrations were cancelled within 90 days of the 2016 General Election using codes that either did not indicate the reason for the cancellation or indicated that it was due to list maintenance activities.

[104] National Voter Registration Act (NVRA), 52 U.S.C. § 20507(c)(2)(A), and the Pennsylvania voter registration law (Act 3 of 2002), 25 Pa.C.S. § 1901(b)(4).

While the number of voter registrations potentially cancelled inappropriately within 90 days of the 2016 Federal General Election may appear relatively small in number, these voters' names would not have appeared in the poll book at their precinct. Therefore, if these voters had tried to vote in that election, they would have been required to vote on a provisional ballot, which takes more time for a county to process.[105] Further, voting via provisional ballot takes more of the voter's time at the polls. Voters who are rushed to vote before work or during their lunch hour may not wait to complete the provisional voting process.

Based on the results of this data analysis, we have concluded that the SURE system does not have safeguards that would prevent counties from inappropriately cancelling voter registrations within 90 days of an election. If the SURE system included hard stops to prevent county staff from cancelling voter registrations using unallowable codes or without entering a code within 90 days of an election, DOS and counties would have more assurance that cancellations made within the restricted period were for valid reasons and not in violation of the law.

Two areas of improvement related to the PennDOT Motor Voter process and the reporting capabilities within the SURE system

Some individuals confuse the change of address prompt at PennDOT's photo license centers with registering to vote.

During interviews and in response to our survey, county election officials informed us of an issue that occurs when an individual is utilizing the change of address services at PennDOT photo license centers. The scenario described is that one of the questions asked during the process is whether the individual would like to update their address for purposes of voter registration. Officials stated that some individuals believe that by completing this portion of the process, they are registering to vote; however, this is not the case. When the change of address information is received by the county, the county searches in SURE for the individual. If they are not currently registered, the change of address information will be declined; however, there is no denial notice generated and sent to the individual that requested the change of address.

County staff are unable to process the information as a new application because not all of the necessary information has been obtained from the individual (e.g., party selection and signature to affirm that the individual is eligible to register to vote). Since the individual is not notified that their request could not be processed because there was no existing record, they may believe that they registered to vote through this action at the PennDOT photo license center. This confusion could be avoided if the individual was notified that their information was declined or if the process at PennDOT's photo license centers was changed to include all the information required to register to vote.

[105] A provisional ballot is used to record a vote when there is a question regarding a voter's eligibility. Within seven days after the election, the County Board of Elections examines provisional ballots to determine if they are valid.

The ability to create reports in the SURE system is too limited and it lacks editable report capabilities.

Both DOS management and Help Desk staff indicated that the way the SURE system is designed, the reports that DOS and counties can run are limited and some of the reports cannot be customized to provide certain detail that would be useful.

Although DOS and counties are limited in their ability to run reports, there are various reports that the Help Desk staff has the ability to run for them regarding areas such as data analysis (e.g., the number of applications processed during a certain time period for a specific county or counties) and voter record list maintenance.

As DOS seeks to obtain a replacement for the SURE system, it is recommended that the new system provide the ability for both DOS and the counties to customize and run reports regarding SURE data directly from the new SURE system themselves rather than having to request the Help Desk to prepare the reports for them. In doing so, the counties could better analyze and review records internally to improve on the accuracy of the records maintained.

Recommendations for Finding 5

We recommend that DOS:

1. Incorporate the following information technology enhancements into its design of the replacement SURE system and consider the feasibility of making some or all of these enhancements into the current SURE system:

    a. A Geographic Information System (GIS) feature and related enhancements that would check addresses to ensure the address is within the county identified on the application. This would help to ensure that electronic applications are forwarded to the correct county for processing and in the case of paper applications, county staff are immediately alerted if the address they are posting to SURE is not within the county listed on the application.

    b. An edit check that would alert or prevent county staff from approving applications that have non-Pennsylvania states and/or zip codes within their residential addresses.

    c. A “Read Only” feature for certain data fields that should not change, such as DOB, DL number, and SSN to prevent unintended edits, but enable these “Read Only” fields to be edited by designated management staff along with documenting the reason for the edit.

d. A hard-stop feature in the SURE system that would prevent county staff from cancelling voter records using unallowable codes within 90 days of an election.

e. A declination notice to be automatically generated and mailed to individuals that are not currently registered to vote but submit a change of address request for their voter registration record. This will assist in notifying those individuals that they are not registered to vote.

f. The ability for DOS and county staff to build and run their own reports, rather than having to obtain reports from the Help Desk.

2. Forward information for the four voting records that contained non-Pennsylvania residential information to the applicable counties for follow up and possible cancellation.

3. Forward information for the 23 voting records that appeared to contain inaccurate non-Pennsylvania residential data to the specific counties to research and/or correct the state name or zip code within SURE.

4. Formally remind counties of the need to properly code transactions when they cancel voter registrations as a result of list maintenance in order to reduce the number of cancellations with no reason code or incorrect reason codes.

5. Consider working with PennDOT to revise the Motor Voter process so that all required voter registration information is obtained when an individual (who may incorrectly believe they are registered to vote) requests to update their voter registration address. This will ensure that a complete application is transmitted to the respective county for further processing.

Finding 6 – A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

One objective of this audit was to assess whether the voter records maintained within the Statewide Uniform Registry of Electors (SURE) system are accurate. Before we focus on this specific objective, we note that we have already identified the following in other findings of this report:

- Several weaknesses in Pennsylvania's voter registration process. (See *Finding 4*)
- Thousands of potential duplicate and inaccurate voter records based on our data analysis. (See *Finding 2*)

Those results do not allow us to project accuracy over the entire population of voter records. Therefore, as part of our audit procedures, we selected a random statistical sample of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018.[106] Our intent was to review source documents to confirm the accuracy of the information maintained in the 196 voter records and thus conclude as to the accuracy of the entire voter population. We could not however, verify the accuracy for 138 of the 196 records selected (or 70 percent) because source documents were either not available or were not provided as further described in detail below. Source documents include the signed voter registration applications (applications) or other documents provided by the individuals to update their voter record, such as a signed affidavit completed by an inactive voter at the polling place or a returned National Change Of Address (NCOA) mailing from the voter.[107] Specifically, we planned to verify the accuracy of the following SURE system data fields by comparing the information to source documents:

---

[106] Statistical sampling means to select a limited number of items from the population on a systematic or random basis, review/test those items, and then draw a conclusion about the entire population based on the results of the items selected for testing with a statistically measurable degree of confidence considering the accepted percent rate of tolerable error. See the *AICPA Audit and Accounting Guide* "Audit Sampling" for additional details. Our statistical sample of 196 voters was determined based on a confidence level of 98 percent and a tolerable error rate of 2 percent.
For the purpose of this audit, a "voter" is a person who is registered to vote in Pennsylvania. It does not indicate that the person has voted in an election.

[107] A person applying to register to vote is required to affirm that they are: (1) a citizen of the United States; (2) a resident of Pennsylvania and the election district in which they want to register for at least 30 days prior to the next elections; and (3) at least 18 years of age on or before the next election. When a person signs their application, they are affirming their eligibility, which includes citizenship. We did not however test citizenship because citizenship information is not maintained in the SURE system. See <https://www.pavoterservices.pa.gov/Pages/VoterRegistrationApplication.aspx>.
When a U.S. citizen submits a change-of-address form to the post office, their new address is recorded in the NCOA database. <https://www.edq.com/glossary/ncoa/> (accessed August 6, 2019). For voter registration purposes,

- Full name (first, last, and middle name or initial, if included)
- Address
- Date of Birth (DOB)
- Last four digits of the Social Security number (SSN) (if included)
- Last four digits of the Pennsylvania driver's license (DL) number or Pennsylvania identification (ID) number (if included)
- Date registered
- Party affiliation

We also planned to verify that each record had a signature image in the SURE system.

Sample selection and results.

There are three methods in which an individual can complete an application:

(1) By manually completing a paper copy of the application and it being sent to a county election office.
(2) Through the Motor Voter process which is part of the DL/ID renewal process at the Pennsylvania Department of Transportation (PennDOT).[108]
(3) Through an online application made available by the Pennsylvania Department of State (DOS).[109]

Pennsylvania (through the individual counties) conducts an annual NCOA mailing using data obtained from the Electronic Registration Information Center (ERIC) to attempt to update the information in SURE by reaching out to voters who may have moved.

[108] The Motor Voter system is the system used by PennDOT to allow a PennDOT customer the opportunity to register to vote, or to update their voter registration at the same time as they have their picture taken for their DL or ID. The Motor Voter system communicates with SURE to transmit the voter registration information from PennDOT to DOS to be parsed out to the counties.

[109] The online method includes those voters that registered either through the application available on DOS' website currently available at <https://www.pavoterservices.pa.gov/pages/VoterRegistrationApplication.aspx> or those that registered through a state agency with online services available to them. See *Appendix C* for a list of agencies through which a person can register to vote.

The following table summarizes the sample of 196 voter records and related test results:

Voter Record Test Results				
Method of Application Source	**Number of Voter Records in our Sample**	**Number of Voter Records Tested**	**Number of Voter Records that Could not be Tested**	**Reason why the Voter Records Could not be Tested**
Paper Application	84	58	26	Inadequate record retention guidance. Four counties did not respond to our request for source documents.
Motor Voter	93	0	93	PennDOT would not provide Motor Voter source documents.
Online Application	19	0	19	DOS does not maintain source documents.
Total	**196**	**58**	**138**	

Additionally, we verified that the voter record in SURE included a signature for all 196 voter records in our sample.

With regard to the table above, for the 58 voter records (30 percent) we tested, we found that the information within each of the data fields matched information contained in the source document. Therefore, we have concluded that these 58 records are accurate. Additionally, for the 138 voter records (70 percent) not tested, we could not compare the information within the data fields for these records to source documents because source documents were either not available or were not provided. As a result, we could not reach a conclusion as to whether these 138 voter records were accurate. Because of this, we could not conclude on our statistical sample, and therefore could not project our results and ultimately conclude on the overall accuracy of the voter record information maintained in the SURE system.

The remainder of this finding discusses the reasons why the 138 voter records could not be tested.

DOS has not provided adequate record retention guidance to the counties.

As noted in the above table, we could not test 26 of the 84 paper applications included in our sample. Of those 26 paper applications, 14 could not be tested because 12 counties acknowledged that they were unable to locate the source documents needed to test each record for accuracy. Further, although the SURE system has the capability of retaining scanned document images, we verified that these 14 paper applications were not scanned and attached to the respective voter record.

We analyzed the registration dates listed in SURE for these 14 paper applications and noted the following:

- Three voters registered between 2004 and 2018 (after the implementation of the SURE system)
- Eleven voters registered between 1959 and 2000 (before the implementation of the SURE system)

Based on the range of registration dates, for the auditors or other external parties to verify the accuracy of voter records for these 14 voters, the source documents (applications) would have had to be maintained by the counties for up to 60 years. In reality, the time period could be longer than 60 years for voters registering prior to the 1959 date noted in the above bullet, given that a person may not need to change voter information after initially registering.
With this information in mind, we wanted to determine the following:

1. How long does each county keep source documents, if at all?
2. What record retention guidance exists?

How long does each county keep source documents, if at all?

As part of our county survey and county visits, we asked counties two related questions. The first question was whether the county currently scans and saves the full voter registration application and attaches it to the voter's electronic record in SURE.[110] Of the 65 counties that responded, 50 replied that they scan and retain an electronic copy of the application, and 15 responded that they do not scan and retain the application.

The second related question in the survey asked whether the counties retained the hard copy applications, regardless of whether or not they scanned the documents into SURE. Of the 65 counties that responded, 58 stated they do retain the hard copy applications; however, their responses varied greatly as to their retention period including:

- Length of time required by law.
- Two years.
- As long as the voter is active/registered.
- Five years after the voter's record is cancelled.
- Indefinitely/lifetime/until the voter moves or dies.

[110] Surveys were sent to all 67 counties, including the seven counties that we visited in person and in which we conducted interviews which included the questions on the survey. Five counties did not respond to the survey; however, three of those five counties were offices that we visited. For reporting purposes, we will report in total the responses received from county staff in both the survey and during county visits. It is also important to note that the surveys were completed by the then-current county election office manager/director who may or may not have been in that position since the implementation of the SURE system.

The counties' answers to the survey relate to how the counties retain applications at the time of the survey. These answers do not necessarily reflect how the counties had been retaining applications since the inception of the SURE system nor how the counties had been keeping records for the past 60 years or longer. They are a momentary snapshot of retention practices but do not establish any longstanding policies or protocols, certainly nothing that would constitute uniformity across the Commonwealth. As a result, we found during our testing that although many of the counties indicated in the survey that they scan applications, certain counties could not provide some of the applications, which may be due to the record retention policies of the counties or a difference in policy from the current election director to the former directors in the same county.

What record retention guidance exists?

Based on the results of the survey, it appears that DOS has not adequately or clearly advised the counties regarding requirements for the method of retaining applications or how long applications should be retained. DOS does not require counties to scan and attach the application to the voter record even though the SURE system has that capability. Failure to require scanning and retaining of applications causes significant non-uniformity among counties as seen by the survey results above.

As a result of the varied responses from the counties, we inquired with DOS as to what record retention policy counties must follow as it relates to the retention of applications. The policy provided to us by DOS notes that an application "must be retained for ***22 months*** from the date of any general, special, or primary election for federal office."[111] It does not, however, clarify whether the application must be retained in hard copy or if a scanned image attached to the voter's record in SURE is considered in compliance with the retention policy.

Additionally, this retention policy is not consistent with the SURE regulations establishing the SURE system which provides that: "[a] commission shall maintain the records that a commission attached to a registrant's record in accordance with § 183.4(c)(1) (relating to uniform procedures for the commissions relating to entering data into the SURE system) for 90 days after the registrant votes in any primary or election."[112] Therefore, counties are to maintain all applications received for ***90 days*** after any primary or election. These regulations have not been updated since they were initially promulgated in 2002.

Neither the *County Records Manual* nor the SURE regulations (which are different and inconsistent) provide counties record retention guidance that would allow an auditor or other external party to independently assess the accuracy of the voter registration records maintained

[111] *County Records Manual* issued by the Pennsylvania Historical and Museum Commission <https://www.phmc.pa.gov/Archives/Records-Management/Documents/RM-2002-County-Records-Manual-2017-Update.pdf> ELECTION – 1 (listed as having been last updated on **9/2012**) (accessed April 30, 2019). Please note that this manual has inconsistent revision dates within the document.
[112] 4 Pa. Code § 183.12(d)(1).

in SURE. Further, based on the counties' responses, it appears that the counties may not be aware of the retention policy in the *County Records Manual* nor the SURE regulations. As a result, it appears that county election officials determine the record retention policy. The problem is further compounded during turnover of county election officials.

A clear record retention policy from DOS and a requirement to scan all applications into SURE would help to ensure uniformity among all counties, ensure complete records, provide a SURE user with the ability to answer questions if/when they arise from either voters or county staff, and allow for documents to be audited, as necessary.

Four counties did not respond to our requests for source documents.

As noted in the above table, we could not test 26 of the 84 paper applications (over thirty percent) included in our sample. Of those 26 paper applications, 12 could not be tested because these documents were not scanned and retained in SURE, nor did the respective counties respond to our requests to provide us the 12 source documents. Overall, we requested these documents at least three times through DOS, but the counties never responded. These four counties were Allegheny, Bucks, Warren, and York.

By failing to respond, we do not know whether or not these counties actually possess the documents in paper copy. As noted above, inadequate record retention guidance may have been a factor. Therefore, the inability to review the documents impeded our ability to complete the audit objective resulting in a scope limitation. See *Finding 1* for further information. Not responding, however, gives the appearance that these counties were not cooperative with the auditors.

PennDOT refused to provide access to Motor Voter source documents.

On December 10, 2018, we requested through DOS that PennDOT provide us with access to review records for our selected sample of voters that support the voter registration information submitted by voters through Motor Voter. Specifically, we wanted to confirm the accuracy of the information maintained in SURE to the voter registration information collected by PennDOT and transferred to DOS. To accomplish this, we requested that PennDOT staff permit us to review with them (in an "over the shoulder" observation) the Motor Voter information for our selected sample records on their system. This method would ensure that our review of any documents deemed sensitive would be done in the presence of a PennDOT employee. This is a common practice that is applied to numerous audits and is generally well-accepted. Utilizing this supervised method of review would avoid the possibility of the auditors inadvertently obtaining documents containing personally identifiable information from PennDOT. In fact, it was consistently communicated to both DOS and PennDOT that the auditors prefer not to review personally identifiable information.

As a result of this request, we met with PennDOT management and legal counsel on January 7, 2019, to explain our request and to answer any questions they had. We also explained that failing to provide the information would preclude us from being able to conclude on the accuracy of the voter registration records in SURE. PennDOT indicated that the information we were requesting to see was not easily retrievable and the timing of it was not good due to their REAL ID Act program which would be starting in March 2019. PennDOT indicated however, that they would consider our request.[113]

We sent requests for this and additional information ***a total of seven times***; however, we did not receive any information from PennDOT until April 17, 2019, which was after our audit procedures closing date of April 16, 2019. In lieu of allowing us to perform the "over the shoulder" procedure, PennDOT provided us with limited documentation, but this did not contain all the Motor Voter information we needed to complete our accuracy test. Therefore, we were unable to verify the accuracy of the voter record information in SURE that was received via the Motor Voter system. The failure to fully cooperate is considered a scope limitation and significantly affected the auditors' ability to reach conclusions on the stated objective, which in turn minimized the overall value of the original objectives agreed upon by DOS. Despite these limitations, we sought to present at least some meaningful conclusions to the public. See *Finding 1* for further information.

DOS does not maintain online application source documents.

We were unable to review voter registration support documents for any of the online applications in our sample. DOS management acknowledged that there is no source document created for online applications. The SURE system is not designed to maintain a record of the original electronic information forwarded to the county election offices in batches for processing, nor are county election staff required to maintain documentation supporting the electronic information they receive. If county election staff were required to print out the information received online, scan it into SURE, and then save it to the voter's record, a source document would be available for review if needed. Although this would require extra steps by the county election staff, it would provide access to source documents and allow for the auditability of the data.

[113] The REAL ID Act, effective May 11, 2005, establishes specific minimum federal standards for state-issued driver's licenses and ID cards to be accepted for certain federal purposes, like entering a federal building or boarding a domestic commercial flight. Enforcement of the REAL ID Act begins on October 1, 2020 in Pennsylvania. https://www.dmv.pa.gov/Pages/REAL-ID-Frequently-Asked-Questions.aspx (accessed August 6, 2019).

Recommendations for Finding 6

We recommend that DOS:

1. Develop an effective audit trail for registration applications received online to enable either DOS or county election staff to review and confirm the accuracy of information in SURE to the original point of entry of information by the registrant. If this cannot be accomplished through electronic means, see Recommendation 2.

2. If DOS is unable to electronically implement Recommendation 1, it should develop a policy requiring county election staff to print out and scan into SURE voter registration related documents that are received online and attach the documents to the voter's record.

3. Develop a policy requiring the counties to scan all voter registration related documents that are received via hard copy to the voter's record. This will allow for access to the original documents that support information entered into a voter's record in SURE and to help ensure uniformity amongst all the counties.

4. Develop and issue a directive regarding records retention for SURE and work with the Pennsylvania Historical and Museum Commission (PHMC) to confirm that its *County Records Manual* regarding election records is entirely uniform with the SURE records retention directive to help ensure consistency of records retention amongst all the counties. Consideration must be given to the availability of source documentation for purposes of evaluating accuracy of the voter registration information by an external party. The directive should be placed in a prominent location of DOS's website and should be sent at least yearly to all county election offices.

5. Update the SURE regulations to ensure that they are in accordance with the newly developed and distributed record retention policy and the updated PHMC *County Records Manual*.

Finding 7 – The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

From January 2003 through December 2005, the Department of State (DOS) utilized a phased-in approach for implementing the Statewide Uniform Registry of Electors (SURE) system in all 67 counties. As a result, county election offices (counties) have been using the SURE system to process and maintain voter records for more than 15 years. Prior to that, each county maintained its own voter registration system. With the creation and implementation of SURE, there was a need to train county election staff and to provide a resource for updated and ongoing guidance. According to DOS officials, DOS provided initial training to all counties as implementation occurred.

Based on our audit procedures covering the period January 1, 2016 through April 16, 2019, we found that DOS generally provided meaningful assistance and guidance to the counties regarding SURE voter registration and list maintenance. We believe, however, that they did not sufficiently address all critical areas. Job aids should be updated and additional job aids should be developed to help improve the accuracy of voter record information. The critical areas not adequately addressed, along with the current level of guidance provided, are listed below:

- Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls.
- Length of time that voter registration applications (for new registrations or change of name, address, or party affiliation) should remain in pending status – No guidance.[114]
- Record retention policy – No clear guidance (See *Finding 6*).

The following sections describe the assistance DOS provides to the counties and the critical areas on which DOS should further develop and distribute guidance to the counties.

Hands-on training upon request.[115]

We found that although DOS does not schedule required, regular/on-going training for county staff, training is available upon request by the counties. Based on our survey results from 65 counties, 19, or approximately 30 percent, indicated that they requested hands-on training since their initial training. According to DOS management, nine counties were provided a total of 13

[114] When an application is missing a required piece of information it is placed in pending status while the county attempts to obtain the missing information from the applicant. The application, while in pending status is neither approved nor denied, and therefore the applicant is not a registered voter.
[115] Training is provided to county staff in person at DOS offices in Harrisburg.

training sessions during our audit period. Training requested by the other ten counties was provided prior to the beginning of our audit period, January 1, 2016.

Access to the SURE Help Desk.

DOS contracts with a vendor to provide assistance to counties regarding day-to-day SURE questions through a SURE Help Desk as well as training for any new SURE system processes. The Help Desk is comprised of two tiers. Tier 1 is the first point of contact for a county official calling for help. The Tier 1 Help Desk staff stated that they are trained and have access to written guidance on the SURE system to answer most questions from the counties. Tier 2 encompasses two areas: (1) operational support and (2) application development and complex/technical assistance. Tier 2 is a resource when Tier 1 staff cannot answer a county's question, as well as providing training to Tier 1 staff when system changes are scheduled. This ensures that Tier 1 staff are ready to answer any questions/concerns the counties have after deployment of the system change.

We visited seven counties as part of our audit procedures. All seven counties informed us that the Help Desk is an invaluable tool that they use regularly. The responses received from the county survey we conducted also supported this with 40 of the 62 counties that responded to the survey indicating that they contact the Help Desk on a weekly basis.

Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and records of potentially deceased voters on the voter rolls.

DOS, in conjunction with Help Desk staff, creates and electronically distributes SURE job aids to the counties. Job aids are documents that are meant to provide guidance on the current processes established in the SURE system and include, among others, the following helpful features: descriptions of a particular job process; step-by-step instructions on how to perform the process in SURE; and screen shots taken from the SURE system with explanations on using the features in SURE. As described in *Finding 2, however,* there are improvements that should be made in the SURE system regarding work that should be performed by the county election office staff regarding checking for: (1) duplicate voters when processing new voter registration applications; and (2) registered voters on the Pennsylvania Department of Health death records. The recommended improvements will assist in ensuring the accuracy of the data in voter registration records. As a result, as improvements are made to the SURE system, the job aids need to be updated to reflect the processes associated with the improvements.

According to DOS management, the job aids are updated as necessary, typically preceding any enhancements to the SURE system. The job aids are emailed to the counties two days prior to an enhancement and are also posted online within SURE. If a job aid needs to be updated, the new

version is posted and the old version is removed in order to avoid confusion as to which one is the most recent.

In order to determine how helpful the counties find the job aids, our survey inquired whether the counties actually use them. The majority of counties (60 of the 65 counties that responded) confirmed that they use the job aids; however, the counties overwhelmingly noted that they find it easier and prefer to call the Help Desk with questions. This is not because the job aids are confusing, but because they find the Help Desk extremely useful.

DOS provided us with copies of the 64 job aids that were used throughout our audit period. Based on job aid topic titles, we determined, and DOS management confirmed, that 19 of the 64 job aids were applicable to our audit objectives. Our audit procedures included a review of these 19 job aids. We found them to be titled in a manner that makes it easy to determine the topic covered in the job aid, as well as being informative and easy to follow. Based on our review and knowledge of the SURE system, we are in agreement with the general responses received from the counties in both the interviews and survey responses that the job aids are adequate for use in navigating the current SURE system; however, as improvements are made to the SURE system, the job aids need to be updated accordingly.

Another area of concern that we noted was that only 62 of the 64 job aids included a date and the format of the issued date varied. Some included the full date, while others only included the month and year, or only the year in some cases. Although, according to DOS management, it removes the outdated job aids from SURE, many county election directors reported to us that they print hard copies and distribute them to their employees for quick reference. For this reason, it is imperative that DOS ensures that all job aids are dated in a uniform manner to provide a means for users to confirm that they are using the most recent and applicable job aid to assist them in performing the necessary function in SURE.

The following section provides details regarding a critical area not addressed in which an additional job aid should be developed to help improve the timeliness of processing applications that are placed in pending status.

No guidance was provided to counties regarding the length of time that applications remain in pending status and whether pending applications past that timeframe should be denied.

Voter registration applications (applications) that are missing required information or require follow-up with the applicant are placed into pending status until a determination can be made to approve or decline the application. Currently, there is no guidance from DOS to counties with regard to the following:

- The evaluation of pending applications to determine whether the applications should be approved or denied.
- The length of time that applications should remain in pending status.

DOS management indicated it was aware of the issue regarding pending applications and was reviewing its legal authority to direct counties on what actions to take to help eliminate the high number of pending applications.

As noted in *Finding 4*, our data analysis identified more than 54,000 potential applications which have been in pending status for one or more years. When an application is placed in pending status due to missing information, the applicant is sent a letter requesting the missing information. Not all applicants, however, respond to the letter and provide the missing information. When an applicant fails to respond, their application remains in pending status indefinitely.

As reported in *Finding 4*, according to the data we reviewed, 95 percent of applications in pending status are waiting for a response from the applicant. DOS management stated that it would be more beneficial to the applicant and the county if the counties rejected the pending applications for a lack of a response from the applicant after a pre-determined amount of time set by DOS. Once rejected, the counties would send a notification to the applicant. This notification could prompt the applicant to re-apply, rather than the applicant being unaware that they are not registered to vote until they arrive at a polling place on Election Day only then to discover that their name is not included in the poll book. It would also be beneficial for the counties as they would no longer have thousands of pending applications remaining stagnant in SURE for years. See *Finding 4* for more information regarding pending applications.

Recommendations for Finding 7

We recommend that DOS:

1. Continue to offer hands-on training on the SURE system and ensure that all counties are made aware of the availability of this training.

2. Update the applicable job aids as appropriate to reflect changes in processes. For example, added steps for identifying duplicate voters when processing applications or linking a Department of Health death record with a registered voter.

3. Include an issued date (month, date, and year) on all job aids distributed to the counties and an indexed list of all job aids readily available on DOS' website to provide a reference as to which version of a job aid is the most current and the date of the revision.

4. Provide guidance to the counties regarding the maximum length of time that an application can remain in Pending status and how to appropriately determine whether the application should be approved or rejected, if it is determined that DOS has the legal authority.

Agency's Response and Auditor's Conclusion

We provided copies of our draft audit findings and related recommendations to the Pennsylvania Department of State (DOS) for its review. On the pages that follow, we included DOS' response in its entirety. Following the agency's response is our auditor's conclusion.

Audit Response from the Pennsylvania Department of State

PENNSYLVANIA DEPARTMENT OF STATE

RESPONSE TO DRAFT PERFORMANCE AUDIT REPORT

I. Introduction and Background

In November 2017, the Department of State (DOS) began discussions with the Department of the Auditor General (DAG) to help DOS in our preparation to transition to a new voter registration system to replace our Statewide Uniform Registry of Electors (SURE) system. We believed that an audit would help us confirm and identify tools and improvements to seek in a new system and help support our requirements-development process for the RFP for the new system. These objectives were built into the audit.

Around the same time, DOS was contacted by a few senators who wished to discuss possible legislation regarding a SURE security audit. In December 2017, DOS staff, DAG staff and Office of Information Technology (OIT) staff attended a meeting with senate staffers. During the meeting, there was discussion about what the scope of the audit should include. Two primary factors limiting the scope of the audit that were discussed were the Commonwealth's obligation to protect critical infrastructure information under state and federal law and policy as well as pursuant to security best practices, and DAG's express acknowledgment of its lack of expertise and knowledge to conduct a substantive security audit.

The three parties worked together to design a compromise as set forth in the Interagency Agreement (IA)[1] which would limit the security portion of the audit to solely a review of the security protocols of the SURE system, *see* IA ¶ 2.a.iii., or in other words, confirm that appropriate protocols are in place to secure our voter registration system. Security experts agree that such protocols include, but are not limited to, practices such as utilization of continuous network monitoring, inventory identification, intrusion detection sensors, engaging in regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection, multi-factor authentication, security awareness training, risk management, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans. The parties agreed that should there be any dispute between the parties, such disputes would be submitted to the Governor's Office of General Counsel for resolution. *See* IA, ¶ 4.i.

A. Election Security in Pennsylvania

As expressed in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General,* the Commonwealth takes its responsibility to protect the vote very seriously, and is proud to lead the country in using strategic partnerships with federal, state, and county officials and the private sector, to deploy election security best practices and innovative responses to the ever-changing world of cyber security threats. This leadership was underscored most recently in

[1] *See* DAG's Report, App. B for a copy of the IA.

Secretary Boockvar's appointment as the co-chair of the Elections Committee of the National Association of Secretaries of State, as well as her invitation to provide expert testimony at the bipartisan hearing "Securing America's Elections" of the Judiciary Committee of the United States House of Representatives on September 27, 2019. *See* Exhibit B*; see also* https://judiciary.house.gov/legislation/hearings/securing-america-s-elections and https://docs.house.gov/meetings/JU/JU00/20190927/110038/HHRG-116-JU00-Wstate-BoockvarK-20190927.pdf

During this audit, DOS and the Office of Information Technology (OIT) provided DAG with hundreds of pages and hours of presentations, meetings to review and discuss security protocols with "over the shoulder" access to certain information, affidavits, and materials evidencing Pennsylvania's leading information technology and other security protocols and practices to secure the SURE system and protect our elections. These materials included but were not limited to:

- A high-level overview, presented by Christopher P. Dressler, the Chief Information Security Officer for the Employment, Banking and Revenue Delivery Center,[2] of the various external security and assessment reports.
- An extensive two-hour presentation by Erik Avakian, the Chief Information Security Officer for the Commonwealth of Pennsylvania, to review the Commonwealth's cybersecurity program and posture.
- An affidavit executed by Christopher Dressler outlining the multiple mitigating security controls employed by OIT to protect the SURE system.
- Access to over 100 security and cyber hygiene assessments, redacted except for the cover page and section headings, to not only demonstrate the existence of such reports but also to corroborate the repeated information DOS provided to DAG regarding the number and frequency with which those security assessments occur.
- Dozens of SURE user manuals and job aids.
- Dozens of DOS policies, directives and memoranda.
- Access to the SURE Portal and over-the-shoulder access to SURE so that DAG staff could not only ask questions but also review records themselves.
- Access to DOS' Continuity of Operation (COOP) plan summary and scope document
- Access to DOS' high-level disaster recovery plan and table exercise

[2] The Employment, Banking and Revenue Delivery Center provides IT service to DOS as part of the shared service model for state agencies under the Governor's jurisdiction.

- A copy of the Department's policy related to identification, handling, and protection of critical election infrastructure, otherwise known as the TLP policy.

- Provided proof of patching schedules related to underlying infrastructure and architecture.

As described in the letter in Exhibit A, and documented in the above and other presentations, affidavits, and materials, the Commonwealth's strong security protocols include, but are not limited to, the following:

- We engage in 24/7 continuous network monitoring, constant contact with the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), inventory identification, intrusion detection sensors, infrastructure/network diagrams, regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection and multi-factor authentication in access to email, file storage, systems, and other resources.

- The Commonwealth utilizes multiple layers of protection, controls, and end-user security awareness training, risk management, policy compliance assessments, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans as part of a comprehensive cybersecurity program. Additionally, several DOS staff have national security clearances to extend our access to classified information that will bolster our election security.

- Pennsylvania continues to be a nationally recognized and award-winning leader among states in cybersecurity. Our extensive collaboration, including the formation of the Pennsylvania Interagency Election Security and Preparedness Workgroup in 2018, is considered a notable model that many other states are interested in replicating. In addition to DOS, OIT, and the Governor's office, our multi-layered and cross-sector partners include the U.S. and PA Department of Homeland Security, Pennsylvania Emergency Management Agency (PEMA), Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, Pennsylvania Inspector General, County Commissioners Association of Pennsylvania (CCAP), and Center for Internet Security (CIS), among others. We also formed a county/state election security workgroup consisting of CCAP, county election directors, DOS staff, and county and state CIOs and IT personnel.

- Beginning in the 2019 primary, our teams moved our election-day operations to PEMA headquarters. To strengthen our security and responsiveness and enhance our collaboration and coordination, the Commonwealth's election experts, security teams, call center, cybersecurity experts, law enforcement, and state emergency personnel are now able to closely monitor developments throughout the day from

one location with all of PEMA's resources close at hand. Our election, security, and preparedness professionals also participate across the state and across the country in real-time information-sharing on cyber issues, as well as on-the-ground and weather-related situations that could impact voting.

- The Commonwealth also provides anti-phishing and security training and tools to all 67 counties at no cost to them, and our state and federal partners such as the U.S. Department of Homeland Security and the Pennsylvania National Guard additionally offer vulnerability and cyber assessments to them at no cost. Furthermore, we have collaborated with all these partners on multiple tabletop exercises for counties and partners modeled after law enforcement and emergency response techniques, to train election, IT, and security personnel in incident response and preparation, simulating scenarios that could impact all aspects of voting operations.

B. Threats to PA Elections

As Secretary Boockvar testified at the bipartisan hearing "Securing America's Elections" before the Judiciary Committee of the U.S. House of Representatives,

> The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Exhibit B, p. 1. These issues and challenges are why the Commonwealth, and our Inter-agency Election Security and Preparedness Workgroup has employed such a committed, multi-layered, and cross-sector security strategy to election security in Pennsylvania.

C. Election-Related Responsibilities of DOS and County Election Offices

On pages 3 and 4 of the draft audit report, DAG briefly describes the duties of two of the bureaus within the Elections Deputate, which was divided in February 2019 into three bureaus to be better equipped to meet the evolving challenges of election security and technology and augment our civic engagement and campaign finance outreach and programs. A summary of these three bureaus are as follows:

- Bureau of Election Services and Notaries (BEN)– Jessica Mathis, Director. This bureau oversees the functions of the Division of Election Services and Voter Registration, as well as the Division of Notaries. The bureau is responsible for serving voters, candidates, counties, and other stakeholders on matters relating to election administration, voter registration, legislation, and notarial acts.

- Bureau of Election Security and Technology (BEST) – Michael Moser, Director. This bureau oversees the functions of the SURE division and election security and technology initiatives. It is responsible for working with federal, state, and local partners to maintain and enhance the security of Pennsylvania's election infrastructure. The bureau also oversees the voter registration and election management systems, certification of equipment, and technology and data innovation.

- Bureau of Campaign Finance and Civic Engagement (BCFCE) – Tiffany Chang Lawson, Director. This bureau oversees the functions of campaign finance and lobbying disclosure, and works closely with stakeholders, candidates, elected officials, and the public. The bureau also houses and leads the Governor's Civic Engagement Award program, as well as manages DOS's Language Access Plan.

D. **Implementation of SURE**

DAG correctly notes on pages 4-5 of the draft audit report the limits of DOS's authority including lack of enforcement authority regarding voter records. However, despite limits to our statutory authority, DOS facilitates the requirements of Act 2002-3, 25 Pa.C.S. §§ 1101 *et seq.*, imposed upon county voter registration commissions through SURE. The SURE system is also the first-time county legacy systems were migrated into one statewide system. In addition to the tools necessary for counties to meet their statutory duties, DOS provides services through SURE and the SURE Portals to counties and voters that are not explicitly mandated by either federal or state law. For example, DOS provides convenient online tools to voters, which enable them to confirm their registration information online and submit an online application if their information needs to be updated. These tools are also an efficiency to county election personnel.

E. **Commonwealth's Voter Registration Process**

DAG's overview in Appendix C (pp. 77-80) summarizes the voter registration process in Pennsylvania. And while DAG correctly cites to court challenges in states that have enacted documentary proof of citizenship, the U.S. Supreme Court has held that the National Voter Registration Act ("NVRA") forbids states from demanding that applicants submit additional information beyond that required by the federal form—striking down

an Arizona law requiring documentary proof of citizenship from people seeking to register using the federal voter registration form. *See Arizona v. Inter Tribal Council of Arizona, Inc.*, 570 U.S 1 (2013).

Additionally, in Appendix D, regarding the issue with the PennDOT motor-voter system that had allowed ineligible individuals to inadvertently register to vote, it is important to note that DOS acted expeditiously as soon as it became aware of the issue. To be clear, the issue spanned several decades and multiple administrations. DOS became aware of the issue in late summer 2017, and the resolution to fix the problem and prevent future occurrences, which necessitated a change to PennDOT's computerized motor-voter procedures, was completed by early December 2017.

Importantly, DOS informed DAG that the expert data analysis requested by DAG is protected by the attorney-client privilege and the attorney work product doctrine and are not subject to disclosure. DOS remains involved in litigation brought by a third party seeking to access this very same privileged information (as DAG is aware, *see* DAG's Report, App. D, n. 130). Disclosure of the privileged analysis to the DAG would have immediate waiver consequences.

Finally, in response to DAG's recommendation that DOS and the counties must continue to address this concern, DOS states unequivocally that we take very seriously the charge to make sure only eligible voters can cast ballots. We have shared the necessary information with the counties, who are authorized to take further action to confirm eligibility and remove ineligible voters as appropriate.

F. Voter Record Maintenance Process

DOS provides counties with multiple tools for maintaining the accuracy of their voter records and conducting list maintenance, including the National Change of Address (NCOA) program, the Electronic Registration Information Center (ERIC) program, and the 5-Year Notice program.

DOS works together with the members of the SURE Advisory Board created by section 1302-C of the Election Code, 25 P.S. § 3150.2, to periodically update the tools and guidance relied upon by the counties to conduct voter list maintenance, including voter correspondence, list maintenance reports, and job aids.

G. Status of Pennsylvania's Voting Systems

The topic of Pennsylvania's Voting Systems falls completely outside the scope of DAG's audit parameters; there is nothing even remotely applicable to voting systems in the Interagency Agreement. Nonetheless, we welcome the opportunity to recount the significant progress Pennsylvania counties are making in transitioning to new voting systems with auditable paper trails.

First, we want to correct several errors in DAG's summary in this section. One, not all PA counties lacked a paper record in April 2018; 50 counties did. Two, Pennsylvania has already received $14.15 million – this occurred in August 2018. Of these funds, 95% were received from the federal government, plus a 5% state match. More than half of the counties have already begun or have completed the process of receiving their share of the funds. Three, in most counties, the federal dollars amount to at least 10-12% percent of the county cost for the new systems.

The counties are very dedicated to upgrading their voting equipment and worked hard over the last year to meet the upcoming deadline. Last spring DOS directed the counties to select new voting systems meeting current security and accessibility standards with voter-verifiable paper trails by December 31, 2019 and implement them by the 2020 primary. All these new systems were subject to penetration testing, access control testing to confirm detection and prevention of unauthorized access, and evaluation that every physical access point is well secured and system software and firmware is protected from tampering.

To date, at least 53 of 67 counties - 79 percent of Pennsylvania's counties- have voted to select new voting systems which meet current security and accessibility standards with voter-verifiable and auditable paper trails, whereas a year ago, 50 out of 67 counties used paperless DRE voting machines. Remarkably, this November 51 out of 67 counties will be voting on systems with auditable paper records.

Additionally, in January 2019, DOS formed a post-election audit workgroup, which since that time has been studying models of post-election audits. The members of the workgroup include:

- Allegheny County Election Director David Voye
- Lancaster County Election Director Randall Wenger
- Mercer County Election Director Jeff Greenburg
- Mifflin County Election Director Zane Swanger
- Philadelphia Deputy City Commissioner Nick Custodio
- Sullivan County Election Director Hope Verelst
- Brennan Center Democracy Program Counsel Liz Howard
- Common Cause PA Executive Director Micah Sims
- Verified Voting Senior Science and Technology Policy Officer Mark Lindeman
- Department of State representatives:
    - Acting Secretary of State Kathy Boockvar
    - Deputy Secretary for Elections & Commissions Jonathan Marks
    - Director of Election Security and Technology Mike Moser
    - Director of Policy Jessica Myers
    - Director of Elections and Notary Services Jessica Mathis
    - Voting Systems Analyst Sindhu Ramachandran

The workgroup will develop recommendations by January 2020, will work with the legislature for any suggested legislative enhancements, and will carry out pilot audits in multiple counties across the Commonwealth in 2019-2021. By November 2022, all counties will utilize the new enhanced audits.

The first audit pilots in PA will occur in November 2019 in Mercer County and Philadelphia. We will be partnering with local election officials and respected experts to audit both the plain text on the paper records and the tabulated votes to confirm the outcome of the election. The feedback from these pilots will enable the Department of State, in conjunction with local election officials, to establish and test real-time best practices.

Expert partners for the pilot audits include the U.S. Election Assistance Commission, University of Michigan, VotingWorks, Democracy Fund, Verified Voting; Common Cause Pennsylvania, and the Brennan Center for Justice at NYU School of Law.

These audits are scientifically designed and utilize highly effective procedures conducted after an election to strengthen election security and integrity, confirm the accuracy of election outcomes, and provide confidence to voters that their votes are being counted accurately.

In July 2019, Governor Wolf announced that the Commonwealth would begin work to issue a bond to assist counties with purchasing new voting systems with a paper trail. Under the arrangement, the Commonwealth would fund up to $90 million to reimburse counties for approximately 60 percent of their actual costs to replace voting systems, on top of the 10-12 percent they are already receiving from the 2018 federal appropriation.

On October 31st, Governor Wolf signed historic bipartisan election reform, Act 2019-77, that included authorization for the $90 million in bond funding to aid counties with the purchase of new voting systems with a paper trail. The Pennsylvania Economic Development Financing Authority (PEDFA) is preparing to issue this bond following a board vote, and the Department of State will make grants available to counties once established.

H. DOS Plans to Replace the SURE System

DOS worked with federal, state, and county partners for more than a year to finalize the RFP for a new voter registration and election administration system to replace the current SURE system. The RFP was posted for vendor solicitation on October 9, 2019. Responses to the RFP are due in late November 2019, and the selection committee, which includes program and security experts in addition to county election personnel, will begin review and scoring after that time, with selection and approvals to be issued in 2020. The new system goes live by the end of 2021, after extensive transition, training, and careful implementation statewide.

II. **Finding 1** – As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS strongly refutes Finding 1 and stands firmly behind its decision to maintain the confidentiality of the Commonwealth's critical infrastructure information. As stated by the *Pennsylvania Interagency Election Security and Preparedness Workgroup*, composed of the Pennsylvania Office of Homeland Security, Pennsylvania Emergency Management Agency, Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, the Pennsylvania Inspector General, DOS, and OIT,

> As security and preparedness experts, we fully concur with the Department of State's and Office of Information Technology's protection of these documents and determination that they could provide only redacted copies of this information to [DAG]. **We believe their actions embody and uphold the highest standards of security protocol for the Commonwealth.**

Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General.*

Alleged Scope Limitation A

The Commonwealth has for quite some time protected documents and other information related to sensitive security matters. In January 2017, the Federal Department of Homeland Security (DHS) designated election infrastructure (EI) as critical infrastructure information (CII) under the "Government Facilities" sector, which generated even stronger protection at all levels, to further strengthen our nation's security.

These significant protocols governing protection of information relating to election security were discussed with DAG from the very early communications before the audit even began and continued throughout the audit. As stated on page 1 of this response, DAG's objective relating to election security was solely to confirm that appropriate protocols were in place to secure our voter registration database. At no point did DOS or OIT ask DAG to evaluate the security assessments, system configuration, action plans, nor any other protected critical infrastructure information. In fact, DAG had explicitly informed DOS that they had nobody on staff who had expertise in evaluating this type of information and they were happy to note that we were working with DHS and OA-OIT, as well as experts at other state and federal agencies.

Rather, DAG was provided with briefings and documentation, albeit redacted to protect critical infrastructure and cybersecurity information, about the components of the internal controls that were and are in place for the election system. This information included an explanation of the use by the Commonwealth of security experts such as the Department of Homeland Security and other expert security advisors, to regularly assess our internal controls and security and make

recommendations to continue to build and strengthen our protections. We follow best practices and are continually advancing these protocols, and we provided DAG with hundreds of pages and hours of presentations, affidavits, and materials evidencing Pennsylvania's leading information technology and security protocols and practices to secure the SURE system and protect the integrity of our elections and voters.

As stated in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup to the Auditor General,*

> Protection of critical infrastructure information is and has been one of the essential security protocols recommended by security experts at every level.... As security and preparedness professionals, we cannot emphasize enough how important this protection is in order to carry out our duty and responsibility to the citizens of our Commonwealth. This means that information such as vulnerability and cyber assessments, system configuration and architecture, disaster recovery plans, and other types of information that relate to our critical infrastructure should under no circumstances be shared with anyone other than those with an absolute need to know in order to perform homeland security duties.

As we informed DAG repeatedly, this protection is supported by exceptions in the Pennsylvania Right to Know Law and the federal Freedom of Information Act, as well as protection under the Commonwealth Information Technology Policy ITP-SEC019, the Cybersecurity Information Sharing Act of 2015, the Protected Critical Infrastructure Information (PCII) program, and the federal and DOS's Traffic Light Protocol (TLP) policy.

In addition, the U.S. Department of Homeland Security (DHS) and Pennsylvania have specifically identified for PCII protection and TLP Red designation critical infrastructure documents including, but not limited to, system assessments, phishing campaigns, risk and vulnerability assessments, vulnerability scanning (cyber hygiene), architecture review, and cybersecurity evaluation tools.

To foster cooperation and help meet the audit objectives, DOS and OA/OIT offered to provide extensive presentations regarding the cybersecurity assessments, controls and frameworks utilized by the Commonwealth, as well as hundreds of pages of redacted assessments in lieu of the protected documents. As a result, in addition to numerous meetings over the course of the audit process, there were at least two key presentations by OIT's security leadership to DAG, one in October 2018, and one in April 2019.

In the October meeting, DOS met with the DAG team in person to review and discuss high-level overviews of the multiple external security assessment and vulnerability reports we have received for years from DHS and other third-party experts. During the meeting, DOS and DAG reviewed a blank sample of the DHS reports indicating the scope of examinations and testing performed as part of the third-party assessments, so DAG could have an understanding of what was included in these evaluations and reports.

In the April presentation, the DAG team was provided with an in-person presentation by OIT giving a comprehensive overview of the Commonwealth's multi-layered cybersecurity approach

and strategy, collaboration between federal, state and local partners, and assessments performed in our technical environment. In addition, the presentation demonstrated that the Commonwealth's IT controls follow the guidance of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and industry best practices. In fact, the presentation covered all five core categories of the NIST CSF (Identify, Protect, Detect, Respond and Recover), and reviewed with the DAG team the various measures, processes and procedures in place within each category.

Furthermore, the DAG team was provided with in-person meetings by DOS giving a comprehensive overview of the user provisioning, privileged user and system administrator roles and access in March and April. While some of the follow-up documentation was redacted to protect copies of sensitive information, the DAG team was afforded the opportunity to see a display, or "over the shoulder" access, of the credentialing process in production as well as privileged user access and responsibilities.

As evidenced in hundreds of pages and hours of presentations, affidavits, and materials shown to DAG, DOS and OIT demonstrated their extensive utilization of leading information technology and other security protocols and controls. Furthermore, they did so in a manner that not only meets best practices and requirements of IT General Controls and other standards, but also embody and uphold the highest standards of security protocol and protection of critical infrastructure information for the Commonwealth.

We were very pleased on Election Day to welcome Chris Krebs, Director of the U.S. Dept of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA). CISA's election security team has been an instrumental partner in securing our elections in Pennsylvania and across the nation, and Director Krebs emphasized both the strength of our election security protocols and our partnerships.

In our joint press release, Director Krebs recognized Pennsylvania for its election security strengths, and noted:

"Election security is a top priority for CISA. Americans should have confidence that they are the ones picking their leaders and deciding elections without concern about foreign interference. Acting Secretary Boockvar and her team have been strong partners in this effort and continue to lead with their move to auditable systems and investment in election systems," Krebs said. "Voters have a role to play too. We know that foreign adversaries seek to influence public sentiment and may seek to spread wrong information during the election. I encourage everyone to ignore the noise and get election information straight from the source—from the Secretary of State's office or their local election office. Armed with this knowledge, Pennsylvanians can go to the polls today with confidence that their vote will be counted as cast."

Following his visit, Director Krebs tweeted "Just wrapped a visit to Harrisburg, PA, where I toured their election day operations, which includes the Pennsylvania Department of State, PEMA and the PA National Guard, all working together throughout the day." . . . "Pennsylvania has an impressive operation and has been a strong partner of the Cybersecurity and Infrastructure Security Agency."

Alleged Scope Limitation B

DAG selected a sample of 196 voter records from 8.5 million plus voters that were registered as of October 9, 2018 and requested live "over the shoulder" access to view screens containing an actual image of each individual driver's license. As was explained to DAG in February 2019, PennDOT does not maintain an actual image of driver's licenses; rather the information used to create a driver's license is stored across several databases and systems.

As a result of this limitation and the inability to provide the requested "over the shoulder" access a compromise was reached whereby DAG on February 14, 2019 requested "screen capture printouts of the original screens from PennDOT's computer files." To gather the requested information, PennDOT requested identifying information for the 196 selected records.

Prior to providing responsive information a Non-disclosure Agreement (NDA) was required between DAG, PennDOT and DOS. The NDA was executed on April 16, 2019 and on that same day responsive information was provided to DAG. PennDOT provided DAG with two cumulative records: one that contained a file export in the form of an excel spreadsheet that contained PennDOT customers whose driver's license was processed after the implantation of DDL (67 records); the other a PDF that contained screen shots of customer records that were processed prior to the implementation of DDL (120 records). PennDOT was not able to provide verification information for six of the requested records as additional information was required for five of the records and one of the records was inactive.

DAG is inaccurate in their statement that DOS does not maintain source documentation for Online Voter Registration applications and Motor Voter applications. DOS maintains source data for both Motor Voter applications and Online Voter Registration applications. This data is stored and never altered even after the applications are sent to county officials for review. This data is housed in multiple locations within the SURE architecture.

Though DOS does not have direct access to PennDOT's database or the original source data for the licensing transactions, we maintain copies of all Motor Voter application data received from PennDOT. This data can be used to audit the DOT applications that are queued in SURE for the counties to process.

With regard to the delay in responding to certain DAG requests for information, DOS agrees that many of its responses were provided beyond the third day after the DAG's requests. However, it is important to note that many of the DAG's requests for information, particularly IT requests, required the compilation of data, data schema, architectural documentation, etc. in non-native formats. Many of the requests for information also required substantial redaction by DOS staff, in consultation with counsel, to avoid unnecessary disclosure of sensitive information. Additionally, despite DAG having asked us to identify for them critical date periods which would be difficult times for DOS to be responsive to their requests, DAG disregarded those blackout periods on multiple occasions and submitted many queries to us during those times, including seventeen additional requests for information, some of which had multiple subparts, all

submitted to us in the spring 2019, despite us having to oversee at least five special elections in addition to the primary election in the month following their requests.

Four of the requests were for information related to ongoing litigation, which also required close consultation with counsel, and at least two requests were for information that DOS explicitly told the DAG it could not provide. One particular data request related to ERIC program data that required DOS to facilitate a separate non-disclosure agreement between DAG and ERIC. In addition, DOS responded to several redundant requests by indicating that the information requested was provided to DAG as part of earlier responses from DOS. Though DOS did not in every case request an extension in writing, DOS staff regularly communicated to DAG staff the status of those requests that required additional review or substantial redaction.

Conclusion Bullets pp. 17-18

- DOS's preliminary data analysis of DAG's data and conclusions causes DOS to conclude that DAG appears to have made significant errors and/or omissions throughout its analysis, which could have been explained to DAG and avoided if they would have shared their data analysis prior to the report draft. More details are enumerated below in Finding 2.

- As described in detail on pp. 1-4 above, as well as in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup*, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

- DOS shares DAG's concerns about ensuring the most accurate voter records, and the SURE system reaching the end of its useable life. It was for these and other reasons that we had already begun the process of seeking to replace the SURE system and had requested this audit to help gather information to use for the RFP and transition to a new voter registration and election administration system.

- DOS agrees that incorporating additional edit checks and other improvements into the design of the replacement voter registration system will reduce errors and improve accuracy. DOS had previously incorporated these requirements into our RFP for the new system prior to the report draft, as well as other tools that will provide improved checks, balances, and controls.

- We agree that source data or documents should be maintained and accessible for all records and have built these controls into our RFP for our replacement system. Additionally, as noted in our earlier response regarding Scope Limitation B, DOS currently maintains source data for both Motor Voter applications and Online Voter Registration applications.

- DOS is reviewing and working to update current job aids, training, and other guidance to the counties for use of the SURE system and related tasks. Further, these documents are always updated if there are new processes or system functionality changes. DOS also built in requirements regarding job aids and system training into the RFP for the new voter registration and election administration system.

Recommendations

1. As described in detail to DAG throughout the audit, including via hundreds of pages and hours of presentations, affidavits, and materials, including actual redacted weekly and annual independent assessments, testing, and recommendations by DHS and expert third party examiners, the Commonwealth has already and continues to employ these best practices.

2. As stated above on pp. 9-11, we stand firmly behind our decision to maintain the protection of the Commonwealth's critical infrastructure information. Furthermore, our decision is strongly supported by the Commonwealth's security and preparedness experts, concurring with our protection of these documents and determination that we could provide only redacted copies of this information to DAG. As stated in Exhibit A by the Election Security Workgroup, "We believe [DOS's] actions embody and uphold the highest standards of security protocol for the Commonwealth."

3. Please see the response to recommendation 2, noted above. Further, and as referenced in page 14 of DAG's report, access to Protected Critical Infrastructure Information (PCII) was denied because DAG does not perform homeland security duties, nor did it need to know the information to complete the audit. References to the USA Patriot Act and to the Critical Infrastructure Information Act of 2002 (CHA) were provided.

Additionally, it is DOS' position that the Critical Infrastructures Protection Act of 2001, 42 U.S.C. §§ 5195 – 5197h, the related Protected Critical Infrastructure Information (PCII) program, the sensitive nature of PCII information as submitted by DOS for Department of Homeland Security Review, and the Traffic Light Protocol (TLP) information protection protocol and its related "Need to Know" mandate for information considered "For Official Use Only" (FOUO), all provide a mandate to ensure security information is jealously protected. The definition of FOUO contained in Department of Homeland Security Management Directive MD 11042.1 underscores this approach when it provides, in part, that disclosure of such information "could adversely impact . . . programs or operations essential to the national interest." Moreover, the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501-1510, and the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 671 – 674, both underscore the severe vulnerabilities that exist in critical infrastructure, the need to protect cyber, critical infrastructure and related information, the methods created for such protections, and the duties incumbent upon the holders of such information to limit disclosure solely to those entities having a demonstrated need for the information. Further, Pennsylvania's Right to Know Law, 65 P.S. §§ 67.101 – 67.3104, provides support for the confidential treatment of such agency information, containing numerous exceptions from public disclosure for different categories of records at 65 P.S. §

67.708(b), including homeland security, physical and infrastructure details, threat assessments, public safety matters, computer and related system security, critical systems configurations,

4. As we did throughout this audit engagement, DOS will encourage counties to cooperate in audits and other performance reviews that can benefit them.

5. Please see above pp. 9-11, Exhibit A, and answers to the recommendations above.

6. Results of assessments and recommendations are already shared with those charged with security and governance of the SURE system.

III. **Finding 2** – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as nearly three thousand potentially deceased voters that had not been removed from the SURE system.

DAG did not provide DOS with the data they identified for us to check until October 9, 2019 and neglected to provide the queries used to complete their analysis for verification even though it had been requested on August 19. Furthermore, the October 9th data received from DAG required extensive cleanup and formatting by DOS before DOS could begin to review their findings. Despite this, they refused to give us a deadline beyond October 28 to respond, notwithstanding DAG's own staff acknowledged that it would take many months to analyze this data and these queries. Remarkably, DAG refused also to extend the deadline beyond Election Day, even with their explicit awareness that the very same DOS and county election staff who are working hard to administer and secure the elections November 5th, are the people needed to respond to DAG's inquiries. DAG apparently decided it was a higher priority to respond to their queries than to administer and secure our elections.

As a result of this unreasonable time period, to date we were only able to assess a small portion of DAG's allegations. Nonetheless, DOS's preliminary data analysis of that small portion of DAG's data and conclusions causes DOS to conclude that DAG appears to have made significant errors and/or omissions throughout its analysis. Consequently, DAG incorrectly flagged thousands of records as potential concerns that through further investigation should not be flagged, including flagrant errors such as identifying individuals who are very much alive as deceased voters.

We will continue to work with the counties to analyze and respond to all DAG's data and queries over the coming weeks and months but have serious concerns about the accuracy and the veracity of the data outlined in this report.

Moreover, regarding the delay in providing electronic files, DAG requested a copy of the voter registration records for SURE; however, within those records is confidential data and information from ERIC. As such, before release of the files and for DOS to not breach its own Non-Disclosure Agreement (NDA) with ERIC, it was necessary for DAG and ERIC to negotiate

an NDA to protect ERIC's confidential data and information from disclosures that would compromise the security of the data and the privacy of individuals whose data resides in ERIC's database. This negotiation occurred over the course of about three months, with DOS diligently facilitating the exchange of information between the parties. The NDA (and not DOS) was the sole reason for the delay in providing the electronic files to DAG.

24,408 cases - the same DL number listed in more than one voter record

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks.

13,913 Potential duplicate cases

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the election requiring our attention, DOS was unable to complete our review of this data set in the inadequate time frame provided. However, DOS was able to carefully review portions of this data and our initial analysis demonstrates that DAG appears to have made significant errors and/or omissions throughout its analysis, and incorrectly flagged thousands of records as potential concerns that through accurate analysis should not have been flagged. DOS focused its initial review on one of the data sets in DAG's analysis, which is comprised of 1,612 potential duplicate records. A summary of our preliminary results is listed below.

	Matching Elements			
	First Name, Last Name, and DOB	First Name, Last Name, and last 4 SSN	First Name, Last Name, DOB, and Last 4 SSN	Total
Total Potential Matches Analyzed	712	896	4	4
(number of records in potential matches)	(1,426)	(1,795)	(8)	(3,229)
Clear Non-Matches	696	894	0	1,590
Requires further information from the counties	16	2	4	22

During our review, it became abundantly clear that the DAG failed to incorporate all data that was provided to them to validate potential matches. For example, when matching on 3 elements (First Name, Last Name, DOB), DOS could clearly demonstrate potential matches were incorrect when also reviewing the last 4 SSN on the individual's record or DL. DOS was also clearly able

to identify a potential match was incorrect when reviewing an individual's middle name and suffix on a potential match. Despite having this information in their possession, DAG irresponsibly failed to utilize this necessary data to accurately match voter records.

As shown, DOS could clearly demonstrate potential matches were incorrect when matching on SSN in addition to the First Name and Last Name. We were able to do so by using a combination of DL, DOB, or other name elements like middle initial and suffix. Only 2 records in that category require county research.

If a match is underdetermined by DOS, it has been referred to the county for additional research so they can review the documentation available on the voter record.

In summary, when reviewing this group of 1,612 alleged matches by DAG, only 22 were referred to counties for additional information, and based on the results to other data reviews discussed below, we expect most, if not all of these to be cleared by further data. We will complete this review and update this response when we receive responses from county election offices.

6,876 potential DOB inaccuracies – DOBs equate to voters being 100 years or older

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to complete our review of this data set. We intend to review the findings in the coming weeks. However, it is important to note that while there could be DOB inaccuracies related to legacy data, some of the records that were identified as erroneous dates of birth are in fact correct. DOS has a policy for county election officials to comply with Act 188 of 2004, which is otherwise known as the Sexual Violence Victim Address Confidentiality Act. It's an important policy to protect victim information, and it requires county election officials to list a generic date of birth to safeguard their personal information.

2,230 potential DOB and/or registration date inaccuracies

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks.

2,991 potentially deceased voter records

Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the election requiring our attention, DOS was unable to complete our review of this data set within the inadequate time frame given. However, DOS was able to carefully review portions of this data, and in a matter of a few weeks completely disproved multiple

allegations, demonstrating how flawed and unreliable their data analysis was and is. Many of the voter records identified by DAG seemed to confuse voters with same or similar names, which may well have been avoidable with closer analysis of the data DAG had in their possession. Based on our analysis to date, we have every reason to expect that DAG'S allegations will continue to be disproven.

Recommendations

DOS is currently reviewing the data provided by DAG to determine whether any of the DAG's conclusions are accurate when compared to the original voter data provided by DOS. DOS will investigate any apparent DL matches and work directly with counties and PennDOT to verify, as necessary.

1. DOS will continue to leverage its membership in ERIC to identify and review and cancel in-state and cross-state duplicate voter records.

2. As is already current practice, DOS will continue to utilize its membership with ERIC to analyze SURE voter records to identify incorrect, out-of-date or duplicate data in SURE. In addition, DOS will be incorporating additional data cleansing in its implementation of data migration to the new voter database. Further, DOS takes data cleaning and analysis seriously and has hired a data specialist to assist with existing data reviews and migration to the new system.

3. As is already current practice, DOS will continue to employ field-level data validation, as necessary, to give counties the tools they need to identify potential duplicate data, without removing the counties' statutory authority to determine the qualifications of individual applicants.

4. As noted previously, DOS consults with the members of the SURE Advisory Board on an ongoing basis to update the user manuals, job aids and directives that counties rely on to guide them through all aspects of maintaining accurate voter records SURE.

5. Pursuant to DOS's existing agreement with ERIC, DOS will continue to send data to ERIC for the purpose of identifying potential in-state and cross-state duplicate voter records. DOS will also direct counties to use the duplicate voter record notices developed for the ERIC program to conduct regular list maintenance in compliance with federal and state law. Also, as mentioned above, DOS will leverage the new data specialist position to assist with periodic system data analysis.

6. As is the typical procedure of DOS, work with counties to conduct data cleanup will continue, as necessary, to identify and correct data entry errors and bad data migrated from legacy voter registration systems.

7. DOS requirements for the new voter registration system, which were developed in consultation with county voter registration and election personnel, require data validation measures to reduce the likelihood of data entry errors. DOS will also continue to development its online voter tools, like Online Voter Registration and Online Absentee Ballot Request, which provide upfront verification for many voters and eliminate manual data entry.

8. Though it appears from our early analysis that the number of potentially deceased voters is vastly overstated due to a flawed data analysis, DOS will continue to work with counties to research the data provided by DAG to identify and remove any apparent deceased voters.

9. In keeping with current protocols, DOS will continue its collaborative work with the Department of Health and ERIC to identify deceased voter records and transmit to counties the information they need to remove them.

10. DOS will continue to collaborate with DOH to identify process improvements and data enhancements to ensure that counties have timely and correct information about potentially deceased voters.

IV. **Finding 3**- The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

As described in detail on pp. 1-4 above, as well as in Exhibit A, *Letter from the PA Interagency Election Security and Preparedness Workgroup*, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

As noted on page 33 of the DAG report, Governor Wolf signed Executive Order 2016-06, which effectively consolidated and centralized management and operation of IT services for all executive agencies. This model over time has led to improvements in overall IT governance and the implementation of additional internal and external controls. DOS, like any other executive agency, conforms to the IT Policy Governance structures set forth in IT Policy BUS000 (ITP-BUS000), which can be found online here:
https://www.oa.pa.gov/Policies/Documents/itp_bus000.pdf

Consistent with its charge under ITP-BUS000, the CIO for the Employment, Banking and Revenue Delivery Center, of which DOS is a part, holds regular steering committee meetings with DOS, Delivery Center IT staff, and DOS IT support staff to ensure alignment between the Commonwealth's IT policies and DOS's strategic and operational planning.

Vendor oversight practices

Per ITP-SEC009, all employees, including contractors, providing IT services must complete a criminal background check. Those background checks are completed by the Pennsylvania State Police (PSP). Further, all employees or contractors must comply with the Department's TLP Policy related to critical infrastructure information. Additionally, SOC reports are currently reviewed by personnel within the EBR Delivery Center and Office of Administration. Further, DAG requested SOC reports from vendors that were a non-party to our Interagency Agreement, and therefore, was not in scope.

DOS management's county-level SURE Equipment Use Policy fails to provide clear guidance to counties.

DOS's SURE Equipment Use Policy contains instructions for county election and county IT officials regarding proper connectivity and proper use of SURE equipment, as well as guidance regarding the use of county-owned equipment. As noted in the DAG report on page 35, DOS's policy includes certain prohibitions that have been put in place to protect SURE equipment and the SURE network. In addition, the policy states on page 7 that county staff are required to notify DOS of any changes that may impact the SURE system in any way at least one week prior to implementation of those changes. Please refer to the relevant excerpt from the policy below:

Very Important: County staff are required to provide DOS with at least one-week notice of any planned changes that may impact the SURE system in any way (e.g. planned power outage, relocation of equipment, etc.). County IT staff are also required to notify DOS of any emergency changes that impact the SURE system in any way. Notification of changes may be made via the SURE Help Desk. Failure to notify DOS of changes will result in the county bearing any costs incurred to identify and resolve any problems that occur.

Currently, the policy directs counties to contact the SURE Help Desk to provide notification of planned changes. The moment that a county contacts the SURE Help Desk, the Help Desk technician creates a "service ticket" in DOS's ticketing system. The Help Desk technician also records the details provided by the county, and either resolves the issue or escalates the ticket to Tier 2 Support staff. The ticketing system is the logging and monitoring tool that agency users and support staff MUST use to log, update, and track SURE-related. This single logging and tracking system is in place to promote accountability and to ensure continuity throughout the routing of the ticket. It also serves as a knowledge base that enables DOS staff to reconstruct the actions taken from the moment a ticket is opened until the ticket is resolved.

We agree that it is necessary to regularly review and update the Equipment Use Policy, which is already in progress. We also agree that providing a form to formalize county configuration requests could augment the current system by serving as the original artifact of a county's request. As a result, we will distribute a link to the policy in the body of every SURE maintenance memo.

Though the DAG's report provides no specific recommendations for updates to the policy, DOS will nonetheless review the current version of the policy to determine what additions or clarifications may be necessary to make clear the risks of not following the policy.

Recommendations

1. As noted in our responses to requests for information 13 and 14, section 1302-C, 25 P.S. §3150.2, provides for a SURE Advisory Board to advise DOS on matters related to the SURE system and voter registration. The six members of the Advisory Board are selected by the Secretary of the Commonwealth and the majority and minority leaders in the two houses of the General Assembly. As articulated in the Board's charter, the Advisory Board and DOS conduct monthly teleconferences to:

- advise DOS so that it can provide the most effective and efficient statewide voter registration system for the Commonwealth of Pennsylvania.
- provide recommendations regarding issues and procedures related to SURE system maintenance and future enhancements.
- provide feedback during the development of new SURE processes to improve the performance of the SURE database, to comply with statutory changes, and to anticipate the future needs of users and stakeholders.
- document and improve existing business processes to make the best use of SURE system technology.
- assist in prioritizing requests for SURE system improvements and changes.
- oversee and direct, as necessary, both government and public SURE user groups.
- work with county election officials, in addition to those on the Advisory Board, to gain consensus on issues affecting SURE.
- assist DOS in designing a communications strategy to effectively reach county election officials, other SURE users, and the public at large.

The monthly teleconferences, except when a month falls during a statewide election, include members of DOS staff, as well as the Department's Project Management Office's Portfolio Manager who serves as the primary liaison between DOS staff, Help Desk support and OIT.

2. When the Department of State was incorporated into the Employment, Banking and Revenue (EBR) Delivery Center, it allowed OA/OIT resources across multiple EBR agencies to start supporting DOS IT activities, including SURE system maintenance. One of the first changes implemented was the removal of Production system access from the primary vendor supporting SURE. Other contracted resources from different vendors (under the management of Commonwealth IT staff) still had access, but required explicit, written approval from DOS and IT Management staff prior to making any changes.

As part of an effort to modify how IT support and maintenance services were provided to DOS, a Request for Proposal (RFP) was issued, including significant changes to how services are being delivered to DOS. This will include (but not be limited to) new documentation requirements, new processes and policies, and an increased ability to monitor and oversee vendor staff working on the systems. Several of the more significant changes include; moving vendor staff into Commonwealth facilities where there will be in-person supervision from IT management staff; utilizing equipment issued, maintained and monitored by Commonwealth IT resources from OA

and the Delivery Center; and the addition of Service Level Agreements (SLAs) requiring greater accountability regarding testing and oversight of system changes.

Another aspect of adding DOS to the EBR Delivery Center is that DOS can incorporate the IT best practices developed over time by the larger EBR DC agencies. This enables DOS-specific IT support practices to mature much more quickly than they could as a stand-alone agency. The new maintenance contract will give DOS greater ability force the vendor to adopt these policies and practices moving forward.

As noted in our response to the DAG's discussion of the governance structure of SURE on pages 32 through 34 of its report, DOS and the CIO for the Employment, Banking and Revenue Delivery Center, of which DOS is a part, conforms to the governance structure established by ITP-BUS000. We appreciate the perspective of DAG regarding employee awareness of the governance structure and how effectively team members are working within that structure. DOS will continue to work with OIT to ensure that all staff working in and supporting SURE are fully aware of the governance structure, understand its lines of authority and communication, and understand expectations regarding how they are to operate within the governance structure.

3. We are in the RFP process for replacement of the SURE system. Please refer to our response on page 8, which outlines the general timeline for the RFP.

4. Many of the security guidelines issued by DHS-CISA in May 2019, *Best Practices for Security Election Systems*, are already part of the library of election security practices and protocols that we already use, and the agency and the Commonwealth are always evaluating opportunities to implement additional controls that improve the security posture of the environment. As described in detail on pp. 1-3 above, as well as in Exhibit A, Letter from the PA Interagency Election Security and Preparedness Workgroup, the Commonwealth utilizes leading information technology security practices and controls, using a multi-layer, strategic approach – leveraging people, policies, technologies, best practices and procedures around the safeguarding of data and the protection of the applications, systems and resources.

5. Vendors are already required to comply with Commonwealth security policies. External suppliers must agree to, and comply with, the Commonwealth IT contracts terms and conditions which requires compliance with Commonwealth information technology policies (ITPs), non-disclosure agreements (NDAs), IT Acceptable Use agreements and audit requirements. Additionally, DOS has agreements in place with agencies and external partners that govern the security, confidentiality and audit provisions as applicable. Further, all vendors who provide IT services must comply with background checks. Additionally, all vendors and Commonwealth employees comply with annual security training requirements.

6. Vendors already are monitored in compliance with management directive 325.13. DOS and the Commonwealth monitor external supplier controls by requiring the delivery of Service Organization Controls (SOC) reports as part of the contract with the data center service provider.

7. As noted in our prior responses, DOS maintains agreements with agencies and external partners that govern acceptable use, security, confidentiality and auditability. The Commonwealth also requires delivery of SOC reports by suppliers be reviewed timely and collaboratively by DOS and OIT to ensure full accountability from internal and external partners.

8. Please see prior section pp. 20-21. DOS agrees that requiring counties to formally acknowledge the policy periodically will ensure awareness and accountability. It is important to keep in mind that the network through which counties connect to SURE is maintained entirely by the Commonwealth and remains segregated from county and other networks. Should a county attempt to reconfigure its connection to the SURE network, DOS is alerted via network monitoring. See below for more details.

9. Whenever a county requires equipment, the county submits a request form to the SURE office. If the request is approved, a ticket is entered in ServiceNow and assigned to the SURE Tier 1 help desk. The requested equipment is provided by the Commonwealth and sent to the requesting county. A few of the counties procure their own high-volume printers. Request for approval to use any county-owned equipment follows the same process as requesting Commonwealth equipment.

The county networks connect to the County Connect Network via a hub (owned by the County or the Commonwealth) connected to a Verizon router under Commonwealth control. It is the single point of connection between the Commonwealth network and the county network. There are no permitted deviations from this architecture model.

Some of the counties use Commonwealth-provided KVM switch to attach mice and keyboards to the Commonwealth WinTerms, others connect county-owned peripherals directly to the WinTerm.

10. DOS SURE staff and the Bureau of Management Information Systems (BMIS) are working together to review and update the SURE Equipment Use Policy and associated procedures. This project is anticipated to be completed by the end of the year. Part of the policy changes will include having all appropriate SURE users sign the policy.

11. Part of the initiative to update this policy as described above includes the review and revision of the *SURE User ID Request Form.*

12. DOS provides SURE system policies to counties via the SURE Extranet, but we will better organize them and will also leverage the CCAP Election Security Workgroup to ensure awareness and understanding of the policies among all relevant county personnel.

V. **Finding 4** - Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

Weaknesses within application process

We strongly disagree that there are significant weaknesses in the voter registration process. In fact, DOS has made and continues to make improvements to the application process and county processing efforts.

We agree that additional edit checks are warranted, and we had already incorporated these and other protections into the RFP for the new voter registration and election administration system that will replace the SURE system. DOS shares the Auditor General's concerns about accuracy and is taking steps to make sure that the new system with provide more robust checks and balances.

DOS had also already integrated automated processes, such as checking for duplicates and running reports, into the RFP for the system that will replace SURE. We intend to move to a system that will provide readily configurable hard stops that will not allow the user to proceed to the next step in the process without completing certain items, like pending applications or upload of source documents. We also intend to do a thorough data analysis prior to moving to a new system so that we are starting with the most accurate data possible in the new election administration system.

Weaknesses regarding maintenance of voter registration records with SURE system

List maintenance was an area DOS focused on heavily in requirements development for the new system. Additionally, DOS is seeking a system that allows for better oversight by DOS and county election officials, including pulling status reports and receiving automated notifications when a process is completed or when a deadline is approaching, and a process remains incomplete by a county.

DOS is seeking a system that allows better visualization of the data for internal and external users. Additionally, DOS hired a data specialist who will assist with analyzing data within the system to identify areas for improvement as well as trends that may enable to DOS to identify efficiencies or areas where additional training is needed by county users. The data specialist will also assist the new "SURE" team in monitoring user activity and flagging incomplete processes, incorrect actions and overdue tasks.

We appreciate the Auditor General's recommendation, but also note that our use of data is impeded by the current language in the Act 2002-3, the voter registration law. DOS continues to work to find ways to use as much of the data we receive from ERIC as possible, while we engage with the Legislature to get the necessary changes to the law.

Applications remain in pending status

DOS has worked proactively to address the issue of applications that remain in pending status. As noted on page 42 of the DAG report, DOS works with counties to "clear" pending applications before closing registration prior to a primary or general election. It is not uncommon for there to be thousands of applications that are still in New or Pending at and immediately after

the voter deadline. Between October 9, 2018 and November 5, 2018, the counties processed 13,130 pending applications.

To reaffirm that counties may not leave voter applications in pending status for long periods of time, DOS issued a directive on July 10, 2018, directing counties to make sure that all New and Pending applications are resolved prior to closing registration. DOS also sent a subsequent memorandum and copy of the directive on October 16, 2018 to remind counties of their statutory obligation to process all pending applications. In addition, the Division of SURE also includes a section in its SURE-related preparations memorandums distributed prior to each primary and election reminding counties to process all new and pending applications before closing out registration. In 2019, these memorandums were distributed to counties on April 24 and October 7. The Department also directly calls each county with pending applications to ensure they are processed prior to printing supplemental poll books so all eligible voters are listed in the poll book.

In the event that any counties have not resolved all of their New and Pending applications by the Monday prior to the election, DOS distributes through SURE a list of all applications in these two statuses, with an additional reminder to resolve those applications and a reminder to rely on those lists as a resource when they are adjudicating provisional ballots.

Recommendations

1. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

2. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

3. DOS disagrees with DAG's recommendation to the extent it relates to rejecting voter registration applications in a pending status for non-match of numbers. To reject such applications would be contrary to DOS's directive to the counties that there is no legal basis under federal or Pennsylvania law to reject or delay processing a voter registration application solely based on a non-match between a registrant's identifying numbers on the application and the comparison database. As it relates to other pending applications, DOS will review DAG's recommendation in consultation with legal counsel as we implement the new election administration system.

4. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

5. We have existing procedures in place but will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

6. DOS provides to counties annually the data and guidance necessary to complete their statutorily-mandated list maintenance duties, which require counties to send NVRA-compliant notices to voters who appear to have moved or who have not voted or otherwise updated their voter record in the five years preceding the date of the notice. The deadlines to complete these list maintenance activities are defined by statute. Both federal and state law establish "quiet periods" within 90 days of an election, before which counties need to complete their annual statutory voter removal programs, otherwise known as list maintenance. So, it's important to note while the DAG alleges records may not have been inactivate or removed, a majority of county offices may not have completed their list maintenance activities until after the 2018 General Election, which fell after they received the datasets from DOS. This is all to say that additional records may have been inactivated or removed for lack of activity after the General Election, but the datasets didn't capture that data as they were current as of October 9, 2018.

As demonstrated in our response to RFI #10, the counties' list maintenance activities are monitored daily via an automated job that summarizes each county's list maintenance activities. These list maintenance activities, with counts of inactivated and cancelled records, are summarized in the DOS's annual report to the General Assembly on voter registration.

DOS will continue to work with SURE Support staff to further develop these automated monitoring notifications, and we will work with the SURE Advisory Board to augment our guidance, as necessary.

7. Please refer to the automated monitoring description provided in our prior response.

8. We have been working towards this goal, and in fact, were already planning to implement extended ERIC functionality in December 2019, having now acquired all the necessary prerequisites for full functionality to take effect.

VI. Finding 5 - Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy

Features that were missing or inadequate within the SURE system which could reduce or prevent errors

DOS already included requirements in the RFP prior to this report for the new system to address and prevent errors, including residential address checks. Until the new system is implemented, DOS will work on implementing a feature in the SURE system that does not allow for a residence outside of the PA.

Like most state election offices nationwide, DOS is in the process of incorporating GIS into all processes where applicable. GIS will be a feature of our new election administration system but was not widely used when the SURE system was built. We agree that it is useful and necessary, in fact, it is so important to DOS that we recently hired a Data Specialist with GIS expertise to our elections team, to help with data analysis, data visualization and GIS implementation.

We are also working with counties on a GIS pilot to develop procedures related to redistricting and use of GIS in elections for residential address verification and other means. The pilot is organized with both state and county representatives with both elections and GIS experience. We anticipate the first GIS procedures will be available in 1st quarter 2020. The pilot also builds off national expertise where Pennsylvania Department of State was recently selected as one of five states to further geo-enabled elections with the National States Geographic Information Council (NSGIC).

https://elections.nsgic.org/five-statewide-pilot-studies-launched-to-further-geo-enabled-elections/

DOS is aware of the lack of "read only" features and spent considerable time during requirements development for the RFP drafting user roles and functions tied to those roles, including read only access. These user roles would allow for better definitions of access for each user as well as allowing better tracking and auditing of the actions each user takes in the system.

Finally, like several other areas already discussed, DOS considered and is requiring several edit checks and hard stops for the new election administration system. In addition to not being able to move forward in certain processes until all information is complete, DOS will "lock" certain areas or functions of the system during certain periods. This will make it impossible for counties to revise or cancel records during certain periods.

Two areas of improvement related to PennDOT Motor Voter process and reporting capabilities within SURE system

DOS has a strong working relationship with PennDOT and has spent considerable time in the last several years improving the Motor Voter process, including changes to the order of the screens and simplification of language used in the Motor Voter system. DOS is currently working with PennDOT on the next round of improvements to the process, which already include potential updates to the change of address matter as identified in the audit report. Additionally, the Department wishes to further simplify the voter registration process at PennDOT and streamline the experience for individual's registering to vote or updating their existing registration.

DOS is very aware of the limitation regarding creation of reports in the SURE system. We are working with developers to write scripts for the most common reports needed from the current system, but also included requirements regarding report generation in the RFP for the new system. We agree that all users need to be able to run customized reports and have prioritized that need for the new system.

Recommendations

1. We acknowledge the recommendations made here and are happy to report that all the following items are already requirements for the new election administration system:

- GIS feature for checking voter addresses, assigning polling places to voters, locating polling places, etc.;
- Edit checks and system stops to alert users of out of state addresses, incomplete information, missing information, the need to upload supporting documents, etc.;
- User roles that allow DOS to create different levels and types of access, including read only access, for system users;
- Hard stops that prohibit users from moving to the next process before completing the current one and that do not allow users to take actions outside of allowed timeframes;
- The ability to generate notifications (emails and letters) automatically and in batches from the system, including notices to those who submit a change of address, but are not currently registered;
- And giving each user the ability to generate reports that contain information that they need rather than requesting report generation through a ticket process to the Help Desk.

2. Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks and will follow up with the county, as necessary.

3. Due to the unreasonable time frame provided, data formatting issues with DAG's data production, and the upcoming election requiring our attention, DOS was unable to review this data prior to the deadline for initial response. We intend to review this data analysis in the coming weeks and will follow up with the county, as necessary.

   The SURE system is designed to automatically associate the proper cancellation reason with the source of the cancellation transaction. For example, voter records that are being cancelled as a result of statutory list maintenance activities are automatically coded with the cancellation reason CANCEL-INACTIVE STATUS FOR TWO FED GEN ELECTION CYCLES and voter records that are cancelled due to a Department of Health death notification are automatically coded with the cancellation reason CANCEL – DOH DEATH NOTIFICATION. DOS will continue to work with the SURE Advisory Board to build in data field validations as necessary, and we will continue to provide step-by-step training and written instructions for county SURE users.

4. Please see our response on page 28. We are currently working with PennDOT to streamline and further enhance the existing registration process, which contemplates updates to the change of address process to capture additional registration information so the county may process a new registration if the applicant thought they already had an existing registration.

VII. Finding 6 - A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

As noted in our response to Scope Limitation B on pages 11 and 12, it is not accurate to state that there is not source documentation available for Motor Voter and Online Voter Registration applications and the source data necessary to test the accuracy of 93 Motor Voter records and 19 Online Voter Registration records was available to the DAG. See above pp. 11-13. We offered copies of the source data available in SURE for Motor Voter applications, but the DAG declined.

While DOS has provided retention guidance previously, we do believe we could expand that guidance. The County Records Manual is the primary resource of guidance on the retention and disposition of county records. This manual is posted on the Bureau of State Archives on its website here: https://www.phmc.pa.gov/Archives/Records-Management/Documents/RM-2002-County-Records-Manual-2017-Update.pdf. This manual serves as the comprehensive guide to county records retention requirements, including those requirements for elections and voter registration records. The manual makes clear that applications must be retained for 22 months in accordance with federal and state law. When necessary, DOS collaborates with the Pennsylvania Historical and Museum Commission (PHMC) to update our portions of the guide.

As noted in our response to RFI #15, we distribute the PHMC documents as the authoritative tools for both election and voter registration records retention requirements because they are legally accurate, compiled in subject-specific documents, and they were last updated in consultation with DOS. Though DOS cannot speak to the PHMC's methods or frequency of distribution of the guide, we acknowledge that infrequent distribution of the relevant portions of the guide could contribute to a lack of awareness on the part of county election officials. DOS plans to reissue retention guidelines prior to the end of 2019 as well as post to the County Extranet.

PennDOT refused to provide access to Motor Voter source documents

Please refer to our response to Scope Limitation B on pp 11 - 12.

DOS does maintain online application source documents

As noted in our response to Scope Limitation B on pp 11- 12, DOS maintains source data for both Motor Voter applications and Online Voter Registration applications.

Recommendations

1. DOS does maintain source data for Online Voter Registration applications, and there is an auditable trail of data housed in multiple locations within the SURE architecture.

2. This is not a necessary option because DOS maintains an electronic audit trail as described in the preceding paragraph.

3. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

4. DOS will expand our communications to counties on the retention policies mandated by the NVRA and state law, as referenced in the County Records Manual. DOS will post a link to the County Records Manual on our website and the County Extranet, and we will include references to the manual in our training materials.

5. DOS will conduct a review of the SURE regulations, and consider amendments if necessary, to ensure the regulations are consistent with federal and state retention requirements.

VIII. Finding 7 - The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, deceased voters on the voter rolls, pending applications, and records retention.

Job aids need to be updated to reflect improvements recommended for the SURE system regarding review for duplicate voter records and deceased voters of the voter rolls

As noted in our response to RFI #25, DOS updates job aids at the time functionality is added or changed. These updated job aids are distributed to all county election and voter registration contacts a few days before the added or changed functionality is deployed to SURE, including the Duplicate Voter Notice and Deceased Voter job aids that were updated in August 2017 and July 2019, respectively. Counties are also provided an opportunity to review the new functionality prior to deployment during county user review sessions.

We agree with the DAG that job aids should be dated consistently, with the month, day and year. To ensure that there is no possible confusion, we will also add a version history log to each job aid to clarify changes or modifications. Further, DOS will engage in a review of all job aids and guidance promptly and update accordingly, as needed.

Please refer to our response on page 26 regarding the July 10, 2018 directive issued by DOS related to pending applications.

Recommendations

1. We will continue to offer hands on training at no cost to the counties. Currently, the Department provides on-site training at the county or on-site training in Harrisburg at their request.

2. We agree with the DAG that job aids should be dated consistently, with the month, day and year. To ensure that there is no possible confusion, we will also add a version history log to each job aid to clarify changes or modifications. Further, DOS will engage in a review of all job aids and guidance promptly and update accordingly, as needed.

3. We will take this recommendation under advisement and discuss this with the SURE Advisory Committee.

4. DOS will review this recommendation with legal counsel and determine what guidance DOS can provide as we implement the new voter registration and election administration system.

EXHIBIT A

COMMONWEALTH OF PENNSYLVANIA
INTERAGENCY ELECTION SECURITY & PREPAREDNESS WORKGROUP

October 28, 2019

Auditor General Eugene DePasquale
613 North Street, Room 229
Finance Building
Harrisburg, PA 17120-0018

Dear Auditor General DePasquale:

As the members of the Pennsylvania Inter-Agency Election Security and Preparedness Workgroup, we strongly disagree with many of the findings of your Draft Performance Audit report relating to the Department of State's SURE system.

The Commonwealth takes its responsibility to protect the vote very seriously. Pennsylvania is proud to lead the country in using strategic partnerships with federal, state, and county officials, along with partners in the private sector, to deploy election security best practices and innovative responses to the ever-changing world of cyber security threats. Based on our extensive security and preparedness experience, we find many of your audit findings to be flawed and misleading, failing not only to accurately reflect the strength of our security protocols, but also the vital importance of protecting our nation's critical infrastructure information as crucial to defending our nation's security.

As evidenced in hundreds of pages and hours of presentations, affidavits, and materials shown to your office, the Department of State (DOS) and the Office of Information Technology (OIT), in partnership with all other members of the Inter-Agency Election Security and Preparedness Workgroup, employ leading information technology and other security practices and controls to protect the Commonwealth's elections. The Commonwealth's strong security protocols include but are not limited to the following:

- We engage in 24/7 continuous network monitoring, constant contact with the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), inventory identification, intrusion detection sensors, infrastructure/network diagrams, regular third-party vulnerability and cyber assessments, firewalls, encryption, password protection and multi-factor authentication in access to email, file storage, systems, and other resources.

Office of the Secretary of State
Room 302 North Office Building | 401 North Street | Harrisburg, PA 17120-0500 | 717.787.6458 | F 717.787.1734 www.dos.pa.gov

- The Commonwealth utilizes multiple layers of protection, controls, and end-user security awareness training, risk management, policy compliance assessments, continuity of operations (COOP) planning, disaster recovery, and code reviews and scans as part of a comprehensive cybersecurity program.

- Pennsylvania continues to be a nationally recognized and award-winning leader among states in cybersecurity. Our extensive collaboration, including the formation of this workgroup in 2018, is considered a notable model that many other states are interested in replicating. In addition to DOS, OIT, and the Governor's office, our multi-layered and cross-sector partners include the U.S. and PA Department of Homeland Security, Pennsylvania Emergency Management Agency (PEMA), Pennsylvania State Police, Pennsylvania Department of Military and Veterans Affairs, Pennsylvania Inspector General, County Commissioners Association of Pennsylvania (CCAP), and Center for Internet Security (CIS), among others.

- Beginning in the 2019 primary, our teams moved our election-day operations to PEMA headquarters. To strengthen our security and responsiveness and enhance our collaboration and coordination, the Commonwealth's election experts, security teams, call center, cybersecurity experts, law enforcement, and state emergency personnel are now able to closely monitor developments throughout the day from one location with all of PEMA's resources close at hand. Our election, security, and preparedness professionals also participate across the state and across the country in real-time information-sharing on cyber issues, as well as on-the-ground and weather-related situations that could impact voting.

- The Commonwealth also provides anti-phishing and security training and tools to all 67 counties at no cost to them, and our state and federal partners such as the U.S. Department of Homeland Security and the Pennsylvania National Guard additionally offer vulnerability and cyber assessments to them at no cost. Furthermore, we have collaborated with all these partners on multiple tabletop exercises for counties and partners modeled after law enforcement and emergency response techniques, to train election, IT, and security personnel in incident response and preparation, simulating scenarios that could impact all aspects of voting operations. Pennsylvania stands out as a leader nationwide in the extensiveness of our cross-sector training, coordination, and collaboration.

- Last spring, DOS directed the counties to select new voting systems meeting current security and accessibility standards with voter-verifiable paper trails by December 31, 2019 and implement them by the 2020 primary. All these new systems were subject to penetration testing, access control testing to confirm detection and prevention of unauthorized access, and evaluation that every physical access point is well-secured and system software and firmware is protected from tampering.

- To date, 79 percent of Pennsylvania's counties have voted to select their new systems. One year ago, 50 out of 67 counties used paperless DRE voting machines. Remarkably, this November, 52 out of 67 counties will be voting on systems with auditable paper records.

- Additionally, In January 2019, DOS formed a post-election audit workgroup, to study models of post-election audits. These audits, such as risk-limiting audits, are scientifically designed and utilize highly effective procedures conducted after an election to strengthen election security and integrity, confirm the accuracy of election outcomes, and provide confidence to voters that their votes are being counted accurately. PA's first pilot RLA audits will be conducted in November 2019 in Mercer and Philadelphia counties. Recently, the Washington Post, in addition to many experts, lauded this post-election audit approach a best practice that all counties across the country should follow.

The Commonwealth has for many years protected documents and other information related to sensitive security efforts and procedures. Developing emphasis at both the federal and state levels in protecting critical infrastructure information has appropriately generated even stronger protocols at all levels, in order to further strengthen our nation's security.

In January 2017, pursuant to the USA Patriot Act, the federal government designated election infrastructure as part of the nation's critical infrastructure. Since that time, federal, state, and local governments have been working to advance policies and procedures as quickly as possible to provide the greatest protection to our elections. Because this designation is so new, these policies and procedures are under constant review and development to be responsive to changing needs and threats.

Late in 2017, the federal government created the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), a first of its kind collaboration among federal, state, and local officials to secure elections, to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge.

When the audit began in 2018, the EIS-GCC was very new, and the development of national and state procedures has grown steadily over the last year. Pennsylvania has worked closely with the federal government and other states to advance these policies, and in August 2019, Acting Secretary Boockvar was named as a representative to the EIS-GCC, on behalf of the National Association of Secretaries of State (NASS).

Protection of critical infrastructure information is and has been one of the essential security protocols recommended by security experts at every level. These significant protections were discussed with your office from the very early communications before the audit even began and continued throughout the audit. As security and preparedness professionals, we cannot emphasize enough how important this protection is in order to carry

out our duty and responsibility to the citizens of our Commonwealth. This means that information such as vulnerability and cyber assessments, system configuration and architecture, disaster recovery plans, and other types of information that relate to our critical infrastructure should under no circumstances be shared with anyone other than those with an absolute need to know in order to perform homeland security duties.

This protection is supported by exceptions in the Pennsylvania Right to Know Law and the federal Freedom of Information Act, as well as protection under the Commonwealth Information Technology Policy ITP-SEC019, the Cybersecurity Information Sharing Act of 2015, the Protected Critical Infrastructure Information (PCII) program, and the federal and Department of State's (DOS) Traffic Light Protocol (TLP) policy.

In fact, the U.S. Department of Homeland Security (DHS) and Pennsylvania have specifically identified for PCII protection and TLP Red designation critical infrastructure documents including, but not limited to, system assessments, phishing campaigns, risk and vulnerability assessments, vulnerability scanning (cyber hygiene), architecture review, and cybersecurity evaluation tools, and DHS has confirmed this protection covers all this information as recently as a few weeks ago.

As security and preparedness experts, we fully concur with the Department of State's and Office of Information Technology's protection of these documents and determination that they could provide only redacted copies of this information to you. We believe their actions embody and uphold the highest standards of security protocol for the Commonwealth.

In closing, based on our extensive experience with election security, we find many of your audit findings to be flawed and misleading, failing to accurately reflect the strength of our security protocols and the vital importance of protecting our nation's critical infrastructure information as crucial to defending our nation's security.

We are very proud to work in partnership with all our member agencies, to leverage our collective expertise in elections, homeland security, cybersecurity, law enforcement, and emergency preparedness, and provide a national model for security protocols and protecting and defending our elections in the Commonwealth. We welcome you and any others willing to join in productive conversations to further our critical collective efforts.

Sincerely,

Major General Anthony J. Carrelli
Adjutant General of Pennsylvania
Department of Military and Veterans Affairs

Colonel Robert Evanchick
Pennsylvania State Police Commissioner
Pennsylvania State Police

Marcus Brown
Director of the Office of Homeland Security
Pennsylvania Office of Homeland Security

Kathy Boockvar
Acting Secretary of the Commonwealth
Pennsylvania Department of State

John MacMillan
Chief Information Officer and
Deputy Secretary for Information Technology
Pennsylvania Office of Administration

Randy Padfield
PEMA Director
Pennsylvania Emergency Management Agency

Bruce Beemer
Pennsylvania Inspector General
Office of the Inspector General

EXHIBIT B

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF STATE

Testimony of Kathy Boockvar
Acting Secretary of the Commonwealth
Commonwealth of Pennsylvania
Hearing on *Securing America's Elections*
U.S. House of Representatives, Committee on the Judiciary
September 27, 2019

Chairman Nadler, Ranking Member Collins, and distinguished members of the House Judiciary Committee, my name is Kathy Boockvar, and I am the acting Secretary of State (or Secretary of the Commonwealth) of Pennsylvania. As Secretary, I lead the Pennsylvania Department of State (DOS) to promote the integrity and security of the electoral process, protect public health and safety by licensing professionals, support economic and nonprofit development through corporate and charitable registrations, and sanction professional boxing, kick-boxing, wrestling and mixed martial arts. Prior to being appointed as Secretary, I served as Senior Advisor to Governor Wolf on Election Modernization, leading and managing initiatives to improve security and technology in Pennsylvania's elections, in collaboration with federal, state, and county officials.

Thank you for inviting me to testify at your *Securing America's Elections* hearing. As the Chief Election Official of Pennsylvania I have the immense privilege of working with extraordinarily dedicated election directors and personnel in all 67 counties across the Commonwealth, as well as committed Secretaries of State across our great nation, to ensure that our elections - elections that allow candidates running for every local, state, and federal office to serve – are free, fair, secure, and accessible to all eligible voters. In August 2019, I was also honored to be asked to serve as the Elections Committee Co-Chair for the National Association of Secretaries of State (NASS).

The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Alongside the great majority of states across the nation, we urge the federal government to provide additional election security funding and support to counties and states and reinforce our collective infrastructure. All of us at the federal, state, and local levels benefit from the security of our elections, so funding these critical operations must be a cost-share by the federal, state, and local levels. Because the technologies and attempted attacks are becoming more

SECRETARY OF THE COMMONWEALTH
302 North Office Building | 401 North Street | Harrisburg, PA 17120-0500 | 717.787.6458 | Fax 717.787.1734 | dos.pa.gov

sophisticated all the time, we need to plan for and invest in election security like we invest in other ongoing initiatives and challenges. Like other types of security, like STEM fields, like education of our children – investment cannot be once and done, and it should never be dependent on political winds. There is nothing partisan about ensuring that our elections are secure and accessible to all eligible voters. We must have a continuous investment in election security at all levels, both in funding and in strengthening our infrastructure, communications, and responsiveness, so that we may advance and adapt to change as new information is gained and new technologies advanced.

NATIONAL LANDSCAPE

There have been some great advances in election security over the last several years at all levels, while challenges continue to emerge as well. All these – continuing to strengthen advances and pursuing additional goals forward - require significant funding, proactive bi-partisan leadership, quick response time, multi-agency collaboration, and other support.

The National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED) and Secretaries and election officials across the country have been resolute in our commitment to bolstering security in elections, and collaboration at all levels. As NASS Elections Committee Co-Chair, I look forward to working with my fellow Co-Chair Secretary Mac Warner (W.Va.) and with colleagues across the country, to share best practices and provide the most secure and accessible elections to eligible voters in Pennsylvania and nationwide. One of my responsibilities as Co-Chair is to serve as a NASS representative on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

In January 2017, when the federal government designated election infrastructure as part of the nation's critical infrastructure, the EIS-GCC was one of the first developments of that designation. The EIS-GCC is a first of its kind collaboration among federal, state, and local officials to secure elections, working to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge. The EIS-GCC has 29 members, of which 24 are state and local election officials. It also includes members from the U.S. Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the National Association of State Election Directors (NASED), the Election Center, and the International Association of Government Officials. The members of the EIS-GCC are working to update an elections-sector specific plan, improve communications protocols and portals, and secure increased resources for state and local election officials. In addition to the GCC, a Sector Coordinating Council (SCC) was also established for non-government, private sector entities to better communicate with election officials and the federal government.

Beyond the EIS-GCC, DHS and the Center for Internet Security (CIS) have been particularly strong partners. Pennsylvania and other states regularly collaborate with DHS on independent risk and vulnerability assessments, intelligence, training, tabletop exercises, communications,

and more. We also work with CIS's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center, (EI-ISAC) to gather and share intelligence about cyber threats that target government or government-affiliated systems, and gain support and resources including forensic analyses and emergency response assistance. Additionally, the cyber defense team of the Pennsylvania National Guard has been an exceptionally strong partner. Within the last year they were the first National Guard team selected to participate in a new DHS program, to be trained to conduct Risk and Vulnerability Assessments to DHS standards.

For all these strong collaborative partnerships to be most effective, and for additional goals to be advanced, more resources are needed. Some top priorities would include the federal government playing a greater role with vendor oversight, including tracking vendor foreign ownership, data hosting, manufacturing and employee background checks, and chain of custody for all voting and election system components; and reinforcing Continuity of Operations Plans (COOP) across levels and sectors, to provide more clarity on primary points of contact in the federal government for incidents and concerns. It would also be beneficial to have broader communications between our federal election security partners and our state legislatures and counties, so that counties and legislators could hear directly about federal election security priorities and concerns. We also need to strengthen lines of communication from the federal government to the state chief election officials, for example to ensure that federal entities notify the state when local incidents are reported, so that we may immediately act when necessary. Additionally, federal funding and support are needed to ensure that all counties have state-of-the-art intrusion detection systems, comprehensive phishing, cyber hygiene, and security awareness training, vulnerability assessments, and more.

PENNSYLVANIA LANDSCAPE

Most people have an understanding that the word "cyber" relates to the study of systems and the intersections and communications between people and machines. But the word "cyber" actually has ancient Greek origins, deriving from the Greek word for the "gift of governance" and "leadership." In Pennsylvania, we have been tapping both aspects of the word in our election security planning, using resilient and integrated governance and leadership to enhance the intersections and communications between people and machines, to continue to advance our technologies while also doing so in a way that protects our democracy and develops collaborative and responsive policy and leadership. This requires a tremendous amount of resources but has immeasurable value.

Collaboration

Thanks to Governor Wolf's deep commitment, we have employed a multi-layered and cross-sector security strategy to election security. We broke down silos and brought together experts from multiple fields and sectors at the local, state, and federal levels, including professionals in information technology, law enforcement, homeland security, defense, elections, and emergency preparedness. Beginning in 2018, we formed an executive Interagency Workgroup on Election

Security and Preparedness, banding together experts from the Department of State (DOS), Homeland Security, Emergency Management Agency, Information Technology, State Police, National Guard, the Inspector General, and the Department of Military and Veterans Affairs. This team of key agencies meets regularly and collaborates on increasing election security training, support, assessment, information, and preparedness, to implement best practices to respond to and mitigate continuously evolving security threats.

We also formed a county/state election security workgroup of County Commissioners Association of Pennsylvania (CCAP), county election directors, DOS staff, and county and state CIOs and IT personnel. This workgroup discusses security issues and shares training resources, including guidance, security awareness training, and resources on strong cyber security practices for voting system and network preparation and security, including pre-election testing, password and permissions management, restricting access, file transfers, and vote canvassing. We are also providing anti-phishing and security training tools to all 67 counties at no cost to them.

We have collaborated with all these state and federal partners to provide tabletop exercises to counties and partners, modeled after common military and law enforcement techniques, to train election, information technology, and security personnel in incident response and preparation, simulating scenarios that could impact voting operations.

We were the first state in the nation to accept DHS's offer to provide vulnerability assessments to the states – we did this in 2016, 2018, and are planning a third assessment in the next several months. We have tools in place to identify vulnerabilities, detect network intrusion, and encrypt data in-transit and at rest. We engage in ongoing continuity and disaster recovery exercises and review and revise as necessary our COOP plans several times each year.

Voting System Upgrades and Post-Election Audits

As of 2018, Pennsylvania was one of the small minority of states still primarily voting on paperless Direct Recording Electronic (DRE) voting systems. In April 2018, DOS directed all 67 counties to purchase new voting systems that meet current security and accessibility standards, and which include a voter-verifiable paper record with plain text language that voters can verify before casting their ballot and that local officials can use in recounts and post-election audits. These new systems must be in use no later than by the primary of 2020, and preferably by the November 2019 election.

In order to bolster our voting system security even further, in 2018 DOS created new security standards by which to evaluate the new voting systems applying for certification in PA. PA law requires both federal and state certification, and because the federal EAC had not updated its standards in some time and did not have a quorum to do so at the time, we decided to update our state security standards, and additionally assess the accessibility of the systems. The new voting system standards incorporated tests to ensure confidentiality, vote anonymity, integrity, security, auditability, and usability of the voting systems. All new certified systems in Pennsylvania have passed the following tests:

- Penetration testing that evaluates the security of the voting system by trying to exploit potential vulnerabilities.
- Access control testing to confirm that the voting system can detect and prevent unauthorized access to the system and election data.
- Evaluation of voting system audit logging capabilities to confirm that the system logs will allow auditing, as well as investigation of any apparent fraudulent or malicious activity.
- Tests that ensure every physical access point is well secured and system software and firmware is protected from tampering.

To evaluate accessibility of voting systems for voters with disabilities, we utilized expert review by usability and accessibility examiners as well as feedback from voters with disabilities and poll workers.

DOS has certified seven new voting systems that meet these standards, and we are very pleased with the remarkable progress made by the counties. The county election directors and commissioners have been incredibly dedicated to acquiring voting systems that best meet their voters' needs and provide the most secure, auditable, and accessible voting systems to all Pennsylvanians. Already, 75 percent of counties have officially voted to select new systems, and 46 out of 67 counties are utilizing their new systems with verifiable paper records in November 2019. The remaining counties are still hard at work planning and evaluating their voting system choices, reviewing vendor quotes and prices, holding new voting system demonstrations for the public, consulting with voters and poll workers and exploring funding and financing options.

Cost, of course, remains a major concern for counties. Since the beginning of this initiative, we have been committed to this enterprise being a cost-share of federal, state, and local dollars. Toward this end, we designated 100% of the federal funds appropriated in 2018 for election security proportionately to the counties for replacement of their voting systems by 2020, totaling $14.15 million in PA (including a 5% state match). Though a welcome down payment and approximately 10-12% of the total costs of the new systems, $14.15 million is not nearly enough, and we are pursuing additional state and federal funding.

We have also formed a statewide post-election audit working group, which includes election officials from six counties of different sizes and demographics across the state, as well as expert advisors on audits and elections. This working group is studying audit models such as risk-limiting audits and is developing best practice recommendations for post-election audits that will review the plain text on the paper records and the tabulated votes to confirm to a reasonable degree of statistical certainty the accuracy of the outcome of the election.

The dedication and thorough examination by the members of this workgroup to developing effective models has been inspirational and should be a model for other states looking to explore these practices. In addition, two of our counties on opposite sides of the state, Philadelphia and Mercer county, have volunteered to pilot advanced post-election audits this November 2019,

which will offer confidence to the voters as well as the opportunity to establish and test real-time best practices. Additional Pennsylvania counties will also be piloting audits over the next several years, and we expect all counties to employ enhanced audits by the 2022 general election.

Looking Forward

Looking forward, we continue to build. The above initiatives have taken and will continue to take significant resources to advance. In addition to advancing and strengthening all of the above, our highest priority goals and need for additional resources include: replacing our statewide voter registration system (SURE); ensuring all counties have advanced intrusion detection systems and practices, ongoing and evolving comprehensive cyber hygiene assessments, COOP and security training, and vulnerability assessments; and implementing new voting systems, strengthened pre-election testing, and enhanced post-election audits statewide.

CONCLUSION

On Election Day 2018, we saw what happens when all of the collaboration and hard work comes to fruition, and the powerful benefits of the intersection of all of the above in action. We were connected throughout the day to the counties, state agencies, other states, and the federal government through shared dashboards and frequent communications. For example, if another state was seeing attempted attacks coming from particular IP addresses, they were able to share with other states, allowing us to block those IP addresses at the state level, and then Pennsylvania would share those IP addresses with all 67 counties to enable them to block those IP addresses as well. We had conference calls throughout the day with our interagency group members and counties, sharing what we were hearing and seeing, any concerns, and any support or resolutions we could provide from our different sectors. This collaboration and communication allowed us to be proactive in our defenses, rather than just reactive as might have occurred in the past.

The right to vote is a fundamental right, and every voter must be provided equal access to the polls and deep-seated confidence in the security and accuracy of their vote. We cannot allow circumstances to develop whereby voters in under-resourced counties have less security or less accessibility in their vote. Pennsylvania — where both the Declaration of Independence and the U.S. Constitution were adopted — takes its legacy as the birthplace of American democracy very seriously, and we know that the foundation of that democracy rests on the security, auditability, accessibility and integrity of our elections. We urge you please to invest additional funds to ensure this for ourselves and for generations to come. Our democracy - and bolstering voters' confidence in their ability to participate fully in that democracy - is worth every dollar.

Thank you for the opportunity to testify on this important issue, and I am happy to answer any questions you may have.

Auditor's Conclusion to the Department of State's Response

Note: The page numbers referred to by the Department of State (DOS) in its response are from a draft report of the findings and recommendations and do not correspond to the page numbers in this final report; therefore, in this conclusion, we will refer to the respective findings and subsections in this report as necessary.

Overall, we are highly discouraged not only by management's responses to our draft findings, but also the general negative tone of the response. This is particularly surprising since the DOS itself requested the audit and the Department of the Auditor General (DAG) made every possible effort to provide a cooperative and constructive auditing process DAG takes exception to DOS' multiple mischaracterizations and flawed arguments. Additionally, DOS did not provide specific examples to us to prove that our analysis of the data was incorrect.

More general comments are below:

We are concerned that DOS' efforts to deflect recognized weaknesses in the SURE system will inhibit its ability to recognize existing shortfalls and improve the SURE system overall. Additionally, we were exceedingly surprised that DOS' response indicates that it strongly disagrees with many of our findings and it completely mischaracterizes information that was provided, or not provided to us in many instances, during the course of our audit. In its attempt to discredit our findings, DOS does not seem to understand that a primary objective of our audit was to assess the accuracy of records maintained in the SURE system. Our audit procedures disclosed internal control weaknesses related to input and maintenance of voter records. Our data analysis revealed examples of potential inaccuracies, all of which should be properly investigated by forwarding the information to the counties for further examination. Tests of accuracy are performed by comparing data to other sources, searching for duplicate information, and checking for inconsistencies and unreasonable values. In one example, DOS appears to assume that because a middle initial is different between two records, then the records are definitively those of different persons despite two or more other personal elements (e.g. date of birth (DOB), last four digits of Social Security number) being exactly the same. We disagree. In light of the internal control weaknesses found, there is potential in this example, that a data entry error could have occurred when typing the middle initial, which is why we continue to recommend that these cases warrant further investigation. We are concerned that DOS, and therefore the counties, will not utilize the information provided to them in the audit because it is assuming that the data in the SURE system is accurate. Our data analysis and internal control assessment strongly suggest otherwise.

Further, while DOS requested this audit, its management does not seem to grasp that we cannot properly conclude and satisfy the audit objectives in accordance with generally accepted *Government Auditing Standards* without obtaining sufficient, appropriate evidence. Yet, in spite of the limitations imposed by DOS, we believe we have provided DOS with recommendations

that, if appropriately implemented, will improve the security of Pennsylvania's voter registration system and the completeness, accuracy, and auditability of its voter registration records.

A large portion of DOS management's comments appears to be an attempt to deflect their uncooperativeness and shortcomings. While DOS spent considerable effort noting how they were not provided sufficient time to respond to our audit report, they failed to acknowledge that per the Interagency Agreement, effective May 15, 2018, the audit was due to be released no later than January 31, 2019. In fact, the Interagency Agreement specifically sought to eliminate any potential timing conflicts with the November 2019 election when it set the release date of January 31, 2019. While DOS agreed to such terms in the Interagency Agreement, they nevertheless failed to follow its spirit and now seek to discredit DAG's overwhelming attempts to accommodate DOS. This deadline was postponed three times due solely to DOS' inability to provide DAG with timely responses. Had DOS cooperated and provided DAG with timely responses to our requests, the report would have been issued as agreed upon, and therefore would not have interfered with the November 2019 election. Contrary to DOS' comments, DAG does not believe that our report is more important than the election; however, we too have a responsibility to deliver, in a timely manner, quality audits to the taxpayers of Pennsylvania.

DOS provided information throughout its response regarding updates and events that have occurred or procedures that have been implemented since the end of our audit procedures on April 16, 2019. As we have not performed a review of all of these events or procedures, we cannot comment regarding these items. We did confirm certain updated information provided regarding the *Introduction and Background* and incorporated this new information into our report. We also appreciate DOS' comments supportive of our results for certain work performed.

The following sections provide clarification regarding DOS' responses to specific information related to our findings and certain background information included in this report.

Finding 1 - As a result of the Department of State's denial of access to critical documents and excessive redaction of documentation, the Department of the Auditor General was severely restricted from meeting its audit objectives in an audit which the Department of State itself had requested.

DOS refutes *Finding 1* and maintains its decision to not provide certain information. DOS further suggests there was a misunderstanding as to our audit objective to review security protocols of the SURE system and believes it provided us with enough evidence to satisfy this objective. We strongly disagree with DOS' response, and in particular, regarding DOS' statement that DAG acknowledged that it had a lack of expertise and the knowledge to conduct a substantive security audit. When DAG was approached concerning a possible audit of the voter registration system, we realized that cybersecurity would be a significant part of the audit. Our IT Audit Managers are all Certified Information Systems Auditors and receive training on cybersecurity. We acknowledged, however, that we had insufficient resources in-house

specifically to perform network penetration testing. Also known as "ethical hacking," penetration testing attempts to locate vulnerabilities in a computer system by breaking into it using the same tools as malicious cyber criminals. While we have observed penetration tests performed by other auditors, we did not have the expertise in-house to hack systems and expressed that fact.

During a preliminary discussion, officials from the Office of Administration, Office for Information Technology (OA/OIT), explained that appropriate network penetration testing had already been performed and we could rely on that testing. We agreed that we would most likely be able to rely on the work performed by other auditors in this area if we could review the reports. We explained that we would require access to the network penetration audit reports since *Government Auditing Standards* require us to consider the work of other auditors and to determine the status of corrective actions.[116] With assurances received that we would have access to the reports, we recommended acceptance of the engagement.

We were therefore, very surprised in July 2018 when access to the reports was abruptly denied on the very day we were scheduled to review the reports. We were surprised again when we attempted to perform our own IT controls testing, both in the area of cybersecurity and the more routine IT general controls, and found that DOS delayed, blocked, or redacted information required to complete the audit in accordance with *Government Auditing Standards*. We explained that assessment of the effectiveness of Information System controls (also referred to as IT controls) was required by *Government Auditing Standards* because IT was so significant to multiple audit objectives including controls over adding and maintaining voter records.[117] While DOS provided verbal and written representations as to the level of controls in place, testimonial evidence alone is not considered sufficient evidence on which to base an audit.[118] Further, hundreds (if not thousands) of pages of reports with the entire contents redacted from top to bottom provides no evidence of scope, results, or corrective actions.[119] We were, therefore, not able to obtain sufficient evidence to comply fully with *Government Auditing Standards* in this area as stated (see *Scope Limitation A* in *Finding 1*).

DOS provided a letter from the *Pennsylvania Interagency Election Security and Preparedness Workgroup* dated October 28, 2019, long after completion of our audit procedures and seven-and-a-half months after a deadline to receive documentation for the audit, supporting DOS' decision not to provide reports and documentation needed to complete the audit (DOS' Exhibit A). As noted in *Finding 1*, however, the Auditor General traveled to Washington D.C. to meet with representatives from the U.S. Department of Homeland Security who stated that sharing Homeland Security reports was left up to the discretion of each particular state. Further, our consultations with cybersecurity audit experts from other state audit organizations during the audit confirmed our absolute need to review these outside reports in order to comply with *Government Auditing Standards*. Experts from the University of Pittsburgh Institute for Cyber

[116] U.S. Government Accountability Office. *Government Auditing Standards.* 2011 Revision. Paragraph 6.62.
[117] Ibid., Paragraph 6.16.
[118] Ibid., Paragraph 6.62.
[119] Ibid., Paragraph 6.36

Law, Policy and Security, in *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations* recommended that DOS cooperate fully with the Pennsylvania Auditor General's audit and recommended specifically that the DAG examine cyber incident response plans. In fact, the report states, *"...it should not be problematic to share sensitive information about cyber incident response plans with those officials."*[120] Finally, it should be noted that the cyber security reports we had attempted to review for purposes of this audit were, prior to our request, available to numerous individuals, including non-DOS employees, who had access to these documents. Although we were told that we could not be provided with these reports because of "DOS policy," no such policy existed until April of 2019, after our deadline to submit documentation for the audit. DOS was unable to determine which individuals who had access to these reports actually viewed, copied or circulated them. This systemic behavior is concerning because it evidences a lack of established, well thought-out, and enforced policy until DAG requested access to documents, which apparently were provided freely to non DAG employees prior to our audit.

Regarding DOS' response related to information provided by the Pennsylvania Department of Transportation (PennDOT), we acknowledge in *Finding 6* that PennDOT provided us with limited documentation, but it did not contain all the Motor Voter information needed to complete our assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law. As DOS indicates in its response, the information provided was in the form of an Excel spreadsheet rather than directly from the data source. Since information can easily be manipulated in Excel, we could not conclude that the data provided was reliable, and therefore, we could not use it for testing purposes. Screen shots provided information regarding the voters' driver's license information but did not contain all the fields of information that we were testing for voter registration such as political party and residence versus mailing address, which could be different as in the case of college students.

Further, DOS is inaccurate in their response that the report states that DOS does not maintain source documentation for Motor Voter applications. We did not request Motor Voter information from DOS since PennDOT, not DOS, is the original recipient of Motor Voter applications. Additionally, although DOS contends that they have source data for Online Voter Registration applications, when we requested that information on January 30, 2019, while at the DOS offices conducting testing, we were verbally informed that there was nothing available for us to review. Although DOS contends that the data is stored in multiple locations within the SURE architecture, the data was not provided to us when requested.

Regarding DOS' delay in responding to our requests for information, we agree that some of the requested information would take longer than the standard three business days to compile. Due

[120] The University of Pittsburgh Institute for Cyber Law, Policy and Security. *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations*, January 4, 2019. Pages 10, 37, 38, and 53. https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report_0.pdf

to this fact, we informed DOS at the beginning of the audit that if they anticipated needing additional time, they could notify us in writing of that request so that we would be aware of the delay. As we noted in *Finding 1*, DOS only requested an extension one time. Although we did submit requests for information during DOS identified blackout periods, this was done to allow for the continuation of the audit after much delay by DOS. As previously stated, we had informed DOS that if additional time was needed to please notify us, which DOS chose not to do. Further, DOS identified multiple blackout periods some of which only affected certain DOS offices or county election offices. As we could not be sure which offices were impacted during the blackout dates, we submitted requests for information, again with the understanding that DOS could notify us if an extension was needed to provide the requested information. Although DOS contends that its staff regularly communicated to DAG the status of outstanding requests, the only response that DAG received from DOS was DOS' acknowledgment that the information requests had been received, that they would review the request and "be in touch," or that staff were working on the requests without providing any detail as to when or if the information would be provided to DAG.

DOS stated in its response that the Request for Proposals (RFP) for the new voter registration system to replace the current SURE system has been completed. We are encouraged that based on a cursory review of the RFP posted on October 9, 2019, it appears that DOS has included certain edit checks and other application controls recommended in our report and preliminarily discussed with DOS management on August 19, 2019. Our recommendations included the use of driver's license numbers in the search for duplicates, the incorporation of Geographic Information System (GIS) capability, and the expansion of the use of data available from the Electronic Registration Information Center (ERIC). We believe this will help reduce errors and inaccuracies when processing voter applications and performing subsequent list maintenance.

Finding 2 – Data analysis identified tens of thousands of potential duplicate and inaccurate voter records, as well as voter records for nearly three thousand potentially deceased voters that had not been removed from the SURE system.

Finding 2 describes the results of our data analysis that DOS requested in the Interagency Agreement to conduct our audit. Due to audit time, financial, and staffing constraints, we did not validate the thousands of cases/situations identified, and as a result, we use the term "potential" to be conservative. We believe, however, that in most of these instances, there are inaccuracies within the data maintained in SURE, and therefore, DOS needs to work with the counties to properly investigate and address all of these situations and correct the voter records as appropriate to ensure that SURE contains accurate information, as required by law. We are concerned that by dismissing specific potential errors noted in the findings, DOS is missing the larger issue that inaccurate data exists in SURE and that they will not properly forward the information to counties to investigate and correct the data, if necessary.

Of note, DOS does not comment on the 24,408 cases where the same DL number is listed in more than one voter record, which appears to be an indication that the data analysis yielded results that will be helpful for improving the accuracy of the data, and that DOS agrees that some of the information in SURE is not accurate. As for the 13,913 other potential duplicate cases, DOS focuses on one subset of 1,612 potential duplicate records and accuses DAG of inaccurate analysis. DOS is assuming, however, the data is accurate stating that because a middle initial may be different between two records, a duplicate does not exist even though the first name, last name, and last four digits of the social security number are the same. DOS is assuming the difference in middle initials is always accurate and states those cases need no further investigation. The complacency of DOS in a matter of such importance is, in a word, disheartening. We wholly disagree in that our report provides examples of many instances where data in the SURE system certainly appears inaccurate. DOS should forward all of the cases and related information to the counties to investigate and determine whether the data is correct or whether a duplicate exists.

DOS claims to have disproved "multiple allegations". Despite DOS' assertion that certain data analysis was flawed, DOS provided no specific examples to us to prove that our analysis of the data was incorrect. As a result, our data analysis stands and we continue to recommend that DOS forward the detailed exceptions to the counties for investigation.

In its response, DOS mischaracterizes data we provided regarding the results of our analysis. To clarify, DAG provided detailed files of each exception noted in the report on October 1, 2019. These files were in Microsoft Excel format and each file included the programming logic that we used in our data analysis software, ACL, to extract the exceptions. On October 8, 2019, DOS requested copies of the entire database used in our analysis. On October 9, 2019, DAG provided copies of the raw data provided by DOS in 2018 in the exact same format as we had received it from DOS. Since it is an exact copy of their own data, we are confused as to why DOS expressed difficulty with its own data format.

DOS maintains that the delay in providing the data files in 2018 was due to the negotiation of a Non-Disclosure Agreement (NDA) with ERIC that occurred over the course of approximately three months. DAG documentation, however, indicates that the DAG received the NDA from DOS on August 7, 2018. DAG reviewed and signed the NDA to DOS on August 15, 2018, or eight days later. DOS did not provide the data until an additional 56 days passed on October 10, 2018. Therefore, we disagree with DOS that the delay was due to the NDA.

DOS expressed concerns about not receiving extensions to investigate the exceptions prior to release of the report and that the deadline for their response would be prior to Election Day. DOS, however, agreed to the response timeline prior to DAG providing management the draft report. Additionally, DAG immediately agreed to an additional one-week extension requested by DOS upon their receipt of the draft report. Therefore, DOS management was fully aware and agreed that its response would be prior to the election. Further, throughout the audit DAG agreed to numerous extensions to the sole benefit of DOS such that the release of this report has been

delayed nearly a full year after the original release date agreed upon in the Interagency Agreement. If we had agreed to further extensions to the audit timeline, there would be insufficient time for the counties to investigate the potential data exceptions and correct them prior to the next Presidential general election. As it is, the counties have less than one year until that election to obtain the exceptions, investigate them, and correct the records, if necessary. We recommend DOS provide the detailed exceptions to the counties as soon as possible to give them more time to validate their data or make corrections as appropriate.

Concerning potential DOB inaccuracies identified by DAG, DOS maintained that some of the records that were identified as erroneous DOB are in fact correct. For instance, they noted that county election officials must comply with the Sexual Violence Victim Address Confidentiality Act that requires county election officials to list a generic DOB in the SURE system to safeguard personal information. DOS informed us of its use of generic DOB when transitioning to the current SURE system; however, it did not provide us any information during the audit regarding the need to use generic DOB to comply with requirements to maintain confidential information of the victims of sexual violence. Therefore, the findings and results of our DOB inaccuracies analysis will remain as written in the revised draft report.

Finding 3 - The Department of State must implement leading information technology security practices and information technology general controls to protect the SURE system and ensure the reliability of voter registration records.

DOS contends that the SURE Advisory Board performs the functions of an oversight body. The Board's charter, however, only allows it to function in an advisory capacity rather than as an IT governance body responsible for ensuring effective IT management. Further, in light of Executive Order 2016-06, OA/OIT and the Employment, Banking, and Revenue (EBR) Delivery Center should have direct representation on the IT governance oversight body.[121] DOS' response notes that the Chief Information Officer for the EBR Delivery Center holds regular steering committee meetings with DOS; however, this committee does not have a formal charter. An IT governance oversight body's charter should include all the key areas of IT governance such as value delivery, strategic alignment, resource management, risk management, and performance management.[122]

We are encouraged by DOS' efforts to modify its vendor's IT support and maintenance services as described in its management response. We are also pleased that our audit results in this area have been helpful.

[121] Executive Order 2016-06, *Enterprise information Technology Governance*, dated April 18, 2016.
[122] Information Systems Audit and Control Association (ISACA). http://www.isaca.org/chapters9/Accra/Events/Documents/ISACA%20Presentation%20-%20IT%20Governance%20V5.pdf. (accessed December 5, 2019).

Although DOS states in its response that vendors are already monitored in accordance with Management Directive 325.13, DOS provided no evidence that this monitoring was actually performed. As stewards of election infrastructure, DOS cannot simply rely on other agencies and their vendors to ensure voter data is secure. We continue to recommend that DOS: (1) ensure agreements with other agencies require that vendors comply with policy; (2) monitor System and Organization Control reports of all vendors key to election infrastructure (EI); and (3) coordinate with PennDOT and OA/OIT to ensure their vendor oversight practices contribute to EI security.

We are pleased that DOS is updating its *Equipment Use Policy* and is planning to have all appropriate SURE users sign the updated policy. We found, however, that the section of the policy on the use of county-owned equipment to be less strongly worded than other sections of the policy and continue to recommend that DOS revise the policy to clearly address the risks of connecting county-owned equipment to SURE. We agree that instituting the use of a form to formalize county configuration requests and organizing county-level policies will help to encourage compliance.

Finding 4 - Voter record information is inaccurate due to weaknesses in the voter registration application process and the maintenance of voter records in the SURE system.

Although DOS strongly disagrees that there are significant weaknesses in the voter registration process, DOS agreed that edit checks are warranted. Edit checks help to ensure the accuracy of data obtained during the voter registration process. DOS further states that it has already implemented some of the recommendations to improve the application process and intends to do a thorough data analysis prior to moving to a new system so that they are starting with the most accurate data possible. We are confused as to why DOS would state that it disagrees that there are significant weaknesses but then also states that they have made and intend to make additional improvements to the process.

DOS disagrees with the recommendation related to rejecting voter registration applications in a pending status for non-match of information. DAG's recommendation, however, was for DOS to determine if it can direct the counties to review their pending applications and process them (either approve or reject), and to establish a maximum amount of time in which an application can remain in pending status before the county either approves or rejects the application. The recommendation did not indicate that applications pending due to a non-match of information be rejected. It is DAG's stance that an application that has been in pending status for months or even years is a disservice to the applicant. Long-term pending applications should be cleaned up prior to migrating to the new system so not to carry unneeded/outdated data into the new system.

Regarding the recommendations made for the remaining areas in *Finding 4*, we are pleased to see that DOS will take them under advisement. We hope that ultimately DOS implements our recommendations to ensure improvements to its processes.

Finding 5 - Incorporating edit checks and other improvements into the design of the replacement system for SURE will reduce data errors and improve accuracy.

Although DOS indicated that the SURE system is designed to automatically associate the proper voter registration record cancellation reason with the source of the cancellation transaction, this does not address the issue we identified for voter registrations that may have been improperly cancelled within 90 days of an election. We welcome DOS' response that it intends to review the data analysis in the coming weeks and will follow up with counties as necessary. A significant purpose of our review was to identify potential data errors and share that information with DOS and the counties so that they could investigate and correct erroneous information, if applicable.

Finding 6 - A combination of a lack of cooperation by certain county election offices and PennDOT, as well as source documents not being available for seventy percent of our test sample, resulted in our inability to form any conclusions as to the accuracy of the entire population of voter records maintained in the SURE system.

We have already addressed in the *Finding 1* portion of this section the issues that DOS takes in its response regarding the lack of source documentation, and are pleased that DOS intends to take our recommendations under advisement regarding the retention of records policy and scanning documents.

Finding 7 - The Department of State should update current job aids and develop additional job aids and guidance to address issues such as duplicate voter records, records of potentially deceased voters on the voter rolls, pending applications, and records retention.

We are most pleased to see that DOS agrees with our recommendations and/or plans to review the job aids and discuss our recommendations with appropriate individuals regarding implementation.

Appendix D

Regarding DOS' comments about the Commonwealth's voter registration process addressed in *Appendix D* of our report, DOS took issue with DAG's statement that DOS and the counties must continue to address the concern with the PennDOT Motor Voter system that allowed ineligible individuals to register to vote. We understand that DOS has shared the information with the counties to take further action; however, we emphasize the vital importance that DOS should continue to follow through and work with the counties to ensure that this work is performed for those voters identified as potentially ineligible voters.

Appendix A Objectives, Scope, and Methodology

The Department of the Auditor General (DAG) conducted this performance audit pursuant to an Interagency Agreement (agreement) entered into by and between the Department of State (DOS) and DAG to assess DOS' administration of the Statewide Uniform Registry of Electors (SURE).[123] We also conducted this audit under the authority of Sections 402 and 403 of The Fiscal Code, 72 P.S. §§ 402 and 403.

We conducted this audit in accordance with applicable *Government Auditing Standards*, issued by the Comptroller General of the United States, except for certain applicable requirements that were not followed. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.[124] Significant scope limitations caused by a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure to provide the necessary information, affected our ability to obtain sufficient, appropriate evidence to fully achieve all of the audit objectives as described below and within *Finding 1*.

Objectives

The agreement specifies the following audit objectives:

1. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law. [See *Findings 2, 4, 5, 6*]
2. Evaluation of the process for input and maintenance of voter registration records. [See *Finding 4*]
3. Review of security protocols of the SURE system. [See *Findings 1, 3*]
4. Review of the efficiency and accuracy of the SURE system. [See *Finding 5*]
5. Review of the internal controls, methodology for internal audits and internal audits review process. [See *Finding 4*]
6. Review of the external controls, methodology for external audits and external audits review process. [See *Finding 1*]
7. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance. [See *Finding 7*]

[123] See *Appendix B* for a copy of the Interagency Agreement.
[124] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient, appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to obtaining an understanding of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.

8. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General. [No Findings]

Scope

This performance audit covered the period January 1, 2016 through April 16, 2019, unless otherwise noted, with updates through the report date.

DOS management is responsible for establishing and maintaining effective internal controls to provide reasonable assurance of compliance with applicable laws and regulations, contracts, grant agreements, and administrative policies and procedures. In conducting our audit, we obtained an understanding of DOS' internal controls, including information systems controls, where possible given the scope limitations placed on the audit that we considered to be significant within the context of our audit objectives.

For those internal controls that we determined to be significant within the context of our audit objectives, including information system controls where possible given the scope limitations, we also assessed the effectiveness of the design and implementation of those controls as discussed in the *Methodology* section that follows. Deficiencies in internal controls that we identified during the conduct of our audit and determined to be significant within the context of our audit objectives are included within the respective audit findings in this report. In addition, during our procedures we identified areas of potential improvement related to computer security, information technology general controls, and interface controls that we have specifically excluded from this report because of the sensitive nature of this information. These conditions and our recommendations have been included in a separate, confidential communication to DOS management.

Government Auditing Standards require that we consider information systems controls "…to obtain sufficient, appropriate evidence to support the audit findings and conclusions."[125] This process also involves determining whether the data that supports the audit objectives is reliable. In addition, Publication GAO-09-680G, *Assessing the Reliability of Computer-Processed Data*, provides guidance for evaluating data using various tests of sufficiency and appropriateness when the data are integral to the audit objective(s).[126] We attempted, where possible despite the scope limitations, to comply with standards concerning the reliability of computer-processed data. See our assessment in the *Data Reliability* section that follows.

[125] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraphs 6.23 through 6.27.
[126] U.S. Government Accountability Office. *Assessing the Reliability of Computer-Processed Data*, July 2009.

Scope Limitations

Due to a lack of cooperation from DOS, the Pennsylvania Department of Transportation (PennDOT), and certain county election offices (counties), as well as a failure to provide the necessary information needed to satisfy three of eight audit objectives, it became evident that DAG would not be able to perform the audit in accordance with certain applicable standards in *Government Auditing Standards*, which is issued by the U.S. Government Accountability Office. The standards in question include obtaining sufficient, appropriate evidence; evaluating the design and operating effectiveness of information systems controls; and reviewing previous audits and attestation engagements significant within the context of the audit objectives.[127] DAG issued a modified *Government Auditing Standards* compliance statement for this audit to account for the significant scope limitations that resulted from DOS' refusal to provide access to documentation and data required to complete the audit. See these scope limitations addressed in detail in *Finding 1* of this report and summarized below.

Due to a lack of source documentation to support voter registration applications (applications) filed online and through paper forms and PennDOT's refusal to provide access to source documentation for Motor Voter registration applications, we were unable to determine if the records within the SURE system are accurate. We were, therefore, unable to satisfy our audit objective to perform a sufficient assessment of whether records maintained within the SURE system are accurate and in accordance with HAVA and Pennsylvania law (Objective 1).

Further, DOS' refusal to provide sufficient access to key documentation related to the security and operation of the SURE system significantly limited our ability to perform our audit procedures. The following list identifies the key documents/information that were not provided (items 1, 2, and 5) or were heavily redacted (items 3 and 4):

1. Contents of external security assessment reports issued by the United States Department of Homeland Security (Homeland Security), as well as reports issued by private firms contracted to assess security.

2. Systems and Organization Control reports detailing the security practices in place at outside vendors key to the security and operation of the SURE system.[128]

3. Detailed information on system configuration and implementation of cybersecurity policies.

[127] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Standards related to obtaining sufficient appropriate evidence are included in Paragraphs 6.56 through 6.72, standards related to obtaining an understanding of information system controls are included in Paragraphs 6.23 through 6.27, and standards related to review of previous audits and attestation engagements are included in Paragraph 6.36.
[128] Systems and Organization Control (SOC) reports are reports on a service organization's controls by an independent auditor.

4. The formal results and corrective action plans from the 2018 test of the emergency recovery system.

5. Documentation of significant IT controls and system interfaces.

Without these critical documents listed above, we were unable to satisfy our audit objective to review the security protocols of the SURE system (Objective 3). In addition, we were unable to comply with *Government Auditing Standards*, which requires auditors to evaluate the design and operating effectiveness of information systems controls and review previous audits and assessments significant within the context of our audit objectives.[129] DOS' refusal to provide these documents resulted in our inability to provide a conclusion regarding the security of the SURE system. Additionally, as a result of not being provided access to the contents of the external security assessment reports, we were not able to determine what these assessments included and therefore, have no assurance that the assessments covered all of the various layers of security protecting the SURE system (Objective 6).

Methodology

Items selected for testing within this audit were based on various methods including statistical sampling and auditor's professional judgment. Due to the scope limitations regarding our testing of the statistical sample, we were not able to project results to the corresponding population. For our other test selections using professional judgment, the results of our testing also cannot be projected to, and are not representative of, the corresponding populations.

To address the audit objectives, we performed the following procedures:

- Interviewed and corresponded with individuals from the following offices to gain an understanding of SURE and security protocols of the SURE system, the individuals involved in managing, maintaining, and monitoring work performed in SURE, the assistance provided when requested by those utilizing SURE, and work performed regarding the issue with non-citizens that had the ability to register to vote at PennDOT photo license centers:

    - DOS management, staff, information technology officials, and legal counsel
    - SURE Help Desk staff
    - County election offices (county) management and staff
    - PennDOT management, staff, and legal counsel

[129] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.23 through 6.27.

- Reviewed the following laws, regulations, contracts, and written policies and procedures applicable to SURE:

  - Help America Vote Act of 2002, 52 U.S.C. § 21083 regarding the requirement to implement a computerized statewide voter registration list, minimum standards for the accuracy of voter registration records and requirements regarding performing list maintenance on a regular basis to remove ineligible voters.
  - National Voter Registration Act, 52 U.S.C. § 20507 regarding the federal requirements to register to vote.
  - Pennsylvania Voter Registration Law (Act 3 of 2002), 25 Pa.C.S. Chapters 12 and 19 regarding the implementation of HAVA in state law.
  - 4 Pa. Code Chapter 183 regarding record retention guidance on applications.
  - *County Records Manual* issued by the Pennsylvania Historical and Museum Commission regarding record retention guidance on applications.
  - SURE job aids, created and distributed by DOS to the counties, that provide guidance regarding the current process established in the SURE system. In particular those processes regarding processing applications, including pending applications, and list maintenance performed on voter registration records.
  - DOS' Memoranda of Understanding with both PennDOT and the Department of Health (DOH) for systems that interface with the SURE system.
  - DOS' contracts with vendors responsible for network administration, driver's license and Motor Voter processes, administration of the SURE Help Desk, and the staff augmentation vendor.

- Reviewed news articles related to election threats such as the Russian involvement in the 2016 presidential election.

- Attended SURE training provided by DOS to gain an overview of how SURE works, what functionality SURE includes and how the counties use SURE to process applications, conduct list maintenance activities, and print poll books.

- Reviewed a list of SURE training DOS provided to counties, both prior to and during the audit period, to determine which counties requested and received training in addition to the initial training provided during the implementation of the SURE system.

- Judgmentally selected and visited seven county election offices between July 11, 2018 and September 11, 2018, to gain an understanding of how the counties process applications in SURE, including performing steps to review: the counties' procedures to detect duplicate registrations; the counties' procedures to conduct the HAVA check, and correspondence mailed to applicants requesting information required to complete the processing of applications. Two of the seven counties visited were at the recommendation

of DOS and the remaining five counties were selected in order to gain variety in geographic location and the number of voter registrations.

- Sent a survey (See copy in *Appendix H*) to all 67 counties in Pennsylvania (including the seven visited) to obtain similar information as gained during the visits such as processing information in SURE, equipment utilized, and security protocols. A total of 65 of the 67 counties provided responses to our questions either during the on-site visit interviews or by returning the survey; however, not all of the counties responded to every question in the survey.

- Included technical experts from the DAG's Bureau of Information Technology Audits as part of the audit team for data analysis and information systems assessment pertinent to our audit objectives.

- Consulted with a network administration expert from DAG's Office of Information Technology and Support Services for specialized network and cybersecurity knowledge.

- Consulted with cybersecurity audit experts from other state auditor offices on applicable cybersecurity control frameworks and auditor access to outside security assessments of critical infrastructure.

- Reviewed and analyzed redacted network and system diagrams of the SURE system in an attempt to obtain a thorough understanding of the various environments.

- Reviewed and analyzed redacted documents regarding the software, hardware, and operating systems supporting the SURE system.

- Reviewed and analyzed functional specifications documents for interfaces, where provided, and assessed the impact of interfaces between SURE and other systems.

- Reviewed DOS organizational charts with DOS officials to gain an understanding of the management structure.

- Reviewed the following reports from other organizations on voting system security and voter registration security to identify relevant security protocols and issues:

    - Brennan Center for Justice. *Defending Elections: Federal Funding Needs for State Election Security,* July 18, 2019.
    - Center for American Progress. *Election Security in All 50 States: Defending America's Elections*, February 12, 2018.

- U.S. Department of Justice. *Report on the Investigation into Russian Interference in the 2016 Presidential Election (also known as the Mueller Report)*, March 31, 2019.
- The Heritage Foundation. *A Sampling of Election Fraud Cases from Across the Country*. April 2017.
- State of Minnesota, Office of the Legislative Auditor. *Voter Registration: 2018 Evaluation Report*. March 8, 2018.
- United States Election Assistance Commission (EAC). *2014 Statutory Overview*, January 2015.
- Press Release of Select Committee on Intelligence, United States Senate, *Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security*. Richard Burr, Mark Warner, Susan Collins, Martin Heinrich, James Lankford. May 8, 2019.
- Report of the Select Committee on Intelligence, United States Senate, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. Released July 25, 2019.
- The University of Pittsburgh Institute for Cyber Law, Policy and Security. *The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations*, January 4, 2019.
- The National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*, September 6, 2018.
- Technology Science. *Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections*, September 06, 2017.

- Received a signed affidavit from the Chief Information Security Officer (CISO) of the Employment, Banking, and Revenue (EBR) Delivery Center of the Office of Administration Office of Information Technology (OA/OIT) describing certain controls in place over the SURE system.

- Interviewed the CISO of the EBR Delivery Center for a verbal briefing on the contents of external security assessment reports issued by the United States Department of Homeland Security and reports issued by private firms contracted to assess security of the SURE system.

- Attended a presentation by the CISO of the Commonwealth providing an overview of OA/OIT's implementation of the National Institute of Standards and Technology Cybersecurity Framework.

- Received letters through DOS from two vendors summarizing security assessments performed on election systems.

- Reviewed working papers testing information technology general controls compiled in prior audits of the Commonwealth's Comprehensive Annual Financial Report.

- Reviewed a Service Organization Control (SOC) report for one vendor significant to the SURE system and attempted to review SOC reports for other relevant vendors.

- Reviewed the following policies governing internal controls, IT management, procurement, IT security, and cybersecurity issued by OA/OIT and DOS:

    - Commonwealth of Pennsylvania Information Technology Policy (ITP) ITP-SEC000 – *Information Security Policy*. May 2016.
    - ITP-SEC007 – *Minimum Standards for IDs, Passwords, and Multi-Factor Authentication*. March 1, 2006.
    - ITP-SEC015 – *Data Cleansing Policy*. May 1, 2013.
    - ITP-SEC019 – *Policy and Procedures for Protecting Commonwealth Electronic Data*. November 16, 2007.
    - ITP-SEC020 – *Encryption Standards for Data at Rest*. August 17, 2007.
    - ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*, April 19, 2007.
    - ITP-SEC024 – *IT Security Incident Reporting Policy*. August 2, 2012
    - ITP-SEC025 – *Proper Use and Disclosure of Personally Identifiable Information*. March 19, 2010.
    - ITP-SEC031 – *Encryption Standards for Data in Transit*. August 17, 2007.
    - Commonwealth of Pennsylvania Information Technology Operations Document (OPD) OPD-SEC007A – *Configurations for IDs, Passwords, and Multi- Factor Authentication*. March 1, 2006.
    - Commonwealth of Pennsylvania Management Directive (MD) MD-205.34 – *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*. Amended January 22, 2016.
    - MD-325.12 – *Standards for Internal Control for Commonwealth Agencies*. Effective July 1, 2015.
    - MD-325.13 – *Service Organization Controls*. Effective November 22, 2017.
    - MD-535.9 – *Physical and Information Security Awareness Training*. October 3, 2006.
    - Commonwealth of Pennsylvania *Information Security Incident Response Procedures* (IRP) V2.11. November 11, 2008.
    - DOS Bureau of Election Security and Technology, Bureau of Elections and Notaries, Bureau of Campaign Finance and Civic Engagement. *Continuity of Operations Plan.* January 02, 2019.
    - DOS *Guidance on Electronic Voting System Preparation and Security*. September 2016.
    - DOS *Policy on Election System Security Measures*, Version 1.1, issued April 23, 2019.

  - DOS *SURE Equipment Use Policy*. September 12, 2003, updated February 29, 2012.

- Reviewed the redacted results of the 2018 test of the SURE Emergency Recovery System conducted by DOS management.

- Inquired of DOS management about the applicability of Commonwealth IT policies to county election offices and IT personnel.

- Reviewed transcripts of the U.S. Senate Select Committee on Intelligence hearing on Election Security, March 21, 2018, the Pennsylvania House of Representatives State Government Committee hearing on Election Integrity and Reforms, October 15, 2018, and the U.S. House of Representatives Committee on Homeland Security hearing on Building Partnerships to Protect America's Elections, February 13, 2019.

- Reviewed the Center for Internet Security (CIS) *Critical Security Controls*, Version 7.1, the CIS *Handbook for Elections Infrastructure Security*, Version 1.0, dated February 2018, and the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS-CISA) publication entitled *Best Practices for Securing Election Systems*, issued May 21, 2019, to assist in developing our audit approach for testing cybersecurity controls.

- On February 25, 2019, the Auditor General traveled to Washington D.C. to meet with representatives of the Department of Homeland Security (Homeland Security) to discuss protocol regarding access to security reports issued by Homeland Security.

- Attempted to perform tests of design of information technology general controls in place over the SURE system in the following baseline control areas:
  - Access management
  - Change management (i.e., configuration management)
  - Segregation of duties
  - Service delivery
  - Business continuity/Disaster recovery.

- Reviewed the SURE database schema, data dictionary, and other database documentation to assist in documenting an understanding of the database and requesting data.

- Obtained from DOS electronic data files of all currently registered voters as of October 9, 2018 (referred to as the Voter Table) and the electronic history of all changes to voter records, such as changes to the voter's name and address that were recorded from January 1, 2016 through October 9, 2018 (referred to as the Application Table). We also obtained copies of each county's Pennsylvania Full Voter Export List as of October 9, 2018, from

the SURE system available to the public through the Department of State (DOS) website (referred to as the Full Voter Export Table).

- Obtained death data from the DOH of deaths recorded in Pennsylvania from October 2010 through October 2018 to compare to voter registration data as of October 9, 2018 to determine if any of the deceased remain as registered voters in SURE.

- Obtained the Social Security Administration's Death Master File of deaths as of August 2010 to determine if any of the deceased are still listed as registered voters in SURE.

- Using data analysis on the Voter Table we performed the following:

  - Tested for duplicate driver's license numbers as well as tests for other potential duplicate records based on first name, last name, date of birth (DOB), and/or last four digits of the Social Security number (SSN).

  - Searched for voters who were 100 years old or older as of October 9, 2019 and for voter registration dates that were prior to the voter's DOB. We then reviewed the U.S. Census Report entitled, *Centenarians:2010*, to compare against the numbers of voter records with dates of birth indicating the voter may be 100 years of age or older.

  - Compared the voter records to the DOH death data based on first name, last name, DOB, and/or the last four digits of the SSN.

  - Compared the voter records to the Social Security Death Master File data as of August 2010 based on first name, last name, DOB, last four digits of SSN, and street name. No additional potentially deceased voters were identified from this data matching procedure.

  - Reviewed voter records associated with potential duplicates or potential deceased voters to determine if votes were cast more than once per record or after the deceased date, as applicable. We did not believe our evidence was sufficient to report in a finding but did report our results to DOS to further investigate.

  - Determined the number of voter records remaining in active status despite having no activity for five or more years.

  - Determined the number of inactive voter records that should have been cancelled after failure to vote in the following two federal general elections.

- Using data analysis on the Application Table, we determined the following:

  - Whether list maintenance activities were being performed by each county and whether voter records were being cancelled for list maintenance activities within 90 days of the 2016 general election.

  - The number of pending applications and the length of time the applications remained in pending status.

- Using data analysis, we evaluated the design and operating effectiveness of application controls in place to prevent and/or detect: duplicate voter records, inaccurate dates of birth, inaccurate registration dates, potentially deceased voters, as well as controls to prevent inappropriate cancellation of voter records within 90 days of an election, controls to ensure residential addresses are within Pennsylvania, and controls to ensure the street name field does not include the street number.

- Judgmentally selected voter records and traced them to the SURE portal in order to investigate and analyze the following:

  - Information that appeared to be different among the Voter Table, the Full Voter Export Table, and the Application Table.

  - Pending records that appeared to have been replaced by a newer, approved voter application.

  - Records where it appeared that the DOB had been changed.

- Selected a random statistical sample, based on a confidence level of 98 percent and a tolerable error rate of two percent, of 196 voters from the total population of 8,567,700 voters registered in SURE as of October 9, 2018 with the intent of reviewing source documents to confirm the accuracy of the following information maintained in SURE for the 196 voters:

  - Full name (first, last, and middle name or initial, if included)
  - Address
  - DOB
  - Last four digits of the SSN (if included)
  - Last four digits of the Pennsylvania driver's license number or Pennsylvania identification number (if included)
  - Date registered
  - Party affiliation

We also planned to verify that each record had a signature image in the SURE system.

Source documents included applications or other documents provided by voters to update their voter record and were submitted by the voter either through a paper application, the Motor Voter process at Pennsylvania driver's license centers, or DOS' online application.

- Reviewed examples of emails sent from the Help Desk to DOS management regarding the progress of each county for specific tasks, such as list maintenance activities and poll book printing.

- Performed procedures to determine if list maintenance activities were performed by the counties such as the following:

  - Reviewed records in the Application and Voter Tables to determine if each county recorded list maintenance codes indicating that list maintenance activities had been performed.
  - Observed, during county visits, county staff processing documents from voters in response to list maintenance correspondence sent to them by the county.
  - Observed during testing of 196 voter's records that records had been updated as a result of information provided by voters in response to list maintenance procedures performed by the county.

- Reviewed a redacted November 2018 Election Support Plan that includes tasks that must be completed leading up to and after Election Day. Tasks include poll book printing by the counties, certification of voter registration numbers, and certification of the results following Election Day.

- Reviewed the Electronic Registration Information Center's (ERIC) website for information regarding when it was created, accomplishments since its inception, the member states, the cost of being a member, as well as what ERIC provides to its members.

- Reviewed examples of the letters sent by DOS to those identified by a tenured Associate Professor of Political Science hired by DOS as potential non-citizens that were not eligible to be registered voters. The letters included 7,702 dated April 27, 2018; 11,198 dated June 12, 2018; and 8,707 dated June 29, 2018.

- Reviewed documents from DOS regarding actions taken by DOS resulting from the responses received to the letters mailed to those identified as potential non-citizens.

- Reviewed screen shots of the Motor Voter process that was in place when non-citizens were permitted to register to vote.

- Reviewed screen shots of the Motor Voter process after the non-citizen issue was corrected by PennDOT, in conjunction with DOS.

- Visited a PennDOT Photo License Center to observe scenarios where a customer, with their camera card, came into the license center to obtain a new driver's license or renew their existing driver's license. The scenarios included:

    - Citizen either over 18 years of age or will be 18 by the date of the next election
    - Non-citizen of any age
    - Naturalized citizen over the age of 18

- Reviewed U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019, to determine funding provided to states to financially help implement the requirements of HAVA.

- Reviewed the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date" to determine expenditures made during fiscal years 2002 through 2013 from the federal funds received to improve the administration of federal elections.

Data Reliability

Government Auditing Standards requires us to assess the sufficiency and appropriateness of computer-processed information that we used to support our findings, conclusions, and/or recommendations. The assessment of the sufficiency and appropriateness of computer-processed information includes considerations regarding the completeness and accuracy of the data for the intended purposes.[130]

- To assess the completeness and accuracy of the data files from the SURE system of 1) all currently registered voters (the Voter Table), 2) the history of all of the changes made to voter records (the Application Table), and 3) the Pennsylvania Full Voter Export List, we conducted audit procedures as follows:

    - Obtained a management representation letter from DOS management confirming that the data provided to us had not been altered and was a complete and accurate duplication of the data from its original source.

[130] U.S. Government Accountability Office. *Government Auditing Standards*. 2011 Revision. Paragraph 6.66.

- Compared record counts to DOS' unaudited annual report of voter statistics, *The Administration of Voter Registration in Pennsylvania: Report to the General Assembly*, submitted by DOS for the calendar year ended December 31, 2017 sent to the General Assembly in June of 2018 to determine the completeness of the information provided. A variance of 1.3% was noted but determined to be reasonable given the timing differences between the report date and receipt of the data.

- Compared data among the three tables obtained from SURE to determine whether the data was accurate and if records were missing. Variances were investigated and ultimately we determined the data to be internally consistent.

- Using data analysis, compared total voter statistics per the data file of all currently registered voters as of October 9, 2018, to the unaudited annual report of voter statistics, *The Administration of Voter Registration in Pennsylvania: Report to the General Assembly*, submitted by DOS for the calendar year ended December 31, 2018, to test the voter data for completeness.

- Obtained reports from PennDOT's Motor Voter program and compared those records to application data within the SURE system to determine completeness.

- Obtained reports from DOS of initial voter application records submitted through PennDOT's Motor Voter system between January 1, 2016 and October 9, 2018, and compared them to the initial applications recorded as received from PennDOT in SURE. Although variances were noted, we found the count of applications sent and recorded to be substantially accurate.

- Attempted to evaluate the design and operating effectiveness of information technology general controls. DOS, however, refused to provide access to the contents of external security reports and other documents needed to perform the evaluation. See scope limitation above and in *Finding 1 (Scope Limitation A)*.

- Used obituaries to confirm a judgmental selection of potentially deceased individuals' first and last name, date of death, and city of residence. We also confirmed the DOB and middle initial if noted in the obituary. These additional tests were performed to validate the reliability of the match between DOH data and SURE data.

- Used Google Maps to confirm for a judgmental selection of records that the street address was within Pennsylvania in order to confirm the accuracy of the *State* field in the voter record and to provide additional evidence as to the eligibility of the voter.

- Randomly selected a sample of 196 records from the 8,567,700 registered voters in Pennsylvania and traced the information back to the source documentation maintained at the county election offices. We were unable to perform these audit procedures for 138 sampled items due to lack of cooperation from the counties, lack of cooperation from PADOT to provide information from the Motor Voter applications, lack of auditable information for online applications, and lack of sufficient record retention requirements and guidance. See the description of the scope limitation above and in *Finding 1 (Scope Limitation B)*.

Based on the procedures we were able to perform, as well as the procedures we were not able to perform due to scope limitations, in accordance with *Government Auditing Standards*, we concluded that the voter registration data extracted from the SURE system had significant limitations. However, due to the close approximation to independently produced reports issued by DOS and the consistency of the data among the three tables, we determined the data to be sufficiently reliable, with significant limitations, to support our findings and recommendations as noted throughout our report.

As noted in *Finding 4* in the report, we did not perform tests to validate the reliability of the "date last voted" field within the voter table. According to SURE job aids, the "date last voted" field is entered into SURE when poll workers scan the bar code (found beside the voter's signature in the poll book) after each election. While the process described appeared reasonable to capture voting dates, since we did not perform tests of the accuracy of the "date last voted" field, we determined this data field to be data of undetermined reliability. The data, however, was the best data available and although this determination may affect the precision of the numbers presented, as noted in *Finding 4*, there is sufficient evidence to support our findings and conclusions that DOS should work with the counties to investigate instances of potentially inactive voters who had not voted in the last two federal general elections and whose voter records may need to be cancelled.

- We did not perform procedures to assess the completeness and accuracy of the data of deceased individuals from the Pennsylvania Department of Health, the data from the Social Security Death Master file, and data from the US Census Bureau. We determined this data to be data of undetermined reliability, as noted in *Finding 2* of this report. This data was the best data available, however, and although this determination may affect the precision of the numbers presented of potentially deceased individuals and those over the age of 100, as noted in *Finding 2*, there is sufficient evidence to support our findings and conclusions.

- We did not perform procedures to assess the completeness and accuracy of the number of letters that DOS sent to voters identified as having questionable voter registration eligibility and the actions that subsequently occurred with each of the voters identified. We determined this data to be data of undetermined reliability, as noted in *Appendix D* of

this report. This data was the best data available, however, and although this determination may affect the precision of the number of individuals identified as potentially ineligible to vote, as noted in *Appendix D*, there is sufficient evidence to support the information noted in *Appendix D*.

Appendix B — Interagency Agreement Between the Department of State and the Department of the Auditor General

On May 15, 2018, the Department of the Auditor General (DAG) entered into an Interagency Agreement (agreement) with the Department of State (DOS) to perform an audit of DOS' Statewide Uniform Registry of Electors. The originally agreed upon date to provide DOS with the audit report was January 31, 2019. Due to delays by DOS in providing DAG requested audit information, the agreement was amended to:

- Extend the report release date to **July 31, 2019.**
- Further extend the report release date to **September 27, 2019**.
- Further extend again the report release date to **November 29, 2019.**

The following is a copy of the original agreement between DAG and DOS:

Doc. No. 2018-IA-002

INTERAGENCY AGREEMENT

This Interagency Agreement ("Agreement") is entered into by and between the Department of State ("DOS") and the Pennsylvania Department of the Auditor General ("Auditor General") for an audit of DOS' Statewide Uniform Registry of Electors ("SURE").

Sections 501 and 502 of *The Administrative Code of 1929* (71 P.S. §§181 and 182) require Commonwealth departments, boards, commissions, and agencies to coordinate their work and activities with other Commonwealth departments and agencies.

DOS, through its Bureau of Commissions, Elections and Legislation ("BCEL"), oversees the administration of the Commonwealth's electoral process which includes voter registration. To ensure a complete and accurate statewide voter registration system, DOS, pursuant to the dictates of the Help America Vote Act ("HAVA"), 52 U.S.C. § 21083(a), and the Pennsylvania voter registration law, 25 Pa.C.S. § 1201(3), administers the SURE system. Part of DOS' responsibility under the law involves maintenance of the database which ensures that the voter registration rolls are accurate and up to date. *Id.* § 21083(b).

The Auditor General is the chief fiscal watchdog of the Commonwealth. The Auditor General's mission is to serve the people of Pennsylvania by improving government accountability, transparency, and the effective use of taxpayer dollars. The Agency is responsible for using audits to gauge whether government programs and activities are meeting stated goals and objectives and to ensure that all state money is spent legally and properly.

DOS has requested that the Auditor General perform an audit of the SURE system to assess its accuracy, operability, and efficiency and DOS has agreed to provide access to the SURE system for the purposes of this audit to the Auditor General under the terms and conditions of this Agreement.

The parties, intending to be legally bound, agree as follows:

1. DOS Responsibilities. DOS shall:
   a. cooperate with the Auditor General's requests involving the proposed audit;
   b. to the extent feasible, provide the Auditor General with read-only, point in time access to the SURE system data for the purpose of conducting the proposed audit;
   c. provide training and ongoing technical assistance to the Auditor General regarding DOS methods of accessing and updating records in the SURE system.

d. pay the Auditor General up to One Hundred Thousand Dollars ($100,000.00) for the expenses associated with conducting the proposed audit. Monthly invoices shall be submitted by the Auditor General to DOS by the 15th day of the following month.

2. Auditor General Responsibilities.

a. The Auditor General shall conduct an audit of the SURE system and provide a report to DOS no later than January 31, 2019. The report shall include all of the following:

i. Assessment of whether records maintained within the SURE system are accurate and in accordance with the Help America Vote Act (HAVA) and Pennsylvania law;

ii. Evaluation of the process for input and maintenance of voter registration records;

iii. Review of security protocols of the SURE system;

iv. Review of the efficiency and accuracy of the SURE system;

v. Review of the internal controls, methodology for internal audits and internal audits review process;

vi. Review of the external controls, methodology for external audits and external audits review process;

vii. Review of the methodology for the issuance of directives and guidance to the counties by DOS regarding voter registration and list maintenance; and

viii. Any other relevant information or recommendations related to the accuracy, operability, and efficiency of the SURE system, as determined by the Auditor General.

b. Audit progression: To the extent feasible, the Auditor General will meet and confer with DOS to provide DOS quarterly audit updates.

c. Audit period: The audit period will be January 1, 2016, through the end of the audit procedures. This will include auditing the processes that were in place for that time period. This will also include testing the accuracy of the data as of a

point-in-time that has not been determined, but preferred to be as current as possible. The Auditor General will ensure that the data accuracy is tested from several sources covering different time periods that will be finalized during the audit.

d. Report information: The information contained with the report shall not include data, documentation, configuration representations, product or supplier names, network addresses, or other critical information that may interfere or jeopardize the security, privacy, or integrity of the SURE system or any of the Commonwealth's or counties' networks or systems. The Auditor General shall coordinate and work in conjunction with DOS to determine what is to be treated as restricted content prior to issuance of the final report.

3. Data Security.

a. The Auditor General and DOS will comply with all federal and state laws and regulations pertaining to any data exchanged pursuant to this Agreement.

b. The Auditor General and DOS will ensure that all data exchanged pursuant to this Agreement is secure, privacy is protected and integrity is maintained as required by OA/OIT requirements.

c. The Auditor General will destroy all data that has been provided by DOS once the data is no longer needed.

d. Only authorized personnel in the Auditor General's Office and DOS with a business need will have access to the data exchanged pursuant to this Agreement.

4. General Provisions.

a. Term. This Agreement will become effective as of the Effective Date, as defined below, and will remain in effect until the final audit report is delivered and accepted by the parties on or before January 31, 2019, unless earlier terminated by either party in accordance with Paragraph 4(c) of this Agreement.

b. Effective Date. The Effective Date of this Agreement shall be May 15, 2018, prior to which the Agreement shall be fully executed by both parties and all approvals required by Commonwealth contracting procedures obtained.

c. Termination. Either party may terminate this Agreement for good cause by sending thirty (30) days prior written notice of termination to the other party

d. Amendments and Modifications. No alterations or variations to this Agreement shall be valid unless made in writing and signed by the parties. Amendments to this Agreement shall be accomplished through a formal written document signed by the parties with the same formality as the original Agreement.

e. Full Understanding of the Parties. This Agreement sets forth the full and complete understanding of the Parties.

f. Agency. The employees or agents of each party who are engaged in the performance of this Agreement shall be employees or agents of that party and shall not be considered for any purpose to be employees or agents of the other party.

g. Notice. Any written notice to DOS under this Agreement shall be sufficient if mailed to:

Chief Counsel
Pennsylvania Department of State
401 North Street
Room 306, North Office Building
Harrisburg, PA 17120

Any written notice to the Agency under this Agreement shall be sufficient if mailed to:

Chief Counsel
Department of the Auditor General Finance Building
613 North Street, Room 224
Harrisburg, PA 17120-0018

h. Applicable Law. This Agreement shall be governed by, and interpreted and enforced in accordance with, the laws of the Commonwealth of Pennsylvania and the decisions of the Pennsylvania courts.

i. Disputes. Any dispute arising hereunder shall be submitted to Office of General Counsel for final resolution.

j. Severability. The provisions of this Agreement shall be severable. If any phrase, clause, sentence or provision of this Agreement is declared to be contrary to the Constitution of Pennsylvania or of the United States or of the laws of the Commonwealth, the applicability thereof to any government, agency, person or circumstance is held invalid, the validity of the remainder of this Agreement and the applicability thereof to any government, agency, person or circumstance shall not be affected.

k. Integration. When fully executed by the parties, this Agreement shall be the final and complete Agreement between the parties containing all the terms and conditions agreed on by the parties. All representations, understandings, promises and agreements pertaining to the subject matter of this Agreement made prior to or at the time this Agreement is executed are superseded by this Agreement, unless specifically accepted by any other term or provision of this Agreement. There are no conditions precedent to the performance of this Agreement, except as expressly set forth in this Agreement.

[SIGNATURE PAGE FOLLOWS.]

The parties, through their authorized representatives, have signed this Agreement below.

Robert Torres 5/15/18
Robert Torres Date
Acting Secretary
Department of State

Eugene A. DePasquale 5/14/18
Eugene A. DePasquale Date
Auditor General

APPROVALS AS TO FORM AND LEGALITY:

5/15/18
Office of Chief Counsel Date
Department of State

5-14-18
Office of Chief Counsel Date
Pennsylvania Department of the
Auditor General

Pamela J. Cross 5/16/18
Office of General Counsel Date

5/21/18
Office of Attorney General Date

5/31/2018
Comptroller Operations Date

RECEIVED
2018 MAY 21 PM 3:10
BUREAU OF
FINANCE & OPERATIONS

Appendix C Voter Registration Process

The voter registration process in Pennsylvania is conducted by county election offices (counties) but involves a partnership with the Department of State (DOS). The National Voter Registration Act and Pennsylvania law requires that the Pennsylvania Department of Transportation (PennDOT) provide a voter registration opportunity to its customers. This process is commonly referred to as Motor Voter.[131] The Motor Voter process provides PennDOT customers the opportunity to register to vote, or change their address if they are currently registered to vote, while receiving or renewing their driver's license (DL) or photo identification (ID) card at a PennDOT photo license center, as well as the ability to update their registration in-person and online.

In addition, applicants have the option to register to vote via paper application, online, and for any person that utilizes the services of various government assistance offices, the person is asked if they want to register at the time of application for benefits or re-certification for benefits.[132] A paper application can be obtained online or at the county and returned to the county by mail or in-person once completed. Online applications are managed by DOS and can be accessed by visiting register.votesPA.com.

Regardless of which application method one chooses, the information required to register is the same. The applicant must provide information including their full name, date of birth, residence address, mailing address (if different than residence), and political affiliation. Applicants are also prompted to provide their DL or ID number and/or the last four digits of their Social Security number (SSN) in order to help verify the applicant's identity; however, the county cannot deny an application if the applicant does not provide their DL or ID number or SSN.[133] The applicant must also confirm that they are eligible to register to vote by answering eligibility questions included on the application and signing the application.

Federal and State law establishes eligibility requirements for residents to register to vote.[134] Eligibility criteria include a minimum age requirement of 18 years of age and citizenship of the

[131] 52 U.S.C. § 20504. *See also* 25 Pa.C.S. § 1323.
[132] 25 Pa.C.S. § 1325. Consistent with the NVRA, the offices in Pennsylvania that have been identified as those that "provide public assistance" for voter registration purposes are: Women, Infant and Children Nutrition Clinics; County Assistance Office; Clerk of Orphans' Courts; Children and Youth Agencies; Area Agencies on Aging; Para-Transit providers; Special Education Programs at the 14 state-owned universities; agencies serving people with disabilities and County Mental Health/Intellectual Disabilities offices; and the armed services recruitment centers. *The Administration of Voter Registration in Pennsylvania, 2017 Report to the General Assembly, June 2018*, page 10.
[133] 25 Pa.C.S. § 1328. The Pennsylvania Voter Registration Application includes a box for the applicant to check if they do not have a PA driver's license or a PennDOT identification card or a Social Security number. All first time voters must show identification at the polling place. The approved list of identification documents can be found at http://www.votespa.com.
[134] 52 U.S.C. § 10701 (Enforcement of the 26th Amendment). Note that HAVA has statutory provisions prohibiting certain discriminatory voting acts, such as poll taxes, in Chapter 103. *See also* 25 Pa.C.S. § 1301(a).

United States (U.S.), the Commonwealth of Pennsylvania, and the applicable district. It should be noted, however, that neither state nor federal law require proof of citizenship in order to register to vote, regardless of the method of application. Neither DOS nor the counties conduct a review to confirm the citizenship of an applicant. When an applicant completes a voter registration application, whether on paper, online, through a voter registration drive, or similar method, they are merely asked to sign a declaration (without providing any validation), which states the following:

- I am a United States citizen and will have been a citizen for at least one month on the day of the next election.
- I will be at least 18 years old on the day of the next election.
- I will have lived at the same address in Section 5 [of the application] for at least 30 days before the election.
- I am legally qualified to vote.[135]

The applicant must indicate by checking a box that: "I affirm that this information is true. I understand that this declaration is the same as an affidavit, and, if this information is not true, I can be convicted of perjury, and fined up to $15,000, jailed for up to 7 years, or both."[136] Given that the law ***does not*** require proof that the applicant's declaration/affirmation is valid, it is possible that an ineligible person, including a non-citizen, could apply to register to vote regardless of whether they knew they were violating the law or if it was done unintentionally, as with those that may not fully understand the questions being asked and statements made due to a language barrier.[137] Regardless of the circumstances, as previously reported, there is a potentially substantial criminal penalty for those found to have provided false information.

Requiring applicants to submit proof of citizenship has been attempted in other states and has been met with court challenges. In June 2018, in a matter involving private citizens represented by several public interest organizations on behalf of the League of Women Voters of Kansas against the Kansas Secretary of State, a federal district court judge found that Kansas could not require documentary proof of U.S. citizenship when registering to vote, because such laws

[135] This declaration is provided in Section 11 of the application.
[136] Ibid.; the application also contains the following notice: "PENALTY FOR FALSIFYING DECLARATION WARNING: If a person signs an official registration application knowing a statement declared in the application to be false, makes a false registration, or furnishes false information, the person commits perjury. Perjury is punishable, upon conviction, by a term of imprisonment not exceeding seven years, or a fine not exceeding $15,000, or both, at the discretion of the court. Submitting an application containing false information may also subject a person to other penalties, including loss of the right of suffrage, under state or federal law." This is commonly referred to as "signing under penalty of perjury" and is enforceable under 18 Pa.C.S. § 4902.
[137] At a 2016 hearing, a former DOS election official claimed that a "glitch in the state's driver licensing software 'may inadvertently register' noncitizen immigrants to vote without their knowledge." <https://thehill.com/blogs/blog-briefing-room/news/357143-pa-officials-find-hundreds-of-illegal-ballots-cast-in-state> (accessed April 29, 2019).

violate the constitutional right to vote.[138] The decision, which is currently under appeal, invalidated Kansas' proof-of-citizenship registration law.[139] In the meantime, however, the holding of the case has national implications, including in Pennsylvania.

To date, the Pennsylvania General Assembly has not attempted to require proof of citizenship to register to vote, but did attempt to enact a voter identification (Voter ID) law in 2012.[140] Pennsylvania's Voter ID law would have required all voters to show specific photo identification at the polling place before being allowed to cast their ballot. The Voter ID law specified that the photo identification must include an expiration date, therefore invalidating several forms of photo identification, including many employee identification cards. Before the law could take effect, however, a lawsuit was filed in Pennsylvania's Commonwealth Court, alleging that the new Voter ID law violated Pennsylvania's Constitution by depriving citizens of their most fundamental constitutional right — the right to vote. The lawsuit sought an injunction blocking enforcement of the law before the November 2012 election.[141] Ultimately, the law was struck down by the Pennsylvania Commonwealth Court, before voters were subject to the new requirements in the next election, and Pennsylvania returned to its original first-time voter identification requirement.[142]

The ability to register to vote ends 30 days prior to any election.[143] Therefore, a person wishing to register for the first time, change their name, address, or party affiliation must submit a completed voter registration application no later than 30 days prior to the next election. Any paper application postmarked after the cut-off is to be processed after the election is finalized. If the applicant applies online, they have until 11:59 P.M. and 59 seconds on the day of the cut-

[138] *Fish v. Kobach*, 309 F. Supp. 3d 1048 (D. Kan. 2018). The matter has been appealed to the United States Court of Appeals Tenth Circuit. On January 14, 2019, the party name of the defendant Kris Kobach has been updated to reflect a change in the state of Kansas' Secretary of State to Scott Schwab as follows: *Fish v. Schwab*. See <https://www.courtlistener.com/docket/4510003/fish-v-kobach/?filed_after=&filed_before=&entry_gte=&entry_lte=&order_by=desc> (accessed April 29, 2019).

[139] Ibid.

[140] Former Act 18 of 2012 was held unconstitutional by the Pennsylvania Commonwealth Court and its enforcement permanently enjoined by *Applewhite v. Com.*, 2014 WL 184988 (Pa. Cmwlth. 2014).

[141] The lawsuit was filed by the American Civil Liberties Union of Pennsylvania, the Advancement Project, the Public Interest Law Center of Philadelphia, and the Washington, DC law firm of Arnold & Porter LLC, on behalf of ten Pennsylvania voters and three prominent advocacy organizations. <https://www.aclupa.org/news/2012/05/01/groups-file-lawsuit-in-commonwealth-court-to-overturn-pennsylvanias-unconstitutional-voter-photo-id-law> (accessed March 21, 2019).

[142] A first time voter, or a voter voting at a new polling place, must show proof of identification. The valid photo identifications include a Pennsylvania DL or PennDOT ID card, ID issued by any Commonwealth agency, ID issued by the U.S. Government, U.S. Passport, U.S. Armed Forces ID, student ID, or an employee ID. If you do not have a photo ID, a first time voter can use one of the following non-photo IDs that includes their name and address: confirmation issued by the County Voter Registration Office, non-photo ID issued by the Commonwealth, non-photo ID issued by the U.S. Government, firearm permit, current utility bill, current bank statement, current paycheck, or a government check. See <https://www.votespa.com/Register-to-Vote/Pages/Voter-ID-for-First-Time-Voters.aspx> (accessed March 20, 2019).

[143] 25 Pa. C.S. § 1326(b).

off.[144] Through Motor Voter at PennDOT, they have until the close of business of the photo license center on the day of the cut-off.

Once registered, a voter will remain registered until they either (1) request their voter registration be cancelled or (2) the county cancels the registration as part of its required list maintenance process.[145] A registered voter can cancel their voter registration at any time by completing and signing a "Request To Cancel Voter Registration" form and forwarding it to the county voter registration office in the county in which they are registered. A county may cancel a voter's registration in the process of performing the annual list maintenance that is required by law. List maintenance activities include cancelling a voter's registration due to death, moving out of the county or state, and not voting and not having any contact with the county elections office for a specified amount of time.[146] List maintenance is discussed in detail in *Finding 4*.

[144] DOS Election Support Plan "Verification and Environment changes."
[145] 52 U.S.C. § 21083(a)(2) (Computerized list maintenance). *See also* 25 Pa.C.S. §1901 (Removal of electors). A voter's county and/or voting precinct may change due to a change in residence within Pennsylvania, but the voter will still remain as a registered voter.
[146] 25 Pa C.S. § 1501.

Appendix D	The lack of oversight that allowed non-citizens the ability to register to vote at PennDOT's photo license centers, even after indicating they are not a citizen, was addressed during the audit period.

In 2017, media reports identified an issue in which non-citizens had the ability to register to vote at the Pennsylvania Department of Transportation (PennDOT) photo license centers.[147] We asked Department of State (DOS) management about this issue, and its responses are summarized below. We did not, however, have access to individuals' records of citizenship status and did not determine whether non-citizens were registered to vote.

According to DOS management, in 2017, DOS became aware of and took subsequent steps to investigate and address a decades-old issue with the Motor Voter process that allowed non-citizens the ability to register to vote even if they indicated that they are not citizens.[148] The issue, as explained by DOS management, was that when a person was offered the opportunity to register to vote during the driver's license (DL) photo card renewal/application process at PennDOT photo licensing centers, those that indicated that they were non-citizens *were not* excluded from the voter registration questions.[149] While voter registration during the DL photo card process requires an individual to twice confirm their citizenship status, both those that indicated they were citizens and those that indicated they were non-citizens were given the opportunity to register to vote.[150]

The National Voter Registration Act of 1993 (Motor Voter), which became effective on January 1, 1995, created requirements that each States' motor vehicle authority must: (1) provide individuals with the opportunity to register to vote at the same time that they apply for a DL or seek to renew a DL; and (2) forward the completed application to the appropriate state or local election official. In Pennsylvania, this was a manual process for many years due to each of the 67 counties having a different voter registration system. PennDOT mailed hard copy voter

[147] <https://philadelphia.cbslocal.com/2017/09/20/it-undermines-integrity-of-elections-glitch-allows-non-citizens-in-pa-to-vote/> (accessed May 17, 2019) and <http://www.mcall.com/news/pennsylvania/mc-nws-pa-voter-registration-glitch-non-citizens-20170920-story.html> (accessed May 17, 2019).

[148] On February 26, 2018, the Public Interest Legal Fund filed a complaint in the U.S. District Court for the Middle District of Pennsylvania seeking injunctive relief to compel DOS to allow the group access to information on non-citizen voting records. As of the date of this audit, the lawsuit is ongoing. See *PILF v. Torres*, 1:18-cv-00463 and 1:19-cv-00622.
<https://freebeacon.com/issues/pennsylvania-state-dept-sued-hiding-noncitizen-voting-records/> (accessed July 26, 2019).

[149] Citizenship is determined based upon documentation that PennDOT requires individuals to provide, such as a birth certificate, U.S. Passport, or a Certificate of Naturalization.

[150] A person applying to register to vote is required to affirm that they are: (1) A citizen of the United States; (2) A resident of Pennsylvania and the election district in which they want to register for at least 30 days prior to the next election; and (3) At least 18 years of age on or before the next election.

registration applications to DOS which were subsequently forwarded to the appropriate county election office (county) for processing.[151] Once new federal and subsequent state laws were enacted and in effect, DOS implemented the Statewide Uniform Registry of Electors (SURE) system. With the creation of SURE, PennDOT's Motor Voter process was electronically connected to the SURE system.[152] When the last county implemented SURE in 2005, the Motor Voter process became fully automated, with applications from PennDOT being electronically received by SURE and then electronically parsed out to the respective counties for processing.

After the non-citizen voter registration issue related to Motor Voter was identified, PennDOT, in conjunction with DOS, made changes to the Motor Voter process to help ensure that those who indicate that they are non-citizens are no longer able to register to vote through PennDOT. DOS management stated that the project to correct the issue was completed in December 2017. We confirmed management's statement through observation of the Motor Voter process during a visit to a photo license center in November 2018. Currently, when a customer arrives at a PennDOT photo license center with their camera card to obtain a new DL or renew their existing DL, their citizenship status is embedded into the bar code on the camera card. Based on this bar code, a non-citizen customer is not asked the voter registration questions. Conversely, when a citizen (either over the age of 18 or who will be 18 by the date of the next election) arrives at a photo license center, they are asked the voter registration questions. We confirmed this process is in place by observing multiple scenarios at a PennDOT photo license center of individuals who were identified in the PennDOT system as non-citizens and citizens (both under age 18 and over age 18).

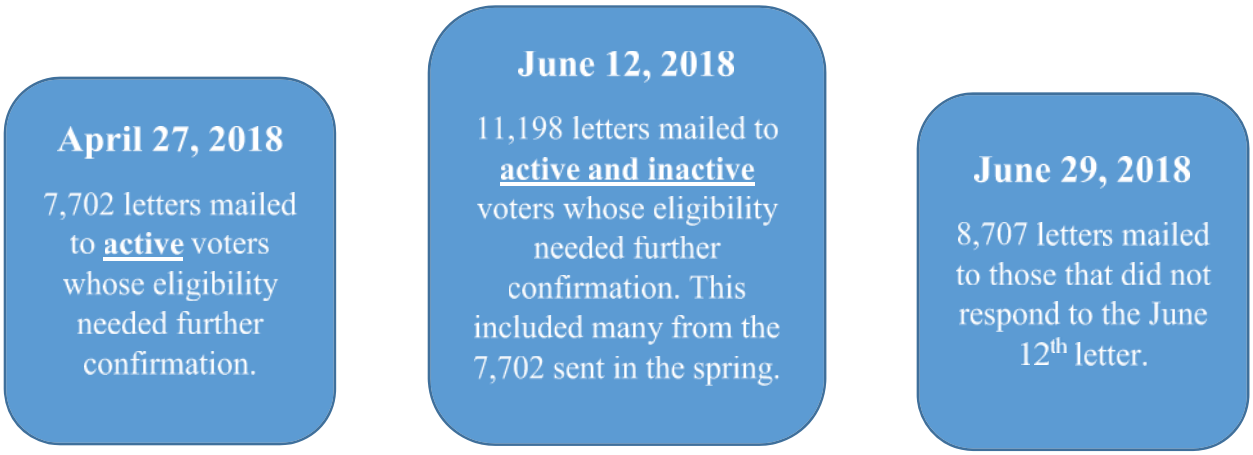
In addition to working with PennDOT to correct the issue, DOS management stated that steps were taken to investigate and address the concern that non-citizens were registered to vote. DOS management stated that they retained an expert, a tenured Associate Professor of Political Science, to conduct an analysis by comparing the Commonwealth's voter registration data with other available Commonwealth databases. We requested information from DOS regarding what Commonwealth databases were used for the analysis and the results of the analysis; however, DOS would not provide this information. Therefore, we were unable to verify the following:

- Whether DOS actually retained an individual to conduct an analysis.
- The scope and methodology of the analysis.
- The results and conclusions of the analysis.

[151] National Voter Registration Act of 1993 (Motor Voter), 52 U.S.C. §§ 20501–20511 (formerly 42 U.S.C. §§ 1973gg–1973gg-10).

[152] In 2002, the U.S. Congress passed the Help America Vote Act (HAVA) and, subsequently, the Pennsylvania General Assembly enacted Act 3 of 2002, which implemented HAVA into Pennsylvania Law. *See* 52 U.S.C. §§ **20901**-21145 (formerly 42 U.S.C. §§ 15301-15545) and **25 Pa.C.S.** §§ 1101-1906 (as noted in an earlier footnote, Act 3 of 2002 was added Part IV to the consolidated Title 25 Elections).

According to DOS management, a series of letters, of which examples of each were provided to us for review, were sent to the individuals identified as having questionable eligibility.[153]



Following the series of letters shown above, DOS management stated that they placed robocalls to the identified individuals that had not responded to the letters from DOS.[154] As a result of these letters and robocalls, DOS management stated that the following actions occurred:

[153] The letters outlined the basic requirements to be a registered voter (as described above), and asked the recipient of the letter to affirm that they were qualified to be a registered voter or request that their registration be cancelled. Information regarding the number of letters sent by DOS was provided to us by DOS management. DOS management, however, did not provide any additional documentation to support the number of letters that DOS reportedly mailed to voters. DOS management indicated that most of the recipients of the April 27, 2018, letter also received the June 12, 2018, letter. If the individual had responded to DOS, however, then they would not have been sent the June 12, 2018, letter.

[154] A **robocall** is a phone call that uses a computerized autodialer to deliver a pre-recorded message. Robocalls were only made to those individuals that had a telephone number available in their voter record.

Actions that occurred with the 11,198 active and inactive voters whose eligibility needed further confirmation based on analysis performed – as represented by DOS management	
215	Requested that their voter registration be cancelled. No reason for cancellation was required to be given by the voter.[a/]
1,948	Affirmed that they were qualified to be a registered voter.
51	Failed to fully complete either the affirmation or cancellation form. Follow-up is being conducted by either DOS or the respective county election office.
286	Voter records were cancelled as a result of unrelated, routine list maintenance conducted by county election offices after the letters were mailed.
8,698	Voter names were forwarded to their respective county election office for further research to be performed to determine their eligibility.
11,198	**Total number of letters mailed to active and inactive voters whose eligibility needed further confirmation.**

[a/] - A request to cancel their voter registration by the recipient of the letter does not necessarily mean that the person is ineligible to be a registered voter. A person may decide that they no longer wish to be a registered voter for reasons other than ineligibility.

Source: This table was compiled by staff of the Department of the Auditor General based on information provided by DOS management. The data are of undetermined reliability as noted in Appendix A. However, this is the best data available. Although this determination may affect the precision of the numbers we present, there is sufficient evidence in total to support our conclusions.

DOS management stated that regarding the 8,698 names forwarded to the counties for follow-up, they have not conducted any follow-up with the counties, noting that it is the counties' obligation to take action to determine eligibility and/or remove ineligible voters as appropriate.

As a result of the decades-old issue with the PennDOT Motor Voter system, individuals who were ineligible to register to vote were in fact allowed to register and, therefore, may have voted in elections. Although the issue with the Motor Voter system has been corrected, DOS and counties must continue to address the concern that ineligible individuals may still be registered to vote.

Appendix E Voter Registration by County

Commonwealth of Pennsylvania Department of State Division of Voter Registration 2018 Voter Registration Statistics - Official November 6, 2018						
County	Democratic	Republican	Green	Libertarian	Other Parties	All Parties
Adams	19,557	36,652	92	449	10,275	67,025
Allegheny	546,641	261,938	1,259	4,964	126,226	941,028
Armstrong	14,419	22,211	34	243	4,443	41,350
Beaver	55,569	41,149	86	575	13,302	110,681
Bedford	7,906	20,587	21	128	2,845	31,487
Berks	116,018	100,459	436	1,613	38,091	256,617
Blair	22,453	44,132	82	382	8,948	75,997
Bradford	9,729	21,971	53	218	4,465	36,436
Bucks	196,280	185,919	647	2,893	71,496	457,235
Butler	40,697	69,840	117	785	17,018	128,457
Cambria	41,300	33,461	81	324	8,172	83,338
Cameron	1,029	1,526	4	13	346	2,918
Carbon	18,008	18,608	63	251	6,249	43,179
Centre	46,205	43,822	184	739	20,182	111,132
Chester	141,384	152,684	502	2,023	60,714	357,307
Clarion	7,354	12,909	21	93	2,533	22,910
Clearfield	17,051	24,359	42	235	5,202	46,889
Clinton	8,090	10,051	28	104	2,584	20,857
Columbia	14,500	18,187	42	256	5,695	38,680
Crawford	18,498	27,626	55	269	6,099	52,547
Cumberland	57,935	86,488	288	1,175	26,370	172,256
Dauphin	84,062	74,276	274	1,013	26,228	185,853
Delaware	188,908	162,271	432	1,498	50,262	403,371
Elk	8,578	8,588	23	77	2,080	19,346
Erie	96,961	68,402	321	1,041	25,185	191,910
Fayette	43,431	27,491	70	315	6,901	78,208
Forest	1,220	1,765	2	12	329	3,328
Franklin	24,150	54,942	89	512	12,898	92,591
Fulton	2,307	5,859	8	49	877	9,100
Greene	11,337	8,411	47	70	1,981	21,846
Huntingdon	9,033	17,749	50	105	3,078	30,015
Indiana	19,070	24,005	57	230	6,056	49,418

Jefferson	9,008	17,354	29	152	3,263	29,806
Juniata	3,718	8,642	16	50	1,373	13,799
Lackawanna	86,740	42,383	223	562	13,702	143,610
Lancaster	106,685	169,621	494	2,050	50,642	329,492
Lawrence	25,341	23,316	32	263	5,807	54,759
Lebanon	26,303	46,814	106	496	12,012	85,731
Lehigh	113,101	79,383	322	1,353	38,721	232,880
Luzerne	106,257	76,235	360	1,007	23,654	207,513
Lycoming	21,179	38,006	69	329	8,771	68,354
McKean	6,710	13,791	32	154	3,165	23,852
Mercer	30,385	31,721	67	349	8,955	71,477
Mifflin	6,805	15,248	20	130	2,502	24,705
Monroe	50,688	36,143	155	653	20,543	108,182
Montgomery	273,860	206,635	743	3,122	85,359	569,719
Montour	4,683	6,383	19	79	2,062	13,226
Northampton	96,393	73,561	322	1,335	37,702	209,313
Northumberland	19,249	26,646	82	290	6,518	52,785
Perry	6,814	18,079	28	188	3,384	28,493
Philadelphia	818,082	118,692	1,531	3,206	122,618	1,064,129
Pike	14,540	18,759	72	300	8,725	42,396
Potter	2,559	7,031	14	61	1,049	10,714
Schuylkill	31,749	43,763	114	448	9,845	85,919
Snyder	5,247	13,506	22	164	2,554	21,493
Somerset	15,546	26,903	30	190	4,330	46,999
Sullivan	1,467	2,449	6	21	433	4,376
Susquehanna	7,488	14,879	54	135	3,213	25,769
Tioga	6,902	16,228	42	153	3,434	26,759
Union	7,297	12,679	33	111	3,923	24,043
Venango	10,229	17,242	43	216	3,704	31,434
Warren	10,107	15,369	50	150	4,514	30,190
Washington	66,867	57,918	115	729	15,778	141,407
Wayne	9,772	18,171	71	194	5,131	33,339
Westmoreland	110,356	107,339	195	1,295	28,165	247,350
Wyoming	5,244	9,714	33	79	1,870	16,940
York	104,274	151,941	480	2,180	46,740	305,615
Totals	**4,111,325**	**3,270,882**	**11,534**	**44,848**	**1,171,291**	**8,609,880**

Source:<https://www.dos.pa.gov/VotingElections/OtherServicesEvents/VotingElectionStatistics/Pages/Voter-Registration-Statistics-Archives.aspx> (accessed June 21, 2019).

Note: The totals in the "2018 Voter Registration Statistics – Official" table above do not match the voter registration totals in the Voter Table data we received from the Department of State (DOS) due to a timing difference. The table above contains totals as of November 6, 2018, whereas, the Voter Table data we received from DOS was extracted

on October 9, 2018, and contains a total of 8,567,700 registered voters. As of June 17, 2019, the voter registration total as reported by DOS was 8,505,621. These changes in the number of registered voters are normal, since voter registration totals change daily due to the ongoing addition and maintenance of records.

Appendix F HAVA Funds Received by Pennsylvania

The United States Election Assistance Commission (EAC) and the United States General Services Administration (GSA), acting on EAC's behalf, awarded three non-discretionary grants, based on a predetermined formula, to states to financially help implement the requirements of the Help American Vote Act of 2002 (HAVA).[155] The following sections briefly explain these grants and show the breakdown of the $160.5 million of HAVA funds received and the amounts expended by Pennsylvania as of September 30, 2018.

Section 101: Payments to States for Activities to Improve Administration of Elections

Section 101 funds were provided to states for activities to improve the administration of federal elections and could be used for various purposes, such as voter education, development of the state plan, and training. GSA distributed a total of $349 million in Section 101 funds to states between April 2003 and August 2003.[156] These funds were required to be deposited in interest-bearing state election accounts and had no restrictions on when they could be expended by the states once obligated at the federal level. Pennsylvania received $11,323,168 in Section 101 funds and expended the funds and interest earned through state fiscal year ended June 30, 2013, as shown in the following table:

[155] EAC also administered three discretionary grant programs (Election Data Collection, College Poll Workers, and Mock Elections) that were awarded through a competitive process, and the United States Department of Health and Human Services administered a grant program to increase the accessibility of polling locations to disabled persons. These other grants were not included in this summary. Source: U.S. Election Assistance Commission, *Strengthening the Electoral System One Grant at a Time: A Retrospective of Grants Awarded by EAC April 2003 – December 2010,* <https://www.eac.gov/assets/1/6/FY2010_Grants_Report_FINAL.pdf> (accessed July 12, 2019).
[156] Ibid.

State Fiscal Year	Grant Expenditures	Interest Expenditures	Total Expenditures
2002	$ 115,738	-	$ 115,738
2003	$ 6,708,787	-	$ 6,708,787
2004	$ (345,881)	-	$ (345,881)
2005	$ 2,119,419	-	$ 2,119,419
2006	$ 1,644,302	-	$ 1,644,302
2007	$ 493,544	-	$ 493,544
2008	$ 540,638	-	$ 540,638
2009	$ 433,052	-	$ 433,052
2010	$ 142,912	$ 235,476	$ 378,388
2011	$ (711,851)	$ 817,782	$ 105,931
2012	$ 182,498	$ 156,541	$ 339,039
2013	$ 10	$ 91,693	$ 91,703
Total	**$11,323,168**	**$ 1,301,492**	**$12,624,660**

Source: Produced by the Department of the Auditor General staff from the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date."

Section 102: Payments to States for Election Administration Improvements and Replacement of Punch Card and Lever Voting Machines

Section 102 funds were required to be used to replace any punch card or lever voting systems. GSA distributed a total of $300 million in Section 102 funds to states in federal fiscal year (FFY) 2003.[157] The deadline for states to have replaced its machines was originally November 2, 2004, however, states could file for subsequent extensions which ultimately expired on the date of the first federal election held after November 1, 2010.[158] States with unobligated funds after the deadline were required by HAVA to return the balance of funds to EAC for redistribution to all states in the form of Section 251 payments. Pennsylvania received $22,897,794 in Section 102 funds and expended the funds and interest earned through state fiscal year ended June 30, 2011, as shown in the following table:

[157] The federal fiscal year is October 1 through September 30.
[158] Ibid.

State Fiscal Year	Grant Expenditures	Interest Expenditures	Total Expenditures
2005	$ 10,658,762	-	$ 10,658,762
2006	$ 9,475,847	-	$ 9,475,847
2007	$ 1,370,102	-	$ 1,370,102
2008	$ 933,803	-	$ 933,803
2009	$ 2,551,075	-	$ 2,551,075
2010	$(2,169,751)	$ 4,002,558	$ 1,832,807
2011	$ 77,956	$ 261,616	$ 339,572
Total	**$ 22,897,794**	**$ 4,264,174**	**$ 27,161,968**

Source: Produced by the Department of the Auditor General staff from the Commonwealth's SAP accounting system report, "Detail Grant Line Items by FM Posting Date."

Section 251: Requirements Payments

Section 251 funds were required to be used to procure voting systems that comply with the new standards of HAVA, develop and implement a computerized statewide voter registration list, and other specific improvements. EAC disbursed a total of $2.6 billion in requirements payments in FFY 2003, 2004, 2008, 2009, 2010, and 2011. Section 251 funds and interest earned on deposits of Section 251 funds had no fiscal year limitation at the state level once obligated at the federal level.[159] Pennsylvania received a total of $112,821,809 in Section 251 funds. The following table shows the amount of funds received by Pennsylvania by FFY. As of September 30, 2018, Pennsylvania earned $16.8 million in interest and had total expenditures of $126.7 million, leaving a balance of $2.9 million in unspent funds.[160]

[159] Ibid.
[160] The U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019, <https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf> (accessed July 12, 2019).

Federal Fiscal Year	Date Received	Amount Received
2003	06/17/2004	$ 35,992,863
2004	06/17/2004	$ 64,585,966
2008	01/06/2009	$ 4,919,086
2009	02/01/2010	$ 4,277,466
2010	09/24/2010	$ 2,994,226
2011	03/16/2012	$ 52,202
Total		**$ 112,821,809**

Source: Produced by the Department of the Auditor General staff from the EAC website <https://www.eac.gov/payments-and-grants/managing-requirements-payments/> (accessed July 12, 2019).

In March 2018, the United States Congress provided states an additional $380 million of Section 251 funding through the Omnibus Appropriations Act of 2018. States could begin spending funds once they received their notice of grant award on April 17, 2018. As of September 30, 2018, Pennsylvania received $13,476,156 in grant funds, earned interest totaling $24,077, and had yet to expend the funds.[161] Pennsylvania plans to replace voting equipment that is reaching the end of its usable life with new equipment that has a voter verifiable paper audit trail.[162]

[161] The U.S. Election Assistance Commission, *Grant Expenditure Report Fiscal Year 2018*, dated April 4, 2019. <https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf> (accessed July 12, 2019).
[162] Ibid.

Appendix G Description of Data Used in the Audit

The table below shows the number of records included in the Voter Table data obtained for this audit as of October 9, 2018. This table differs from the numbers included in *Appendix E*, which shows the number of registered voters by party, by county certified as of the November 6, 2018, election.

Status of Voter Records in the Voter Table as of October 9, 2018	
Number of Records	**Voter Status**
7,693,493	Active[a/]
874,207	Inactive[b/]
8,567,700	**Subtotal – Eligible to Vote**
7,789	Hold[c/]
16	Blank[d/]
7,495,963	Cancelled[e/]
16,071,468	**Total number of records in the voter table from the Statewide Uniform Registry of Electors (SURE) Database as of October 9, 2018**

[a/] An active voter is a person who is fully registered to vote.
[b/] An inactive voter is a person who is fully registered to vote but has not voted in at least five years, nor has had certain types of communication with their county election office. An inactive voter can vote once they complete an affidavit attesting to their eligibility to vote at that polling place.
[c/] A voter's registration can be placed on hold for several reasons, including imprisonment.
[d/] No status was included in the status field.
[e/] A voter whose registration has been cancelled will no longer be printed in the poll book and will not be able to vote until they re-register.

Source: This table was compiled by the staff of the Department of the Auditor General from data received from the Department of State that was extracted from the SURE system.

Appendix H SURE Survey

As part of our audit procedures, the following survey was sent on September 24, 2018, to the County Election Office Director in each of Pennsylvania's 67 counties. We requested that each director respond to the survey questions in order to assist us in gaining a comprehensive understanding of the Statewide Uniform Registry of Electors (SURE).

SURE Survey

County Name:

Name(s) and title(s) of individual(s) completing the survey:

General Questions

- How many people work on a daily basis processing voter registration related documents?
- Number of employees considered full time?
- Number of employees considered part time (approximate number of hours per week)?
- Of those employees, how many work in a supervisory/management position?
- How many precincts are in your county September 21, 2018?

Guidance/Training

1. Do you utilize the SURE Job Aids developed by DOS? ◯ Yes ◯ No

   Do you find them to be useful and/or sufficient? ◯ Yes ◯ No

   If you don't use the SURE Job Aids, why not?

2. How often do you generally utilize the SURE Help Desk?

   ◯ Weekly
   ◯ Monthly
   ◯ Bi-annually
   ◯ Annually
   ◯ Don't use

   If you utilize the SURE Help Desk, what is it typically regarding?

3. Have you received other guidance from DOS or another source regarding registration and maintenance of your voter rolls? ◯ Yes ◯ No

   If yes, please describe.

4. Do you request SURE training from DOS for new employees? ◯ Yes ◯ No

   If no, how do you provide training to new employees?

5. Do you notify DOS when you hire a new employee? ◯ Yes ◯ No

6. Do you notify DOS when an employee leaves employment with the county?
   ◯ Yes ◯ No

Processing Applications

7. Do you review work completed in SURE by your employees to ensure that it is accurate?
   ◯ Yes ◯ No

   If yes,

   Who reviews (Please list the title of the reviewer)?

   How often?

   Is the review documented and maintained?

8. How does your office handle applications that you cannot initially register or deny?

9. If the HAVA check comes back without a match, do you:
   Reject without further investigation ○ Yes ○ No
   Conduct further investigation ○ Yes ○ No

   If further investigation is conducted, please provide explanation of additional work performed.

10. Do you scan and retain within SURE all paper voter registration applications?
    ○ Yes ○ No

    If no, why not?

    Do you retain the hard copy paper applications? ○ Yes ○ No

    If yes, for how long?

Poll Books

11. How do you print your poll books? ○ In-house ○ Contracted vendor

    If neither, please explain.

12. Do you have procedures in place to ensure that the printed poll books include all applicable records from SURE? ◯ Yes ◯ No

    If yes, please describe:

List Maintenance

13. Does your office conduct list maintenance as prescribed by state law (NCOA, 5 year mailings, etc.)? ◯ Yes ◯ No

    If yes, when is each type of maintenance activity conducted?
    NCOA
    Five year mailing
    Other list maintenance activities (please include the type of activity and approximate date activity is conducted)

14. Do you conduct a review to ensure that the required list maintenance activities have been completed and completed accurately? ◯ Yes ◯ No

    If yes,

    Who reviews (Please list the title of the reviewer)?

    How often is a review conducted?
    Is the review documented and maintained?

External reviews/audits

15. Has your office received any external reviews/audits (excluding DOS and the current Department of the Auditor General audit) of your operations related to voter registration or elections? ◯ Yes ◯ No

    If yes, who conducted the review/audit?

SURE Changes

16. Please provide your thoughts on issues within SURE and if you could recommend changes or additions to functionality what would they be?

IT Questions

17. Has your County connected any county-owned IT equipment to the SURE system (i.e., servers, printers, switches, monitors, keyboards, etc.)? ◯ Yes ◯ No

    If so, please list

18. Do County Election Workers or contractors share user IDs and passwords to the SURE system? ◯ Yes ◯ No

    If yes, why?

19. Do you periodically review SURE users to determine whether access is still appropriate? ◯ Yes ◯ No

    If yes, please describe:

20. Do you monitor security events and respond to security breaches in the IT equipment connected to the SURE system? ◯ Yes ◯ No

    If yes, please describe:

21. During the recent disaster recovery test of SURE in July 2018, were you able to log in and perform all the required tests successfully? ◯ Yes ◯ No

    Please list any tasks you were unable to perform:

22. Has anyone with access to the SURE system (employee or contractor) attended any cybersecurity awareness training since January 2016? ◯ Yes ◯ No

    If yes, please describe the training, including who conducted the training and who attended from the County:

23. Has anyone with access to the SURE system (employee or contractor) participated in cybersecurity awareness groups such as the Center for Internet Security's Multi-State Sharing and Analysis Center (MS-ISAC)? ◯ Yes ◯ No

    If yes, please describe the group and who attends:

24. DOS has recently developed the Online Voter Registration Web Application Programming Interface (PA OVR WEBAPI) to facilitate uploading large numbers of voter registration applications into SURE from outside organizations (i.e., voter registration drives). Has your office processed applications uploaded from the PA OVR WEBAPI? ◯ Yes ◯ No

If yes, please describe any problems you may have encountered.

Please use the space below if additional space is necessary.

Appendix I Distribution List

This report was distributed to the following Commonwealth officials:

The Honorable Tom Wolf
Governor

The Honorable Kathy Boockvar
Secretary of the Commonwealth
Pennsylvania Department of State

The Honorable Jonathan Marks
Deputy Secretary for Elections
and Commissions
Pennsylvania Department of State

Mr. Timothy E. Gates
Chief Counsel
Pennsylvania Department of State

The Honorable John MacMillan
Deputy Secretary for Information
Technology and Chief Information
Officer
Office of Administration

The Honorable Garth Everett
Majority Chair
House State Government Committee

The Honorable Kevin Boyle
Democratic Chair
House State Government Committee

The Honorable Kristin Hill
Vice-Majority Chair
Senate State Government Committee

The Honorable Michaele Totino
Majority Executive Director
Senate State Government Committee

The Honorable Anthony Williams
Democratic Chair
Senate State Government Committee

The Honorable Jen Swails
Secretary of the Budget
Office of the Budget

The Honorable Joseph M. Torsella
State Treasurer
Pennsylvania Treasury Department

The Honorable Josh Shapiro
Attorney General
Office of the Attorney General

The Honorable Michael Newsome
Secretary of Administration
Office of Administration

Mr. William Canfield
Director
Bureau of Audits
Office of Comptroller Operations

Ms. Mary Spila
Collections/Cataloging
State Library of Pennsylvania

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

This report is a matter of public record and is available online at www.PaAuditor.gov. Media questions about the report can be directed to the Pennsylvania Department of the Auditor General, Office of Communications, 229 Finance Building, Harrisburg, PA 17120; via email to: News@PaAuditor.gov.