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

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

TABLE OF CONTENTS

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

TABLE OF CONTENTS (continued)

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

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 <u>all</u> 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.

A Performance Audit

Pennsylvania Department of State
Statewide Uniform Registry of Electors

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:

Number of Registered Voters	Number of Potentially Deceased[a/]	Age Range
Voter Registration Records Indicating that the Voter was 100 Years of Age or Older as of October 9, 2018		
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.

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**

Analysis of Potentially Deceased Individuals as of October 9, 2018

[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.
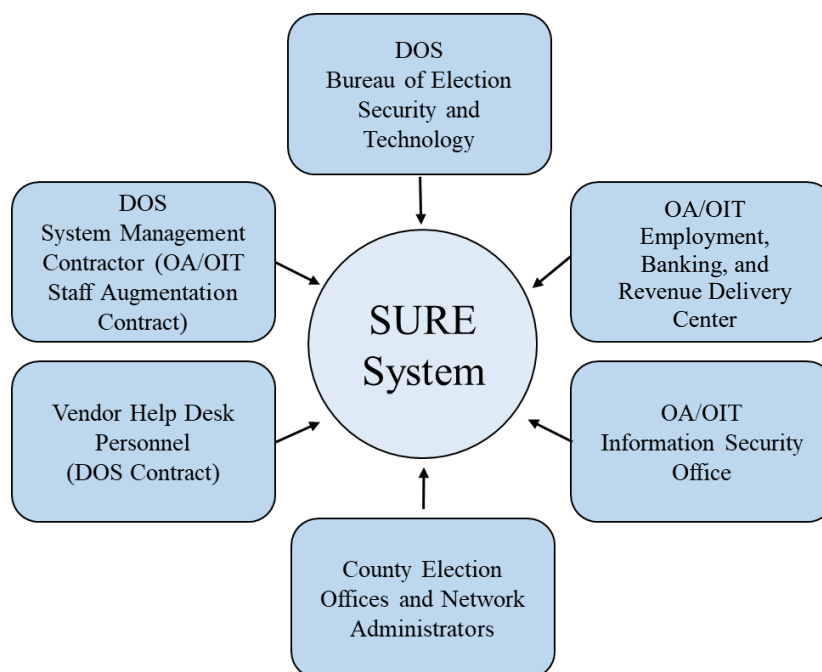
Source: Produced by the Department of the Auditor General staff based on information provided by DOS management.

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 <u>data</u> 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 I 401 North Street I Harrisburg, PA 17120-0500 I 717.787.6458 I F 717.787.1734 www.dos.pa.gov

113

- 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.

Page 2 of 5

114

- 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

Page 3 of 5

115

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
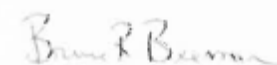Pennsylvania Office of Homeland Security

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

119

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 <u>all</u> 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:

  o Brennan Center for Justice. *Defending Elections: Federal Funding Needs for State Election Security,* July 18, 2019.
  o Center for American Progress. *Election Security in All 50 States: Defending America's Elections*, February 12, 2018.

- o 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.
- o The Heritage Foundation. *A Sampling of Election Fraud Cases from Across the Country*. April 2017.
- o State of Minnesota, Office of the Legislative Auditor. *Voter Registration: 2018 Evaluation Report*. March 8, 2018.
- o United States Election Assistance Commission (EAC). *2014 Statutory Overview*, January 2015.
- o 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.
- o 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.
- o 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.
- o The National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*, September 6, 2018.
- o 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.

- o 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:
  - o Access management
  - o Change management (i.e., configuration management)
  - o Segregation of duties
  - o Service delivery
  - o 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. <u>DOS Responsibilities</u>. 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.

Page 1 of 6

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. <u>Auditor General Responsibilities.</u>

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

Page 2 of 6

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.

Page 3 of 6

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.

Page 4 of 6

j. <u>Severability</u>. 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. <u>Integration</u>. 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.]
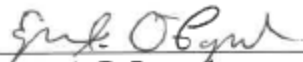
The parties, through their authorized representatives, have signed this Agreement below.

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:
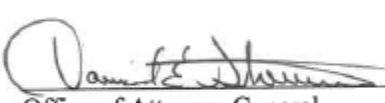
signature   5/15/18
Office of Chief Counsel   Date
Department of State

signature   5-14-18
Office of Chief Counsel   Date
Pennsylvania Department of the
Auditor General

Pamela F. Cross   5/16/18
Office of General Counsel   Date

signature   5/21/18
Office of Attorney General   Date

_John Onda___   5/31/2018
Comptroller Operations   Date

Page 6 of 6

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]

April 27, 2018

7,702 letters mailed to **active** voters whose eligibility needed further confirmation.

June 12, 2018

11,198 letters mailed to **active and inactive** voters whose eligibility needed further confirmation. This included many from the 7,702 sent in the spring.

June 29, 2018

8,707 letters mailed to those that did not respond to the June 12th letter.
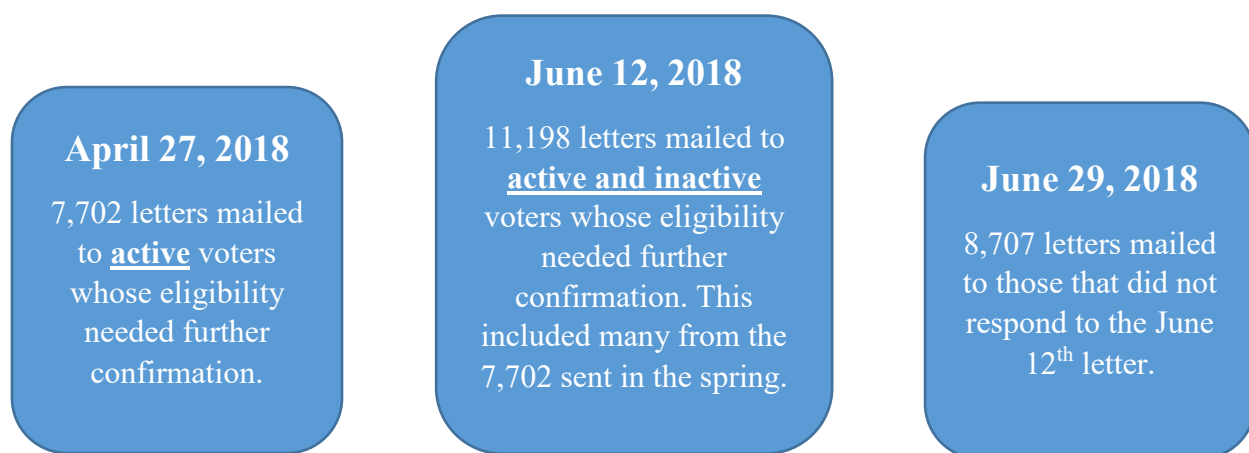
Following the series of letters shown above, DOS management stated that they placed robocalls to the identified individuals that had not responded to the letters from DOS.[154] As a result of these letters and robocalls, DOS management stated that the following actions occurred:

---

[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

<table>
<tr><td colspan="7">Commonwealth of Pennsylvania
Department of State
Division of Voter Registration
2018 Voter Registration Statistics - Official
November 6, 2018</td></tr>
<tr><th>County</th><th>Democratic</th><th>Republican</th><th>Green</th><th>Libertarian</th><th>Other
Parties</th><th>All
Parties</th></tr>
<tr><td>Adams</td><td>19,557</td><td>36,652</td><td>92</td><td>449</td><td>10,275</td><td>67,025</td></tr>
<tr><td>Allegheny</td><td>546,641</td><td>261,938</td><td>1,259</td><td>4,964</td><td>126,226</td><td>941,028</td></tr>
<tr><td>Armstrong</td><td>14,419</td><td>22,211</td><td>34</td><td>243</td><td>4,443</td><td>41,350</td></tr>
<tr><td>Beaver</td><td>55,569</td><td>41,149</td><td>86</td><td>575</td><td>13,302</td><td>110,681</td></tr>
<tr><td>Bedford</td><td>7,906</td><td>20,587</td><td>21</td><td>128</td><td>2,845</td><td>31,487</td></tr>
<tr><td>Berks</td><td>116,018</td><td>100,459</td><td>436</td><td>1,613</td><td>38,091</td><td>256,617</td></tr>
<tr><td>Blair</td><td>22,453</td><td>44,132</td><td>82</td><td>382</td><td>8,948</td><td>75,997</td></tr>
<tr><td>Bradford</td><td>9,729</td><td>21,971</td><td>53</td><td>218</td><td>4,465</td><td>36,436</td></tr>
<tr><td>Bucks</td><td>196,280</td><td>185,919</td><td>647</td><td>2,893</td><td>71,496</td><td>457,235</td></tr>
<tr><td>Butler</td><td>40,697</td><td>69,840</td><td>117</td><td>785</td><td>17,018</td><td>128,457</td></tr>
<tr><td>Cambria</td><td>41,300</td><td>33,461</td><td>81</td><td>324</td><td>8,172</td><td>83,338</td></tr>
<tr><td>Cameron</td><td>1,029</td><td>1,526</td><td>4</td><td>13</td><td>346</td><td>2,918</td></tr>
<tr><td>Carbon</td><td>18,008</td><td>18,608</td><td>63</td><td>251</td><td>6,249</td><td>43,179</td></tr>
<tr><td>Centre</td><td>46,205</td><td>43,822</td><td>184</td><td>739</td><td>20,182</td><td>111,132</td></tr>
<tr><td>Chester</td><td>141,384</td><td>152,684</td><td>502</td><td>2,023</td><td>60,714</td><td>357,307</td></tr>
<tr><td>Clarion</td><td>7,354</td><td>12,909</td><td>21</td><td>93</td><td>2,533</td><td>22,910</td></tr>
<tr><td>Clearfield</td><td>17,051</td><td>24,359</td><td>42</td><td>235</td><td>5,202</td><td>46,889</td></tr>
<tr><td>Clinton</td><td>8,090</td><td>10,051</td><td>28</td><td>104</td><td>2,584</td><td>20,857</td></tr>
<tr><td>Columbia</td><td>14,500</td><td>18,187</td><td>42</td><td>256</td><td>5,695</td><td>38,680</td></tr>
<tr><td>Crawford</td><td>18,498</td><td>27,626</td><td>55</td><td>269</td><td>6,099</td><td>52,547</td></tr>
<tr><td>Cumberland</td><td>57,935</td><td>86,488</td><td>288</td><td>1,175</td><td>26,370</td><td>172,256</td></tr>
<tr><td>Dauphin</td><td>84,062</td><td>74,276</td><td>274</td><td>1,013</td><td>26,228</td><td>185,853</td></tr>
<tr><td>Delaware</td><td>188,908</td><td>162,271</td><td>432</td><td>1,498</td><td>50,262</td><td>403,371</td></tr>
<tr><td>Elk</td><td>8,578</td><td>8,588</td><td>23</td><td>77</td><td>2,080</td><td>19,346</td></tr>
<tr><td>Erie</td><td>96,961</td><td>68,402</td><td>321</td><td>1,041</td><td>25,185</td><td>191,910</td></tr>
<tr><td>Fayette</td><td>43,431</td><td>27,491</td><td>70</td><td>315</td><td>6,901</td><td>78,208</td></tr>
<tr><td>Forest</td><td>1,220</td><td>1,765</td><td>2</td><td>12</td><td>329</td><td>3,328</td></tr>
<tr><td>Franklin</td><td>24,150</td><td>54,942</td><td>89</td><td>512</td><td>12,898</td><td>92,591</td></tr>
<tr><td>Fulton</td><td>2,307</td><td>5,859</td><td>8</td><td>49</td><td>877</td><td>9,100</td></tr>
<tr><td>Greene</td><td>11,337</td><td>8,411</td><td>47</td><td>70</td><td>1,981</td><td>21,846</td></tr>
<tr><td>Huntingdon</td><td>9,033</td><td>17,749</td><td>50</td><td>105</td><td>3,078</td><td>30,015</td></tr>
<tr><td>Indiana</td><td>19,070</td><td>24,005</td><td>57</td><td>230</td><td>6,056</td><td>49,418</td></tr>
</table>

Pennsylvania Department of State
Statewide Uniform Registry of Electors

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?

1

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.

   [ ]

2

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?

```



```

3

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.

    ```

    ```

4

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? `                        `

5

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

6

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:

[   ]

7

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:

8

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.

9

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