practical matter: a few individual voters may have detected that there was a problem, but there's no procedure by which this translates into any action that election administrators can take to correct the outcome of the election. Polling place procedures *cannot correct or deter hacking, or even reliably detect it*, as we discuss next. This is essentially the distinction between a system that is merely software independent and one that is contestable: a change to the software that alters the outcome might generate evidence for an alert, conscientious, individual voter, but it does not generate public evidence that an election official can rely on to conclude there is a problem.

Even if some voters notice that BMDs are altering votes, there's no way to correct the election outcome. Suppose a state election official wanted to detect whether the BMDs are cheating, and correct election results, based on actions by those few alert voters who notice the error. What procedures could possibly work against the manipulation we are considering?

1. How about, "If at least 1 in 400 voters claims that the machine misrepresented their vote, void the entire election."[17] No responsible authority would implement such a procedure. A few dishonest voters could collaborate to invalidate entire elections simply by falsely claiming that BMDs changed their votes.
2. How about, "If at least 1 in 400 voters claims that the machine misrepresented their vote, then investigate." Investigations are fine, but then what? The only way an investigation can ensure that the outcome accurately reflects what voters expressed to the BMDs is to void an election in which the BMDs have altered votes and conduct a new election. But how do you know whether the BMDs have altered votes, except based the claims of the voters?[18] Furthermore, the investigation itself would suffer from the same problem as above: how can one distinguish between voters who detected BMD hacking or bugs from voters who just want to interfere with an election?

This is the essential security flaw of BMDs: few voters will notice and promptly report discrepancies between what they saw on the screen and what is on the BMD print-

[17]Note that in many jurisdictions, far fewer than 400 voters use a given machine on election day: BMDs are typically expected to serve fewer than 300 voters per day. (The vendor ES&S recommended 27,000 BMDs to serve Georgia's 7 million voters, amounting to 260 voters per BMD [24].) Recall also that the rate 1 in 400 is tied to the amount of manipulation. What if the malware flipped only one vote in 50, instead of 1 vote in 20? That could still change the margin by 4%, but—in this hypothetical—would be noticed by only one voter in 1,000, rather than one in 400. The smaller the margin, the less manipulation it would have taken to alter the electoral outcome.

[18]Forensic examination of the BMD might show that it *was* hacked or misconfigured, but it cannot prove that the BMD *was not* hacked or misconfigured.

out, and even when they do notice, there's nothing appropriate that can be done. (Nor should it be the responsibility of voters to test voting-machine security and accuracy—this is a difficult burden that should not be placed on the voters.)

Therefore, BMDs should not be used by most voters.

Why can't we rely on pre-election and post-election logic and accuracy testing? Most, if not all, jurisdictions perform some kind of *logic and accuracy testing* (LAT) of voting equipment before elections. LAT generally involves voting on the equipment using various combinations of selections, then checking whether the equipment tabulated the votes correctly. As the Volkswagen/Audi "Dieselgate" scandal shows, devices can be programmed to behave properly when they are tested but misbehave in use. Therefore, LAT can never prove that voting machines performed properly in practice.

Don't voters need to check hand-marked ballots, too? It is always a good idea to check one's work. The difference is, with hand-marked paper ballots, voters are responsible for catching and correcting *their own errors*, while if BMDs are used, voters are also responsible for catching *machine errors, bugs, and hacking*. Voters are the *only* people who can detect such problems with BMDs—but, as explained above, if voters do find problems, there's no way they can prove to poll workers or election officials that there were problems and no way to ensure that election officials take appropriate remedial action.

Other tradeoffs, BMDs versus hand-marked opscan

Supporters of ballot-marking devices advance several other arguments for their use.

- **Mark legibility.** A common argument is that a properly functioning BMD will generate clean, error-free, unambiguous marks, while hand marked paper ballots may contain mistakes and stray marks that make it impossible to discern a voter's intent. However appealing this argument seems at first blush, the data are not nearly so compelling. Experience with statewide recounts in Minnesota and elsewhere suggest that truly ambiguous handmade marks are very rare.[19] For instance, 2.9 million hand-marked ballots were cast in the 2008 Minnesota race

[19] States do need clear and complete regulations for interpreting voter marks.

between Al Franken and Norm Coleman for the U.S. Senate. In a manual recount, between 99.95% and 99.99% of ballots were unambiguously marked.[20] [21] In addition, usability studies of hand marked bubble ballots—the kind in most common use in U.S. elections—indicate a *voter* error rate of 0.6%, much lower than the 2.5–3.7% error rate for machine-marked ballots [12].[22] Moreover, modern image-based opscan equipment is better than older "marksense" machines at interpreting imperfect marks. Thus, mark legibility is not a good reason to adopt BMDs for all voters.

- **Undervotes, overvotes.** Another argument offered for BMDs is that the machines can alert voters to undervotes and prevent overvotes. That is true, but modern PCOS can also alert a voter to overvotes and undervotes, allowing a voter to eject the ballot and correct it. Other solutions, such as non-tabulating scanners that simply warn voters of overvotes and undervotes on hand-marked ballots, would be less risky than BMDs.
- **Bad ballot design.** Ill-designed paper ballots, just like ill-designed touchscreen interfaces, may lead to unintentional undervotes [19]. For instance, the 2006 Sarasota, Florida, touchscreen ballot was badly designed. The 2018 Broward County, Florida, opscan ballot was badly designed: it violated three separate guidelines from the EAC's 2007 publication, "Effective Designs for the Administration of Federal Elections, Section 3: Optical scan ballots." [27] In both of these cases (touchscreens in 2006, hand-marked optical-scan in 2018), undervote rates were high. The solution is to follow standard, published ballot-design guidelines and other best practices, both for touchscreens and for hand-marked ballots [3, 19].
- **Low-tech paper-ballot fraud.** All paper ballots, however they are marked, are vulnerable to *loss*, *ballot-box stuffing*, *alteration*, and *substitution* between the

[20] "During the recount, the Coleman and Franken campaigns initially challenged a total of 6,655 ballot-interpretation decisions made by the human recounters. The State Canvassing Board asked the campaigns to voluntarily withdraw all but their most serious challenges, and in the end approximately 1,325 challenges remained. That is, approximately 5 ballots in 10,000 were ambiguous enough that one side or the other felt like arguing about it. The State Canvassing Board, in the end, classified all but 248 of these ballots as votes for one candidate or another. That is, approximately 1 ballot in 10,000 was ambiguous enough that the bipartisan recount board could not determine an intent to vote." [1] See also [20]

[21] We have found that some local election officials consider marks to be ambiguous if *machines* cannot read the marks. That is a different issue from *humans* not being able to interpret the marks. Errors in machine interpretation of voter intent can be dealt with by manual audits: if the reported outcome is wrong because machines misinterpreted handmade marks, a RLA has a known, large chance of correcting the outcome.

[22] Better designed user interfaces (UI) might reduce the error rate for machine-marked ballots below the historical rate for DREs; however, UI improvements cannot keep BMDs from printing something other than what the voter is shown on the screen.

time they are cast and the time they are recounted. That's why it is so important to make sure that ballot boxes are always in multiple-person (preferably bipartisan) custody at any time when they are handled, and that appropriate physical security measures are in place. Strong, verifiable chain-of-custody protections are essential.

Hand-marked paper ballots are vulnerable to alteration by anyone with a pen. Both hand-marked and BMD-marked paper ballots are vulnerable to substitution: anyone who has poorly supervised access to a legitimate BMD during election day can create fraudulent ballots, not necessarily to deposit them in the ballot box immediately (in case the ballot box is well supervised on election day) but with the hope of substituting it later in the chain of custody.[23]

All those attacks (on hand-marked and on BMD-marked paper ballots) are fairly low-tech. There are also higher-tech ways of producing ballots indistinguishable from BMD-marked ballots for substitution into the ballot box, where there is inadequate chain-of-custody protection.

- **Accessible voting technology.** If everyone voted on a BMD, it would guarantee that an accessible device had been set up in the polling place for all voters who needed one. But this is not a good reason to adopt BMDs for *all* voters. Among other things, it would expose all voters to the security flaws described above, decreasing public confidence in the entire election. Some accessibility advocates argue that requiring disabled voters to use BMDs compromises their privacy since hand marked ballots are easily distinguishable from machine marked ballots. This argument has been undercut by the availability in the marketplace of BMDs that mark ballots that cannot easily be distinguished from hand marked ballots. Other advocates object to the idea that disabled voters must use a different method of marking ballots, arguing that their rights are thereby violated. Both HAVA and ADA require accommodations for voters with physical and cognitive impairments, but neither law requires that those accommodations must be used by all voters. To best enable and facilitate participation by all voters, each voter should be provided with a means of casting a vote best suited to their abilities.
- **Ballot printing costs.** Preprinted optical-scan ballots cost 20–50 cents each.[24] Blank cards for BMDs cost up to 15 cents each, depending on the make and model of BMD.[25] But optical-scan ballots must be preprinted for as many vot-

[23] Some BMDs print a bar-code indicating when and where the ballot was produced, but that does not prevent such a substitution attack against currently EAC-certified, commercially available BMDs. We understand that systems under development might make ballot-substitution attacks against BMDs more difficult.

[24] Single-sheet (one- or two-side) ballots cost 20-28 cents, double-sheet ballots needed for elections with many contests, up to 50 cents.

[25] Ballot cards for ES&S ExpressVote cost about 15 cents. New Hampshire's (One4All / Prime III)

ers as *might* show up, whereas blank BMD cards are consumed in proportion to how many voters *do* show up. The Open Source Election Technology Institute (OSET) conducted an independent study of total life cycle costs[26] for hand-marked paper ballots and BMDs in conjunction with the 2019 Georgia legislative debate regarding BMDs [21]. OSET concluded that, even in the most optimistic (i.e., lowest cost) scenario for BMDs and the most pessimistic (i.e, highest cost) scenario for hand-marked paper ballots and ballot-on-demand (BOD) printers—which can print unmarked ballots as needed—the total lifecycle costs for BMDs would be higher than the corresponding costs for hand marked paper ballots.[27]

- **Vote centers.** To run a vote center that serves many election districts with different ballot styles, one must be able to provide each voter a ballot containing the contests that voter is eligible to vote in, possibly in a number of different languages. This is easy with BMDs, which can be programmed with all the appropriate ballot definitions. With preprinted optical-scan ballots, the PCOS can be programmed to *accept* many different ballot styles, but the vote center must still maintain *inventory* of many different ballots. BOD printers are another economical alternative for vote centers.[28]
- **Paper/storage.** BMDs that print summary cards rather than full-face ballots can save paper and storage space. However, many BMDs print full-face ballots, while many BMDs that print summary cards use thermal printers and paper that is fragile and can fade in a few months.[29]

Advocates of hand-marked paper ballot systems advance these additional arguments.

BMDs used by sight-impaired voters use plain paper that is less expensive.

[26]They include not only the cost of acquiring and implementing systems but also the ongoing licensing, logistics, and operating (purchasing paper stock, printing, and inventory management) costs.

[27]BOD printers currently on the market arguably are best suited for vote centers, but less expensive options suited for polling places could be developed. Indeed, BMDs that print full-face ballots could be re-purposed as BOD printers for polling place use, with modest changes to the programming.

[28]Ballot-on-demand printers *may* require maintenance such as replacement of toner cartridges. This is readily accomplished at a vote center with a professional staff. Ballot-on-demand printers may be a less attractive option for many small precincts on election day, where there is no professional staff—but on the other hand, they are less necessary, since far fewer ballot styles will be needed in any one precinct.

[29]The California Top-To-Bottom Review (TTBR) of voting systems found that thermal paper can also be covertly spoiled wholesale using common household chemicals https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-diebold.pdf, last visited 8 April 2019. The fact that thermal paper printing can fade or deteriorate rapidly might mean it does not satisfy the federal requirement to preserve voting materials for 22 months. http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title52-section20701&num=0&edition=prelim, last visited 8 April 2019.

- **Cost.** Using BMDs for all voters substantially increases the cost of acquiring, configuring, and maintaining the voting system. One PCOS can serve 1200 voters in a day, while one BMD can serve only about 260 [24]—though both these numbers vary greatly depending on the length of the ballot and the length of the day. OSET analyzed the relative costs of acquiring BMDs for Georgia's nearly seven million registered voters versus a system of hand marked paper ballots, scanners, and BOD printers [21]. A BMD solution for Georgia would cost taxpayers between 3 and 5 times the cost of a system based on hand marked paper ballots.
- **Mechanical reliability and capacity.** Pens are likely to have less downtime than BMDs. It is easy and inexpensive to get more pens and privacy screens when additional capacity is needed. If a precinct-count scanner goes down, people can still mark ballots with a pen; if the BMD goes down, voting stops. Thermal printers used in DREs with VVPAT are prone to jams; those in BMDs might have similar flaws.

These secondary pros and cons of BMDs do not outweigh the primary security and accuracy concern: BMDs, if hacked or erroneous, can change votes in a way that is not correctable. BMD voting systems are not contestable, defensible, or strongly software independent. Therefore, ballots cast by BMD cannot effectively be audited.

Barcodes

A controversial feature of some BMDs allows them to print 1-dimensional or 2-dimensional barcodes on the paper ballots. A 1-dimensional barcode resembles the pattern of vertical lines used to identify products by their universal product codes. A 2-dimensional barcode or QR code is a rectangular area covered in coded image *modules* that encode more complex patterns and information. BMDs print barcodes on the same paper ballot that contains human-readable ballot choices. Voters using BMDs are expected to verify the human-readable printing on the paper ballot card, but the presence of barcodes with human-readable text poses some significant problems.

- **Barcodes are not human readable.** The whole purpose of a paper ballot is to be able to recount (or audit) the *voters'* votes in a way independent of any (possibly hacked or buggy) computers. If the official vote on the ballot card is the barcode, then it is impossible for the voters to verify that the official vote they cast is the vote they expressed. Therefore, before a state even *considers* using BMDs that print barcodes (and we do not recommend doing so), the State must ensure by statute that recounts and audits are based *only* on the human-readable portion of

the paper ballot. Even so, audits based on untrusted paper trails suffer from the verifiability the problems we outlined above.

- **Ballot cards with barcodes contain two different votes.** Suppose a state does ensure by statute that recounts and audits are based on the human-readable portion of the paper ballot. Now a BMD-marked ballot card with both barcodes and human-readable text contains two different votes in each contest: the barcode (used for electronic tabulation), and the human-readable selection printout (official for audits and recounts). In few (if any) states has there even been a discussion of the legal issues raised when the official markings to be counted differ between the original count and a recount.
- **Barcodes pose technical risks.** Any coded input into a computer system—including wired network packets, WiFi, USB thumbdrives, *and barcodes*—pose the risk that the input-processing software can be vulnerable to attack via deliberately ill-formed input. Over the past two decades, many such vulnerabilities have been documented on *each* of these channels (including barcode readers) that, in the worst case, give the attacker complete control of a system.[30] If an attacker were able to compromise a BMD, the barcodes are an attack vector for the attacker to take over an optical scanner (PCOS or CCOS), too. Since it is good practice to close down all such unneeded attack vectors into PCOS or CCOS voting machines (e.g., don't connect your PCOS to the Internet!), it is also good practice to avoid unnecessary attack channels such as barcodes.

End-to-End Verifiable BMDs

In all BMD systems currently on the market, and in all BMD systems certified by the EAC, the printed ballot or ballot summary is the only channel by which voters can verify the correct recording of their ballots, independently of the computers. The analysis in this paper applies to all of those BMD systems.

There is a class of voting systems called "end-to-end verifiable" (E2E-V), which provide an alternate mechanism for voters to verify their votes [2]. Some E2E-V systems incorporate BMDs, for instance STAR-Vote[31] [5]. If such a voting system could

[30] An example of a barcode attack is based on the fact that many commercial barcode-scanner components (which system integrators use to build cash registers or voting machines) treat the barcode scanner using the same operating-system interface as if it were a keyboard device; and then some operating systems allow "keyboard escapes" or "keyboard function keys" to perform unexpected operations.

[31] The STAR-Vote system is actually a DRE+VVPAT system with a smart ballot box, rather than a BMD system: voters interact with a device that captures their votes electronically and prints a paper record that voters can inspect, but the electronic votes are held "in limbo" until the paper ballot is de-

be demonstrated to be contestable, defensible, and adequately usable by voters, then the analysis in this paper might not be applicable to such BMDs. No E2E-V systems are currently certified by the EAC, nor to our knowledge is any such system under review for certification, nor are any of the 5 major voting-machine vendors offering such a system for sale.[32]

Design Flaws in All-in-One BMDs

Some voting machines incorporate a BMD interface, printer, and optical scanner into the same cabinet. Other DRE+VVPAT voting machines incorporate ballot-marking, tabulation, and paper-printout retention, but without scanning.

These are often called "all-in-one" voting machines. Any such machine that includes *ballot marking* and *deposit into the ballot box* in the same paper path, is unsafe.

Using an all-in-one machine, the voter makes choices on a touchscreen or through a different accessible interface. When the selections are complete, the BMD prints the completed ballot for the voter to review and verify, before depositing the ballot in a ballot box attached to the machine.

- The ES&S ExpressVote (in all-in-one mode) allows the voter to mark a ballot by touchscreen or audio interface, then prints a paper ballot card and ejects it from a slot. The voter has the opportunity to review the ballot, then the voter redeposits the ballot into the same slot, where it is scanned and deposited into a ballot box.
- The ES&S ExpressVoteXL allows the voter to mark a ballot by touchscreen or audio interface, then prints a paper ballot (cash-register tape format) and displays it under glass. The voter has the opportunity to review the ballot, then the voter touches the screen to indicate "OK," and the machine pulls paper ballot up (still under glass) and into the integrated ballot box.
- The Dominion ImageCast Evolution (ICE) allows the voter to deposit a hand-marked paper ballot, which it scans and drops into the attached ballot box. *Or*, a voter can use a touchscreen or audio interface to direct the marking of a paper ballot, which the voting machine ejects through a slot for review; then the voter

posited in the smart ballot box. The ballot box does not read the votes from the ballot; rather, depositing the ballot tells the system that it has permission to cast the vote that it had already recorded from the touchscreen.

[32] Some vendors, notably Scytl, have sold systems advertised as E2E-V in other countries. Those systems were not in fact E2E-V. Moreover, serious security flaws have been found in their implementations. See, e.g., [16].

redeposits the ballot into the slot, where it is scanned and dropped into the ballot box.

In all three of these machines, the ballot-marking printer is in the same paper path as the mechanism to deposit marked ballots into an attached ballot box. This opens up a very serious security vulnerability: the voting machine can mark the paper ballot (to add votes or spoil already-cast votes) after the last time the voter sees the paper, and then deposit that marked ballot into the ballot box without the possibility of detection.

Vote-stealing software could easily be constructed that looks for *undervotes* on the ballot, and marks those unvoted spaces for the candidate of the hacker's choice. This is very straightforward to do on optical-scan bubble ballots (as on the Dominion ICE) where undervotes are indicated by no mark at all. On machines such as the ExpressVote and ExpressVoteXL, the normal software indicates an undervote with the words NO SELECTION MADE on the ballot summary card. Hacked software could simply leave a blank space there (most voters wouldn't notice the difference), and then fill in that space and add a matching bar code after the voter has clicked "cast this ballot."

An even worse feature of the ES&S ExpressVote and the Dominion ICE is the *auto-cast* configuration setting (in the manufacturer's standard software) that allows the voter to indicate, "don't eject the ballot for my review, just print it and cast it without me looking at it." If fraudulent software were installed in the ExpressVote, it could change *all* the votes of any voter who selected this option, because the voting machine software would know *in advance of printing* that the voter had waived the opportunity to inspect the printed ballot. We call this auto-cast feature "permission to cheat" [4].

Regarding these all-in-one machines, we conclude:

- Any machine with ballot printing in the same paper path with ballot deposit is not *software independent*; it is *not* the case that "an error or fault in the voting system software or hardware cannot cause an undetectable change in election results." Therefore such all-in-one machines do not comply with the VVSG 2.0 (the Election Assistance Commission's Voluntary Voting Systems Guidelines).
- All-in-one machines on which all voters use the BMD interface to mark their ballots (such as the ExpressVote and ExpressVoteXL) *also* suffer from the same serious problem as ordinary BMDs: most voters do not review their ballots effectively, and elections on these machines are not contestable or defensible.
- The auto-cast option for a voter to allow the paper ballot to be cast without human inspection is particularly dangerous, and states must insist that vendors disable or eliminate this mode from the software. However, even disabling the auto-cast feature does not eliminate the risk of undetected vote manipulation.

Remark. The Dominion ImageCast Precinct ICP320 is a precinct-count optical scanner (PCOS) that also contains an audio+buttons ballot-marking interface for disabled voters. This machine can be configured to cast electronic-only ballots from the BMD interface, or an external printer can be attached to print paper optical-scan ballots from the BMD interface. When the external printer is used, that printer's paper path is *not* connected to the scanner+ballot-box paper path (a person must take the ballot from the printer and deposit it into the scanner slot). Therefore this machine is as safe to use as any PCOS with a separate external BMD.

Conclusion

Ballot-Marking Devices produce ballots that do not necessarily record the vote expressed by the voter when they enter their selections on the touchscreen: hacking, bugs, and configuration errors can cause the BMDs to print votes that differ from what the voter entered and verified electronically. Furthermore, in cases where the BMD-marked paper ballot does not record the expressed vote, the election system overall is not *contestable* or *defensible*, meaning that errors in elections conducted on compromised BMDs cannot be reliably detected or corrected, and that election officials cannot provide convincing evidence that correct reported outcomes of elections conducted using BMDs are indeed correct. Therefore BMDs should not be used by voters who can use hand-marked paper ballots.

All-in-one voting machines, that combine ballot-marking and ballot-box-deposit into the same paper path, are even worse. They have all the disadvantages of BMDs (they are neither contestable or defensible), and they can mark the ballot after the voter has inspected it. Therefore they are not even *software independent*, and should not be used by those voters who are capable of marking, handling, and visually inspecting a paper ballot.

When computers are used to record votes, the original transaction (the voter's expression of the votes) is not documented in a verifiable way.[33] When pen-and-paper is used to record the vote, the original expression of the vote *is* documented in a verifiable way (provided that secure chain of custody of paper ballots is maintained). Therefore, audits of elections conducted with BMDs cannot ensure that reported outcomes are correct, while audits of elections conducted with hand-marked paper ballots, counted by optical scanners, can.

[33] It is conceivable that cryptographic protocols used in E2E-V systems could be used to create BMD-based systems that are contestable and defensible, but no such system exists, nor, to our knowledge, has such a design been worked out in principle.

References

[1] A.W. Appel. Optical-scan voting extremely accurate in Minnesota. *Freedom to Tinker*, January 2009. https://freedom-to-tinker.com/2009/01/21/optical-scan-voting-extremely-accurate-minnesota/.

[2] A.W. Appel. End-to-end verifiable elections. *Freedom to Tinker*, November 2018. https://freedom-to-tinker.com/2018/11/05/end-to-end-verifiable-elections/.

[3] A.W. Appel. Florida is the Florida of ballot-design mistakes. *Freedom to Tinker*, November 2018. https://freedom-to-tinker.com/2018/11/14/florida-is-the-florida-of-ballot-design-mistakes/.

[4] A.W. Appel. Serious design flaw in ESS ExpressVote touchscreen: "permission to cheat". *Freedom to Tinker*, September 2018. https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/.

[5] J. Benaloh, M. Byrne, B. Eakin, P. Kortum, N. McBurnett, O. Pereira, P.B. Stark, , and D.S. Wallach. Star-vote: A secure, transparent, auditable, and reliable voting system. *JETS: USENIX Journal of Election Technology and Systems*, 1:18–37, 2013.

[6] R. K. Bothwell, K.A. Deffenbacher, and J.C. Brigham. Correlation of eyewitness accuracy and confidence: Optimality hypothesis revisited. *Journal of Applied Psychology*, 72:691–695, 1987.

[7] Election Assistance Commission. Voluntary voting systems guidelines 2.0, September 2017. https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.

[8] K. Deffenbacher. Eyewitness accuracy and confidence: Can we infer anything about their relation? *Law and Human Behavior*, 4:243–260, 1980.

[9] R. DeMillo, R. Kadel, and M. Marks. What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots, November 2018. https://ssrn.com/abstract=3292208.

[10] S.L. Desmarais, T.L. Nicholls, J. D. Read, and J. Brink. Confidence and accuracy in assessments of short-term risks presented by forensic psychiatric patients. *The Journal of Forensic Psychiatry & Psychology*, 21(1):1–22, 2010.

[11] D. Dunning, D.W. Griffin, J.D. Milojkovic, and L. Ross. The overconfidence effect in social prediction. *Journal of Personality and Social Psychology*, 58:568–581, 1990.

[12] S.P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. PhD thesis, Rice University, 2007.

[13] A.J. Feldman, J.A. Halderman, and E.W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 2007)*, August 2007.

[14] Verified Voting Foundation. The verifier – polling place equipment – november 2018, November 2018. https://www.verifiedvoting.org/verifier/.

[15] D. Kahnemann. *Thinking, fast and slow*. Farrar, Straus and Giroux, 2011.

[16] S. J. Lewis, O. Pereira, and V. Teague. Ceci n'est pas une preuve: The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system, 2019. https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf.

[17] M. Lindeman and P.B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security and Privacy*, 10:42–49, 2012.

[18] National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*. The National Academies Press, Washington, DC, September 2018.

[19] L. Norden, M. Chen, D. Kimball, and W. Quesenbery. Better Ballots, 2008. Brennan Center for Justice, http://www.brennancenter.org/publication/better-ballots.

[20] Office of the Minnesota Secretary of State. Minnesota's historic 2008 election, 2009. https://www.sos.state.mn.us/media/3078/minnesotas-historic-2008-election.pdf.

[21] E. Perez. Georgia state election technology acquisition: A reality check. OSET Institute Briefing, March 2019. https://trustthevote.org/wp-content/uploads/2019/03/06Mar19-OSETBriefing_GeorgiaSystemsCostAnalysis.pdf.

[22] K. Rayner and M.S. Castelhano. Eye movements during reading, scene perception, and visual search, 2009. Q J Experimental Psychology, 2009, August 62(8), 1457-1506.

[23] R.L. Rivest and J.P. Wack. On the notion of software independence in voting systems, July 2006. http://vote.nist.gov/SI-in-voting.pdf.

[24] Election Systems and Software. State of Georgia Electronic Request for Information New Voting System Event Number: 47800-SOS0000035, 2018. http://sos.ga.gov/admin/files/ESS%20RFI%20-%20Final%20-%20Redacted.pdf.

[25] P.B. Stark. Conservative statistical post-election audits. *Annals of Applied Statistics*, 2:550–581, 2008.

[26] P.B. Stark. Risk-limiting post-election audits: P-values from common probability inequalities. *IEEE Transactions on Information Forensics and Security*, 4:1005–1014, 2009.

[27] U. S. Election Assistance Commission. Effective designs for the administration of federal elections, June 2007. https://www.eac.gov/assets/1/1/EAC_Effective_Election_Design.pdf.

[28] J.T. Wixted and G.L. Wells. The relationship between eyewitness confidence and identification accuracy: A new synthesis. *Psychological Science in the Public Interest*, 2017.

EXHIBIT 6

July 16, 2019

Honorable Kathy Boockvar
Acting Secretary of the Commonwealth
Pennsylvania Department of State
Bureau of Commissions, Elections and Legislation
302 North Office Building, 401 North Street
Harrisburg, PA 17120

Dear Secretary Boockvar,

Pursuant to 25 P.S. § 3031.5, on behalf of the undersigned electors of the Commonwealth of Pennsylvania, we hereby request a re-examination of the ES&S ExpressVote XL electronic voting machine. We enclose at least ten (10) certifications of duly registered electors in the Commonwealth of Pennsylvania who seek this re-examination. We have enclosed a check for $450 payable to the Treasurer of the Commonwealth of Pennsylvania.

As you know, "[t]he Secretary's duty to re-examine the machines upon proper request is mandatory." *Banfield v. Aichele*, 51 A.3d 300, 314 (Commw. Ct. Penn. 2012), *aff'd sub nom. Banfield v. Cortes*, 110 A.3d 155 (2015).

We have attached a list of deficiencies in the ExpressVote XL which require attention during re-examination. We also note that the ES&S ExpressVote HW 2.1 used as a tabulator shares many of the same deficiencies as the ExpressVote XL.

We respectfully request that the Secretary of the Commonwealth re-examine the ExpressVote XL electronic voting machine and issue a report relating to the functionality of the system. We request that this re-examination be conducted expeditiously because several counties in the Commonwealth have chosen or are considering the ExpressVote XL, and all counties must act quickly to comply with the Department of State directive to select new voter-verifiable paper record voting systems no later than December 31, 2019.

If the Secretary of the Commonwealth determines that the attached deficiencies are compelling evidence to preemptively decertify the ExpressVote XL, we would withdraw our petition for re-examination.

Respectfully submitted,

Ronald A. Fein, Legal Director
John C. Bonifaz, President
Free Speech For People
1320 Centre St. #405
Newton, MA 02459
(617) 244-0234
rfein@freespeechforpeople.org
jbonifaz@freespeechforpeople.org

Susan Greenhalgh
Vice President of Policy and Program
National Election Defense Coalition

Kevin Skoglund
Chief Technologist
Citizens for Better Elections,
A member of the Protect Our Vote Philly Coalition

Petition Pages

200 signatures by duly registered electors in the Commonwealth of Pennsylvania

From the counties:

Philadelphia
Allegheny
Montgomery
Bucks
Delaware
Westmoreland
Northampton

Attachment: ES&S ExpressVote XL Deficiencies

We seek re-examination of the ES&S ExpressVote XL voting machine on these grounds.

1. Tampering with Ballot Cards

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7 (12), which requires that a voting system:

> "Provides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards."

Since the Pennsylvania Certification of ES&S EVS 6.0.2.1, security researchers discovered[1] that the ExpressVote XL exposes a ballot card cast by a voter to an internal printer prior to tabulation and impoundment. The internal printer is controlled exclusively by software which has the ability to tamper with the content of the ballot card. A malfunctioning or manipulated ExpressVote XL could add, modify, or invalidate votes *after* the voter has viewed, confirmed, and cast her ballot. It could change election outcomes without detection. This is a very high impact defect which affects the integrity and auditability of the voting system.

This defect violates the principle of software independence: "A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome."[2] Software independence will be VVSG 2.0 Guideline 9.1 and is recognized as necessary for effective auditing. It is a "crucial" requirement for evidence-based elections as defined by Professors Philip Stark and David Wagner: "All three components are crucial. The risk-limiting audit relies on the integrity of the audit trail, which was created by the software-independent voting system (the voters themselves, in the case of paper ballots) and checked for integrity by

---

[1] References available at:
https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine
https://freedom-to-tinker.com/2018/10/22/an-unverifiability-principle-for-voting-machines
https://securiosa.com/posts/how_the_expressvote_xl_could_alter_ballots.html
https://securiosa.com/posts/how_expressvote_barcodes_could_be_modified.html

[2] "On the Notion of Software-Independence in Voting Systems," Ronald Rivest and John Wack, *Philosophical Transactions of The Royal Society*, August 6, 2008, Page 1, *available at* https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

the compliance audit."[3] Acceptable ballot security procedures to prevent tampering must include ensuring auditability and enabling evidence-based elections.

It is common sense that a voting machine should not have the ability to change votes after the voter has confirmed and cast her ballot. The same reasoning is evident and explicitly stated in § 1222, 25 P.S. § 3062 (a), "No person while handling the ballots shall have in his hand any pencil, pen, stamp or other means of marking or spoiling any ballot." Acceptable ballot security procedures to prevent tampering must include a similar restriction on any machine while handling the ballots.

2. Chronological Ballot Storage

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7 (1), which requires that a voting system:

> "Provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting."

The ExpressVote XL ballot container stores ballot cards in chronological order. It allows any poll worker or election official who knows even limited details about the sequence of voters to violate the absolute secrecy of one or more voters. A voter's ballot could be determined by referencing the order of voters in the poll book or on the poll list, by counting from the first or last ballot in the set, or by counting from another identifiable ballot, such as one with a known write-in vote. This is a significant defect. Chronologically ordered ballots fail to protect voters' right to a secret ballot and enable information harvesting, vote buying and selling, and voter coercion.

The Pennsylvania Department of State has long held the position that voting systems with chronologically ordered ballots violate absolute secrecy. Dr. Michael Shamos, statutory examiner for the Secretary of the Commonwealth from 1980 to 2010, testified to a U.S. Senate committee in 2007, "Even paper trail advocates recognize that scrolled paper trails make it easy, not just possible, to determine how every voter in a precinct voted. The first voter's ballot is first on the tape; the last voter's is last; and everyone else's is sequential order in between. A simple comparison between the paper trail and the poll list gives away everyone's vote, in violation of the Section 201 requirement of a secret ballot. Even

---

[3] "Evidence-Based Elections," Philip Stark and David Wagner, *IEEE Security and Privacy*, May 8, 2012, Page 2, *available at* https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

if only two percent of the vote is audited, it means that two percent of the voters are at risk of having their votes revealed."[4]

The "Conditions of Certification" for ES&S EVS 6.0.2.1 do not require any procedures to randomize the order of ballot cards or to otherwise protect ballot secrecy. Even if procedures had been required, the voting system cannot depend on procedures—which may not be consistently or correctly employed—to restore ballot secrecy. The voting system itself must provide it.

3. Ballot Cards Colored by Party

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (e):

> "In primary elections, the Secretary of the Commonwealth shall choose a color for each party eligible to have candidates on the ballot and a separate color for independent voters. The ballot cards or paper ballots and ballot pages shall be printed on card or paper stock of the color of the party of the voter and the appropriate party affiliation or independent status shall be printed on the ballot card or at the top of the paper ballot and on the ballot pages."

The ballot cards used by the ExpressVote XL are made of solid white thermal paper. The card stock is not colored for each party. The ballot cards are blank and do not have the appropriate party affiliation or independent status printed on the ballot card.

In primary elections, the party affiliation of a voter is determined definitively when the voter checks in, signs the poll book, and is given a ballot card. Before the voter may vote, a poll worker must configure the ExpressVote XL to display the ballot style of the voter's party. If ballot cards are not on colored card stock with the party affiliation, the voter can tell the poll worker a different party affiliation, cast fraudulent votes in another party's election, and the impounded ballot card would show no evidence of the fraud. Colored card stock with the party affiliation printed also reduces the chance that a poll worker will set the wrong ballot style for a voter by accident.

It should be demonstrated that the required ballot cards are possible and that the ExpressVote XL is capable of using them.

---

[4] Testimony before the U.S. Senate Committee on Rules and Administration, July 25, 2007, http://euro.ecom.cmu.edu/people/faculty/mshamos/Senate20070725.pdf

4. Serially Numbered Perforated Stubs

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (f):

> "…Each ballot card shall have an attached serially numbered perforated stub, which shall be removed by an election officer before the ballot card is deposited in the district automatic tabulating equipment or in a secure ballot box. The name of the county, and a facsimile of the signature of the members of the county board shall be printed on the ballot card stub."

The ExpressVote XL violates § 1112-A, 25 P.S. § 3031.12 (b)(6), which requires a procedure for a district using paper ballots or ballot cards:

> "Following the completion of his vote, the voter shall leave the voting booth and return the ballot to the election officer by a means designed to insure its secrecy; upon removal of the stub of the ballot by the election officer, the voter shall insert the ballot into the district automatic tabulating equipment or, in the event district tabulation is not provided for by the voting system or such district tabulation equipment is inoperative for any reason, into a secure ballot box. No ballot card from which the stub has been detached shall be accepted by the election officer in charge of such equipment or ballot box, but it shall be marked "spoiled" and shall be placed in the envelope marked "Spoiled Ballots"."

In addition, § 1113-A, 25 P.S. § 3031.13 (a) requires that, after the polls have been closed, the serially numbered stubs be used as evidence of the number of ballots issued to electors so that number may be announced in the polling place and recorded.

The ballot cards used by the ExpressVote XL do not have attached serially numbered perforated stubs. The ballot cards are blank and do not have a facsimile of the signature of the members of the county board printed on the ballot card stub.

The ExpressVote XL is designed such that a voter does not handle the ballot after the completion of her vote. The voter cannot leave the voting booth with the ballot card to return it to an election officer. The election officer does not have an opportunity to remove the stub. The election officer is not able to verify that the stub has not been detached from the ballot card in order to mark it as spoiled.

Without serially numbered stubs and signatures, any person could forge ballot cards. Forged ballot cards can be submitted for tabulation secretly and independently because, unlike most district tabulating equipment, the ExpressVote XL tabulator is inside a privacy curtain, where election workers cannot observe voter activity.

Serially numbered stubs prevent "chain voting." Professor Doug Jones describes the fraud technique and the defense against it: "The organizer of the chain needs one valid ballot to begin with. He then marks this ballot and gives it to a voter willing to participate in the fraud. With each participant, the organizer instructs the participant to vote the pre-voted ballot and bring back a blank ballot from the polling place. Voters are paid for the blank ballot. The best defense against chain voting involves printing a unique serial number on a removable stub on each ballot. When ballots are issued to voters, the stub numbers should be recorded. No ballot should be accepted for deposit in the ballot box unless its stub number matches a recently issued number. Finally, to preserve the voter's right to a secret ballot, the stub should be torn from the ballot before it is inserted in the ballot box."[5]

It should be demonstrated that the required ballot cards are possible and that the ExpressVote XL is capable of using them.[6]

5. Valid Marks on a Ballot Card

The ExpressVote XL violates § 1112-A, 25 P.S. § 3031.12 (b)(2-4), which applies to districts using paper ballots or ballot cards.

The three procedures in § 3031.12 (b)(2-4) each specify that a voter shall vote on a ballot card by "making a cross (X) or check (✓) mark or by making a punch or mark sense mark in the square opposite the name" of the candidate, the party, the write-in position, or the answer to a ballot question. The type of mark and its position relative to the name is specified six times in total.

The ExpressVote XL does not make a cross or check mark or make a punch or mark sense mark, nor does it permit a voter to do so. On an ExpressVote ballot card there is no

---

[5] "On Optical Mark-Sense Scanning," Douglas W. Jones, in *Towards Trustworthy Elections*, 2010, Page 178, *available at* http://homepage.cs.uiowa.edu/~jones/voting/OpticalMarkSenseScanning.pdf

[6] Upon information and belief, the ExpressVote XL could be made to use compliant ballot cards, as ES&S apparently offered serially numbered cards in Michigan. However, the machines certified and used in Pennsylvania do not use compliant ballot cards.

square opposite the name in which to place any mark. Instead a barcode is printed near the top of the ballot card, separate and far from the name. The barcodes are not even listed in the same order as the names are listed.

The type of mark and its position relative to the name is an important requirement. A valid mark next to a corresponding name allows the voter to verify that each vote matches her intent prior to casting the ballot card, ensuring the principle of "cast as intended." A valid mark next to a corresponding name allows election officials or any person to easily observe, count, and audit the vote, without software or special equipment. The Election Code intends for the meaning of each vote to be transparent and software independent.

6. Indicated Voting Positions on Ballot Cards

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (a)(2).

> "The pages placed on the voting device shall be of sufficient number to include, following the listing of particular candidates, the names of candidates for any nonpartisan offices and any measures for which a voter may be qualified to vote on a given election day, provided further that for municipal, general or special elections, the first ballot page shall list in the order that such political parties are entitled to priority on the ballot, the names of such political parties with designating arrows so as to indicate **the voting square or position on the ballot card** where the voter may insert by one mark or punch the straight party ticket of his choice." (Emphasis added).

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (d).

> "In partisan elections **the ballot cards shall include a voting square or position** whereby the voter may by one punch or mark record a straight party ticket vote for all the candidates of one party or may vote a split ticket for the candidates of his choice." (Emphasis added).

The ExpressVote XL lists political parties on the touchscreen. If a voter makes a straight party choice, the ExpressVote XL will later record the selection by printing a barcode and human-readable text on the ballot card. This process does not meet the requirements.

An electronic voting machine is required to list the political parties with arrows to indicate positions *on the ballot card*. The ExpressVote XL does not indicate voting positions on the ballot card, nor does it use any "designating arrows." In fact, there are no fixed positions on the ballot card—the location of the barcode and human-readable text will vary depending on the voter's other selections.

7. Unlawful Assistance in Voting

The ExpressVote XL would require voters to violate § 1218, 25 P.S. § 3058 (a):

> "No voter shall be permitted to receive any assistance in voting at any primary or election, unless there is recorded upon his registration card his declaration that, by reason of blindness, disability, or inability to read or write, he is unable to read the names on the ballot or on the voting machine labels, or that he has a physical disability which renders him unable to see or mark the ballot or operate the voting machine, or to enter the voting compartment or voting machine booth without assistance, the exact nature of such condition being recorded on such registration card, and unless the election officers are satisfied that he still suffers from the same condition."

The ExpressVote XL would require election officers to violate § 1111-A, 25 P.S. § 3031.11 (b):

> "At the polling place on the day of the election, each voter who desires shall be instructed, by means of appropriate diagrams and a model, in the operation of the voting device before he enters the voting booth. If any voter shall ask for further instructions concerning the manner of voting after entering the voting booth, any election officer may give him **audible instructions without entering such booth**, but no such election officer shall when giving such instructions in any manner request, suggest or seek to persuade or induce any such voter to vote any particular ticket or for any particular candidate or other person or for or against any particular question." (Emphasis added).

The ExpressVote XL would require voters and election officers to violate § 1220, 25 P.S. § 3060 (a):

> "… No elector shall be allowed to occupy a voting compartment or voting machine booth already occupied by another, except when giving assistance as permitted by this act."

When any voter using the ExpressVote XL wants to spoil her ballot card or wants to handle the ballot card for physical review, they must select an option in the interface to "Quit." The ExpressVote XL displays on screen (and reads into the audio ballot) the message: "Vote Session Canceled. Your ballot was canceled with no votes cast. Ask an election official for help." The ExpressVote XL emits a chiming sound to alert a poll worker. A poll worker must enter the voting booth, touch a designated location on the screen, enter an administrator password using an on-screen keypad, and retrieve the ballot card from the windowed container where it is held.

All voters have the right to spoil their ballot card. (§ 1112-A, 25 P.S. § 3031.12 (b)(5): "Any voter who spoils his ballot may return it and secure another.") A voting system is required to allow voters to spoil their ballot card. (§ 1107-A, 25 P.S. § 3031.7 (10): "If it is of a type that uses paper ballots or ballot cards to register the vote and automatic tabulating equipment to compute such votes, the system shall provide that a voter who spoils his ballot may obtain another ballot".) The ExpressVote XL does not allow a voter to spoil her ballot card without a poll worker entering the booth in violation of the above requirements.

Voters with disabilities may wish to handle the ballot card to verify it using a magnifier or other personal assistive device. This is only possible with poll worker assistance and is only permitted if the voter has previously recorded their disability on their voter registration. Voters who have recorded a disability may "select a person" to enter the voting booth (§ 1218, 25 P.S. § 3058 (b)). This person could be a poll worker, but if another person has already been selected to assist, a poll worker entering the booth would violate the above requirements.

This deficiency has consequences for both the voter and the poll worker. § 1830, 25 P.S. § 3530 ("Unlawful assistance in voting") specifies that any voter "who, without having made the declaration under oath or affirmation required by section 1218 of this act … shall permit another to accompany him into the voting compartment or voting machine booth" or "any person who shall go into the voting compartment or voting machine booth with another while voting or be present therein while another is voting" is guilty of a misdemeanor and will be sentenced to pay a fine, imprisonment, or both.

8. Poll Workers in the Booth and Ballot Secrecy

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7 (1), which requires that a voting system:

> "Provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting."

The ExpressVote XL violates the Help America Vote Act of 2002 (HAVA), § 301(a)(1)(A)(ii), which requires that a voting system shall:

> "provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error)"

The previously described procedure for spoiling a ballot card on the ExpressVote XL allows the poll worker, upon entering the voting booth, to view the selections on the ballot card through the windowed container and while handling the ballot card. The poll worker will look directly at the ballot card while extracting it from the container. The poll worker can see and know for whom the voter has voted or is voting. The ExpressVote XL does not allow any voter to privately and independently correct an error through the issuance of a replacement ballot.

It is also noteworthy that this procedure reveals an administrator password to the voter. The poll worker enters the password in front of the voter using an on-screen keypad and each character is displayed in the input field as it is typed. During public demonstrations of the ExpressVote XL, several members of the public reported easily observing the administrator password used.

9. Accessibility

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7(5), which requires that a voting system:

> "Permits **each** voter to vote for any person and any office for whom and for which he is lawfully entitled to vote, whether or not the name of such

person appears upon the ballot as a candidate for nomination or election." (Emphasis added).

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7(3), which requires that a voting system:

> "Permits **each** voter…to vote a straight political party ticket…by one mark or act, to vote for all the candidates of one political party for every office to be voted for, and every such mark or act shall be equivalent to and shall be counted as a vote for every candidate of the political party so marked including its candidates for presidential electors, except with respect to those offices as to which the voter has registered a vote for individual candidates of the same or another political party or political body, in which case the automatic tabulating equipment shall credit the vote for that office only for the candidate individually so selected, notwithstanding the fact that the voter may not have individually voted for the full number of candidates for that office for which he was entitled to vote." (Emphasis added).

The ExpressVote XL violates the Help America Vote Act of 2002 (HAVA), § 301(a), which requires that a voting system shall:

> 1.A.i: "permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."
>
> 1.A.ii: "provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error)."
>
> 3.A: "be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

To the extent that any HAVA Section 261 funds are involved, use of the ExpressVote XL also violates HAVA § 261 (b):

> An eligible State and eligible unit of local government shall use the payment received under this part for— (1) making polling places . . . accessible to individuals with disabilities, including the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

The Pennsylvania Certification of ES&S EVS 6.0.2.1 included an accessibility testing report on pages 68-94. The ExpressVote XL was harshly reviewed by the accessibility test group.

"Every participant had at least one problem, despite relatively high election knowledge and digital experience, suggesting that the issue would be more severe for voters without these personal resources to help them understand what is happening." (Page 70)

"None of the participants could verify the ballot in the glass cage:
- Blind voters had no access to the ballot to use personal technology
- Low vision voters could not position the ballot so they could read the small text
- Other voters had problems reading the ballot because of glare and because the sides of the ballot were obscured by the cage.
- Although it is possible to have the ballot ejected to handle it while verifying, the procedure is unclear and it requires voters to tell the system they want to "Quit" and call a poll worker." (Page 74)

Participants in the accessibility study found the ExpressVote XL made it difficult to cast write-in votes. For a vote for a write-in candidate to count, spelling must be perfect and "[a]ll of the participants knew that a misspelled write-in would not be counted, but could not figure out how to review what was typed." (Pages 70-71, 86-87). Furthermore, the ExpressVote XL did not allow participants to review any write-in votes through the audio ballot because the text of the write-in is not encoded in the barcodes printed on the ballot card. (Pages 73, 75, 88).

Voters relying on the audio ballot had significant issues with voting a "straight-party" ticket. If a voter selects a single candidate outside the straight-party ticket, the ExpressVote XL deselects all other candidates, without informing the audio-guided voter. The accessibility testing report describes this problem as "not only a failure to vote independently, but identifying and solving the problem requires revealing their votes to a poll worker or assistant." (Pages 68-69). The audio ballot also "does not announce the party of each candidate. This made it impossible to

complete tasks based on party, including confirming straight party selections." (Pages 83, 86).

The Pennsylvania Department of State's accessibility testing report makes it clear that the ExpressVote XL is not accessible for individuals with disabilities "in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters." Most importantly for these voters, it does not "permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."

10. The *Stein* Settlement

The ExpressVote XL violates the settlement in *Stein v. Cortes*:[7]

> "2. The Secretary will only certify new voting systems for use in Pennsylvania if they meet these criteria:
>
> a. The ballot on which each vote is recorded is paper;
> b. They produce a voter-verifiable record of each vote; and
> c. They are capable of supporting a robust pre-certification auditing process.
>
> 3. The Secretary will continue to direct each county in Pennsylvania to implement these voting systems by the 2020 primaries, so that every Pennsylvania voter in 2020 uses a voter-verifiable paper ballot."

The ExpressVote XL does not provide the voter a paper ballot, as that term is defined by 25 P.S. § 3031.1. Instead, it provides a "ballot card." A paper ballot is a piece of paper with the options pre-printed, whereas a ballot card only prints a voter's selection on blank piece of paper. *See id.* (defining paper ballot as "a printed paper ballot which conforms in layout and format to the voting device in use" and ballot card as "a card which is compatible with automatic tabulating equipment and on which votes may be registered").

Because the ExpressVote XL does not provide a paper ballot, Pennsylvania voters in counties using the ExpressVote XL will not receive a voter-verifiable paper ballot in 2020, in contravention of the *Stein* settlement's requirement that the Secretary "direct each county in Pennsylvania to implement these voting systems by the 2020 primaries, so that every Pennsylvania voter in 2020 uses a voter-verifiable paper ballot."

---

[7] *Stein v. Cortes*, No. 16-cv-06287, ECF No. 108 (E.D. Pa. Nov. 28, 2018), *available at* http://bit.ly/SteinSettlement.

EXHIBIT 7

COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

REPORT CONCERNING THE REEXAMINATION RESULTS OF ELECTIONS SYSTEMS AND SOFTWARE EXPRESSVOTE XL

Issued By:

Kathy Boockvar

Kathy Boockvar
Acting Secretary of the Commonwealth
September 3, 2019

REEXAMINATION RESULTS OF ELECTION SYSTEMS AND SOFTWARE EXPRESSVOTE XL

I. INTRODUCTION

Article XI-A of the Pennsylvania Election Code, 25 P.S. §§ 3031.1 *et seq.* (the "Code"), authorizes the use of electronic voting systems. Section 1105-A of the Code, 25 P.S. § 3031.5(a), allows any ten or more qualified electors of Pennsylvania to request a reexamination of an electronic voting system certified by the Secretary of the Commonwealth ("Secretary"). On July 17, 2019, the Acting Secretary of the Commonwealth ("Acting Secretary") received a Petition to Reexamine the ExpressVote XL (the "Petition"). A copy of that Petition is attached hereto as Appendix A.

The ExpressVote XL was initially examined and certified as part of the ES&S EVS 6021 electronic voting system to both federal and state voting system standards by the Election Assistance Commission ("EAC") on November 12, 2018 and by the Secretary of the Commonwealth on November 30, 2018.

The Petition sets forth ten claims for why the Acting Secretary should de-certify the ExpressVote XL (XL). After a thorough and considered review of the Petition, the Acting Secretary has determined that claims three through seven, nine, and ten amount to purely legal arguments which do not apply to reexamination or certification of an electronic voting system. With respect to claims one, two, and eight, the Acting Secretary, in consultation with the Department of State's expert voting system examiner, reexamined the XL and concluded that the XL meets the requirements of Section 1107-A of the Pennsylvania Election Code, 25 P.S. § 3031.7, and can be safely used to conduct elections in the Commonwealth.

To satisfy the Secretary's statutory obligation to reexamine the XL system based on claims one, two, and eight in the Petition, the Pennsylvania Department of State ("Department") entered into an agreement with expert professional consultant SLI Compliance ("SLI") to conduct a focused reexamination of the XL. Jesse Peterson, Security Specialist, and Mike Santos, Senior Test Manager, served as the examiners ("Examiners").

The off-site reexamination was conducted at the laboratory of SLI Compliance located in Wheat Ridge, Colorado. The Department was represented by Sindhu Ramachandran, Voting System Analyst, for the reexamination on August 7 and 8, 2019. The Examiners then provided findings from the examination, and the test results and conclusion have been included in further sections of this report.

II. THE EXPRESSVOTE XL VOTING SYSTEM

ExpressVote XL

ExpressVote XL is a polling place voting device that provides touch screen vote capture which incorporates printing of a voter's selections as a paper voter-verifiable record and tabulation scanning into a single unit. The system uses a touch-operated screen and/or assistive technology to capture a voter's choices. The integrated thermal printer prints the voter's choices on a voter-verifiable paper vote summary record and the system scans and saves an image of the printed vote summary record. The vote summary record is the voter-verifiable paper record with plain text words of the votes to be cast, which, once cast, will be retained as the official vote record and used for audits and/or recounts.

The software/firmware version of ExpressVote XL certified as part of the EVS 6021 system is 1.0.1.0 and the hardware version is 1.0.

Test Materials

Test support materials utilized during the examination included:

- Two ExpressVote XL devices
- CFAST cards for both ExpressVote XL devices
- Thermal receipt paper for the Expressvote XL
- Activation card stock for processing vote summary records on the ExpressVote XL
- CFAST Cards
- USB thumb drives

- Pens to modify marks

III. REEXAMINATION APPROACH

A. Approach Summary

The reexamination focused on the alleged violations of Sections 1107-A(1) and (12) of the Pennsylvania Election Code, 25 P.S. §§· 3031.7(1) & (12), relating to vote record secrecy and security, set forth in items one, two, and eight of the petition. The Examiner evaluated the petition and relevant system documentation to develop test protocols for the examination. All hardware necessary to perform the reexamination was supplied by ES&S. Software and firmware for the EVS 6021 voting system was obtained from the Voting System Test Lab ("VSTL") that performed the EAC certification test campaign. The Examiner installed the firmware using the appropriate media and process for installation.

The test protocols separated the requirements for the reexamination into three main areas of test execution: (1) Security Analysis and Evaluation; (2) Functional Testing; and (3) Documentation Review.

1. Security Analysis and Evaluation

The Examiners performed security analysis of the XL, with special consideration to the items set forth in the Petition. The Examiners' security specialist reviewed the system to evaluate the system's security protocols. In order to gather details for the functional test execution, SLI included a review of internal security, functional and architectural diagrams, software specification, as well as ExpressVote XL hardware schematic documentation. The analysis was done to reexamine the system architecture and operations and to plan a comprehensive approach to analyze and evaluate each allegation. The Examiners also utilized the vulnerability assessment performed during the initial examination of the EVS

6021 voting system. This evaluation was used during test planning to identify the specific test cases to be executed during the functional testing and documentation review phases.

2. Functional Testing

The functional testing phase involved SLI personnel executing test cases identified during the security analysis and evaluation. This phase provided a means to assess the security and functional properties of the voting system under examination to ascertain whether they provide acceptable security procedures to prevent tampering with or substitution of vote summary records, as required by the Pennsylvania Election Code at 25 P.S. § 3031.7(12). The Examiner also used the functional testing to evaluate compliance of the system to the Pennsylvania Election Code requirement at 25 P.S.§ 3031.7(1) to ascertain whether the system provides for processes and procedures to maintain the secrecy of a voter's ballot.

3. Documentation Review

The documentation review phase consisted of reviewing the ES&S EVS 6021 voting system documentation to verify that appropriate processes and procedures are in place to provide acceptable security and privacy as required by 25 P.S.§§ 3031.7(1) and (12).

IV. Examination Results and Discussion

A. Examination Results and Discussion regarding Allegation #1

The Petition's allegation number one alleges that the XL violates Section 1107-A(12) of the Pennsylvania Election Code, 25 P.S. § 3031.7(12), which requires that a voting system "provides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards," because it does not provide acceptable procedures to prevent tampering.

As detailed below, The Examiner evaluated these claims and determined through security analysis and evaluation, functional testing, and documentation review that the XL **does not** violate Section 1107-A(12) of the Pennsylvania Election Code because it has

protocols and mechanisms to provide for acceptable security procedures to prevent tampering with or substitution of the vote summary records. The results of the Examiner's documentation review and testing are summarized in the following paragraphs of this section.

1. Security Analysis and Evaluation

The security specialist reviewed the internal security, functional and architectural diagrams, software specifications, as well as the XL hardware schematic documentation. The Examiners also utilized the vulnerability assessment performed during the initial examination of the EVS 6021 voting system. The Examiners gathered information about the system security protocols in place to prevent undetectable malicious manipulation of the XL, as well as information about the programmatic and physical access controls in place to prevent tampering. The Examiners then used the information gathered during this evaluation to identify specific test cases to be executed during the functional testing and documentation review phases.

2. Functional Testing

The XL was set up following all the physical security measures described in the relevant system documentation. The Examiners reviewed and tested each of the physical security measures in place, which demonstrated that different system access points and the CFAST cards could not be reached without proper keys and tools. The Examiners then performed a hash code validation successfully, confirming that the installed image matched the certified image.

The Examiners installed the trusted build and loaded a test general election on the XL devices used for the testing effort. The security specialist tried to penetrate the system using the system access points/ports and was unsuccessful. The Examiner also performed a hash code validation on the XL after the tests to confirm that the trusted build firmware was still present on the device. The Examiners confirmed that any modifications to the files on the CFAST cards would be identified as a mismatch during hash code validation and hence

any unauthorized changes would be detected.

The Examiners demonstrated the XL voting process and reviewed the system schematics and software actions. The voting process was demonstrated as follows: the terminal is opened for voting and the voter inserts a blank activation card. The voter selects the candidate choices and then selects the "Print" button. The XL prints the voter's choices on a paper vote summary record using the thermal printer. The vote summary record is then scanned and presented to the voter via the front facing voter verification window. The voter reviews and verifies the vote summary record and selects the "Cast" button. The system then saves and tabulates the votes and deposits the printed vote summary record into the collection bin without being re-scanned. During the examination of the system it was observed that the location of the print head, after the initial print, allows the vote summary record to pass to the collection bin without making contact with the print head again during the vote summary record deposit process.

The Examiners also carefully evaluated the voting process to identify any distinct cues during the printing process and observed that the printing process was audible and thus detectable. Hence, a successful attempt to activate the printer to print on the vote summary record after the voter verifies his or her selections would be heard.

The Examiners also attempted to change the tabulation of the vote by modifying the bar code on the paper vote summary record after verification by the voter but were unsuccessful. Attempts were also made to insert and tabulate modified bar codes by the system and those attempts too were unsuccessful.

3. Documentation Review

The Examiners conducted documentation review to determine if there are acceptable security processes in place to prevent unauthorized access or tampering, and to determine if there are mechanisms in place to identify if any unauthorized or malicious acts have taken place. The system documentation cited multiple procedures in place to ensure that the security of the XL is maintained, including: warehouse security for storage/maintenance/transportation, poll worker selection, poll worker training, physical

security of the polling place environment, physical security of the device (keys, security screws, tape, other tamper resistant/evident items), USB security, bar code security, programmatic security of the XL, as well as system auditing. The Examiner reported that the system executables and bar codes have mechanisms in place to detect unauthorized modification. Configuration of the paper vote summary record also allows the voter-verifiable text to be formatted with options to leave no blank lines between contest and selections, which prevents malicious software from leaving out a voter's selections and/or filling them in after a voter reviews their vote summary record.

B. Examination Results and Discussion regarding Allegation #2

The Petition's allegation number two alleges that the XL violates Section 1107-A(1) of the Pennsylvania Election Code, 25 P.S. § 3031.7(1), which requires that a voting system "provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting," because it stores the voter verified paper records in chronological order.

As detailed below, the Examiners evaluated these claims and determined through security analysis and evaluation, functional testing, and documentation review that the XL **does not** violate Section 1107-A(1) of the Pennsylvania Election Code because, when used in accordance with statutory and recommended procedures for maintaining proper chain of custody and canvassing votes, it provides for voting in "absolute secrecy," with exception for voters who are receiving assistance.

1. Security Analysis and Evaluation

The security specialist reviewed the internal security, functional and architectural diagrams, software specifications, as well as the XL hardware schematic documentation. The Examiners also utilized the vulnerability assessment performed during the initial examination of the EVS 6021 voting system. The Examiners gathered information about the system security protocols and procedures in place to prevent and detect unauthorized access to the ballot bin and to maintain voter secrecy during the process of voting and after the close of polls. The Examiners then used the information gathered during this evaluation to

identify specific test cases to be executed during the functional testing and documentation review phases.

2. Functional Testing

The Examiners completed vote sessions and demonstrated the actions at close of polls by the poll worker. The Examiners concluded that in accordance with recommended procedures, once an election has been closed, a poll worker will not be handling the paper vote summary records which are sealed in the collection bins. The Examiners provided a recommendation suggesting that processes to randomize vote summary records should be performed at the county office in accordance with the Pennsylvania Election Code, which will be a required condition for use of this system.

3. Documentation Review

The Examiners concluded that system documentation identifies procedures recommended by the vendor during implementation and operation to prevent violation of vote record secrecy, including: physical security to prevent and/or detect unauthorized attempts to access the paper vote summary records, assigning voters in a relatively equal distribution among multiple devices, as well as assigning multiple officials from different parties to handle vote record collection bins. In addition, vote record secrecy is maintained when statutory procedures for commingling ballots is conducted prior to canvass and storage by the county board of elections.

C. Examination Results and Discussion regarding Allegation #8

The Petition's allegation number eight alleges that the XL violates Section 1107-A(1) of the Pennsylvania Election Code, 25 P.S. § 3031.7(1), which requires that a voting system "provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting," because it requires a voter to request assistance from a poll worker during the process of "spoiling" the paper vote summary record when the voter made an error during the process of voting.

As detailed below, the Examiners evaluated these claims and determined through security analysis and evaluation, functional testing, and documentation review that the XL **does not** violate Section 1107-A(1) of the Pennsylvania Election Code because, when used in the context of proper statutory and recommended procedures for polling place setup and poll worker training, it provides for voting in "absolute secrecy," with exception for voters who are receiving assistance in the voting booth.

1. Security Analysis and Evaluation

The security specialist reviewed the internal security, functional and architectural diagrams, software specifications, as well as the XL hardware schematic documentation. The Examiners also utilized the vulnerability assessment performed during the initial examination of the EVS 6021 voting system. The Examiners gathered information about the system security protocols and procedures in place to prevent unauthorized access to the paper vote summary records and to preclude unauthorized access to the system administration screen used during the process of assisting voters who need to spoil their ballots before they are cast. The Examiners also evaluated what, if any, malicious activity could be accomplished if an unauthorized person or persons learned the passcode used to access the system administration screen. The Examiners then used the information gathered during this evaluation to identify specific test cases to be executed during the functional testing and documentation review phases.

2. Functional Testing

To test this Petition item, the Examiners demonstrated the process of spoiling a vote summary record and concluded that appropriate voter and poll worker training and instructions on the screen can ensure vote record secrecy. This will also be made a condition of this recertification report. The allegation about the password compromise was also reviewed and the Examiners determined that a compromise of all the characters of the supervisor password would be very difficult, and an audible chime sounds after three failed attempts to enter the password. The Examiners noted that even if the password was known to an unauthorized person, they would not be able to access any functions related to voting

or tabulation and any actions performed by the session user are recoverable. The Examiners also noted that the position of the poll worker during the process doesn't lend itself to easily viewing the voter's choices, and also pointed out that since the voter has decided to spoil the vote summary record it is not his/her final intended vote selection.

3. Documentation Review

The Examiners concluded that the system documentation identifies multiple procedures to protect voter privacy and prevent the compromise of the supervisor password. Please refer to Section V, Additional Conditions for Certification, for details regarding the required procedures.

V. Additional Conditions for Certification

Given the results of the reexamination that occurred in August 2019, and the findings and recommendations of the Examiners, **the Acting Secretary of the Commonwealth maintains the certification of the XL subject to the following additional conditions:**

A. Jurisdictions selecting the XL must implement proper poll closing and vote record transportation procedures to ensure that collection bins containing paper vote summary records are sealed and transported with proper chain of custody to the county office. Poll worker training must include the details of the procedures to ensure that collection bins remain sealed until delivered to the county office. Collection bins must be opened in the presence of board of election members and must be commingled before canvass and storage, in a manner consistent with the procedure outlined for the canvassing of absentee ballots under Section 1308(e) of the Election Code, 25 P.S. § 3146.8(e).

B. Jurisdictions implementing the XL must ensure that vote summary record instructions include specific voter and poll worker instructions added on the screen detailing spoiling procedures and cues to protect voter privacy. In addition, poll worker training must:

- Emphasize the need to obscure any view of the paper vote summary record during the process of spoiling the record;

- Educate poll workers on the proper steps to be taken when they respond to a voter request for spoiling the vote summary record to ensure that the secrecy of the spoiled record is maintained. These steps include ensuring that the voter intends to spoil the record, has read the instructions on the screen and has been informed by the poll worker how to prevent inadvertent view of the vote summary record before the poll worker enters inside the privacy curtain;

VI. Conclusion

As a result of the reexamination, and after consultation with the Department's staff, counsel and the Examiners, the Acting Secretary of the Commonwealth concludes that the ExpressVote XL certified as part of the EVS 6021 voting system can be safely used by voters at elections, as provided in the Pennsylvania Election Code, and meets all of the requirements set forth in the Election Code, **provided the voting system is implemented under the conditions listed in Section IV of the initial certification report released on November 30, 2018 and the conditions listed in Section V of this report**. Accordingly, the Acting Secretary maintains the certification of EVS 6021 - ExpressVote XL for use in this Commonwealth.

Appendix A

July 16, 2019

Honorable Kathy Boockvar
Acting Secretary of the Commonwealth
Pennsylvania Department of State
Bureau of Commissions, Elections and Legislation
302 North Office Building, 401 North Street
Harrisburg, PA 17120

Dear Secretary Boockvar,

Pursuant to 25 P.S. § 3031.5, on behalf of the undersigned electors of the Commonwealth of Pennsylvania, we hereby request a re-examination of the ES&S ExpressVote XL electronic voting machine. We enclose at least ten (10) certifications of duly registered electors in the Commonwealth of Pennsylvania who seek this re-examination. We have enclosed a check for $450 payable to the Treasurer of the Commonwealth of Pennsylvania.

As you know, "[t]he Secretary's duty to re-examine the machines upon proper request is mandatory." *Banfield v. Aichele*, 51 A.3d 300, 314 (Commw. Ct. Penn. 2012), *aff'd sub nom. Banfield v. Cortes*, 110 A.3d 155 (2015).

We have attached a list of deficiencies in the ExpressVote XL which require attention during re-examination. We also note that the ES&S ExpressVote HW 2.1 used as a tabulator shares many of the same deficiencies as the ExpressVote XL.

We respectfully request that the Secretary of the Commonwealth re-examine the ExpressVote XL electronic voting machine and issue a report relating to the functionality of the system. We request that this re-examination be conducted expeditiously because several counties in the Commonwealth have chosen or are considering the ExpressVote XL, and all counties must act quickly to comply with the Department of State directive to select new voter-verifiable paper record voting systems no later than December 31, 2019.

If the Secretary of the Commonwealth determines that the attached deficiencies are compelling evidence to preemptively decertify the ExpressVote XL, we would withdraw our petition for re-examination.

Respectfully submitted,

Ronald A. Fein, Legal Director
John C. Bonifaz, President
Free Speech For People
1320 Centre St. #405
Newton, MA 02459
(617) 244-0234
rfein@freespeechforpeople.org
jbonifaz@freespeechforpeople.org

Susan Greenhalgh
Vice President of Policy and Program
National Election Defense Coalition

Kevin Skoglund
Chief Technologist
Citizens for Better Elections,
A member of the Protect Our Vote Philly Coalition

Petition Pages

200 signatures by duly registered electors in the Commonwealth of Pennsylvania

From the counties:

Philadelphia
Allegheny
Montgomery
Bucks
Delaware
Westmoreland
Northampton

Attachment: ES&S ExpressVote XL Deficiencies

We seek re-examination of the ES&S ExpressVote XL voting machine on these grounds.

1. Tampering with Ballot Cards

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7 (12), which requires that a voting system:

> "Provides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards."

Since the Pennsylvania Certification of ES&S EVS 6.0.2.1, security researchers discovered[1] that the ExpressVote XL exposes a ballot card cast by a voter to an internal printer prior to tabulation and impoundment. The internal printer is controlled exclusively by software which has the ability to tamper with the content of the ballot card. A malfunctioning or manipulated ExpressVote XL could add, modify, or invalidate votes *after* the voter has viewed, confirmed, and cast her ballot. It could change election outcomes without detection. This is a very high impact defect which affects the integrity and auditability of the voting system.

This defect violates the principle of software independence: "A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome."[2] Software independence will be VVSG 2.0 Guideline 9.1 and is recognized as necessary for effective auditing. It is a "crucial" requirement for evidence-based elections as defined by Professors Philip Stark and David Wagner: "All three components are crucial. The risk-limiting audit relies on the integrity of the audit trail, which was created by the software-independent voting system (the voters themselves, in the case of paper ballots) and checked for integrity by

---

[1] References available at:
https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine
https://freedom-to-tinker.com/2018/10/22/an-unverifiability-principle-for-voting-machines
https://securiosa.com/posts/how_the_expressvote_xl_could_alter_ballots.html
https://securiosa.com/posts/how_expressvote_barcodes_could_be_modified.html

[2] "On the Notion of Software-Independence in Voting Systems," Ronald Rivest and John Wack, *Philosophical Transactions of The Royal Society*, August 6, 2008, Page 1, *available at* https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

the compliance audit."[3] Acceptable ballot security procedures to prevent tampering must include ensuring auditability and enabling evidence-based elections.

It is common sense that a voting machine should not have the ability to change votes after the voter has confirmed and cast her ballot. The same reasoning is evident and explicitly stated in § 1222, 25 P.S. § 3062 (a), "No person while handling the ballots shall have in his hand any pencil, pen, stamp or other means of marking or spoiling any ballot." Acceptable ballot security procedures to prevent tampering must include a similar restriction on any machine while handling the ballots.

2. Chronological Ballot Storage

The ExpressVote XL violates § 1107-A, 25 P.S. § 3031.7 (1), which requires that a voting system:

> "Provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting."

The ExpressVote XL ballot container stores ballot cards in chronological order. It allows any poll worker or election official who knows even limited details about the sequence of voters to violate the absolute secrecy of one or more voters. A voter's ballot could be determined by referencing the order of voters in the poll book or on the poll list, by counting from the first or last ballot in the set, or by counting from another identifiable ballot, such as one with a known write-in vote. This is a significant defect. Chronologically ordered ballots fail to protect voters' right to a secret ballot and enable information harvesting, vote buying and selling, and voter coercion.

The Pennsylvania Department of State has long held the position that voting systems with chronologically ordered ballots violate absolute secrecy. Dr. Michael Shamos, statutory examiner for the Secretary of the Commonwealth from 1980 to 2010, testified to a U.S. Senate committee in 2007, "Even paper trail advocates recognize that scrolled paper trails make it easy, not just possible, to determine how every voter in a precinct voted. The first voter's ballot is first on the tape; the last voter's is last; and everyone else's is sequential order in between. A simple comparison between the paper trail and the poll list gives away everyone's vote, in violation of the Section 201 requirement of a secret ballot. Even

---

[3] "Evidence-Based Elections," Philip Stark and David Wagner, *IEEE Security and Privacy*, May 8, 2012, Page 2, *available at* https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

if only two percent of the vote is audited, it means that two percent of the voters are at risk of having their votes revealed."[4]

The "Conditions of Certification" for ES&S EVS 6.0.2.1 do not require any procedures to randomize the order of ballot cards or to otherwise protect ballot secrecy. Even if procedures had been required, the voting system cannot depend on procedures—which may not be consistently or correctly employed—to restore ballot secrecy. The voting system itself must provide it.

3. Ballot Cards Colored by Party

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (e):

> "In primary elections, the Secretary of the Commonwealth shall choose a color for each party eligible to have candidates on the ballot and a separate color for independent voters. The ballot cards or paper ballots and ballot pages shall be printed on card or paper stock of the color of the party of the voter and the appropriate party affiliation or independent status shall be printed on the ballot card or at the top of the paper ballot and on the ballot pages."

The ballot cards used by the ExpressVote XL are made of solid white thermal paper. The card stock is not colored for each party. The ballot cards are blank and do not have the appropriate party affiliation or independent status printed on the ballot card.

In primary elections, the party affiliation of a voter is determined definitively when the voter checks in, signs the poll book, and is given a ballot card. Before the voter may vote, a poll worker must configure the ExpressVote XL to display the ballot style of the voter's party. If ballot cards are not on colored card stock with the party affiliation, the voter can tell the poll worker a different party affiliation, cast fraudulent votes in another party's election, and the impounded ballot card would show no evidence of the fraud. Colored card stock with the party affiliation printed also reduces the chance that a poll worker will set the wrong ballot style for a voter by accident.

It should be demonstrated that the required ballot cards are possible and that the ExpressVote XL is capable of using them.

---

[4] Testimony before the U.S. Senate Committee on Rules and Administration, July 25, 2007, http://euro.ecom.cmu.edu/people/faculty/mshamos/Senate20070725.pdf

4. Serially Numbered Perforated Stubs

The ExpressVote XL violates § 1109-A, 25 P.S. § 3031.9 (f):

> "…Each ballot card shall have an attached serially numbered perforated stub, which shall be removed by an election officer before the ballot card is deposited in the district automatic tabulating equipment or in a secure ballot box. The name of the county, and a facsimile of the signature of the members of the county board shall be printed on the ballot card stub."

The ExpressVote XL violates § 1112-A, 25 P.S. § 3031.12 (b)(6), which requires a procedure for a district using paper ballots or ballot cards:

> "Following the completion of his vote, the voter shall leave the voting booth and return the ballot to the election officer by a means designed to insure its secrecy; upon removal of the stub of the ballot by the election officer, the voter shall insert the ballot into the district automatic tabulating equipment or, in the event district tabulation is not provided for by the voting system or such district tabulation equipment is inoperative for any reason, into a secure ballot box. No ballot card from which the stub has been detached shall be accepted by the election officer in charge of such equipment or ballot box, but it shall be marked "spoiled" and shall be placed in the envelope marked "Spoiled Ballots"."

In addition, § 1113-A, 25 P.S. § 3031.13 (a) requires that, after the polls have been closed, the serially numbered stubs be used as evidence of the number of ballots issued to electors so that number may be announced in the polling place and recorded.

The ballot cards used by the ExpressVote XL do not have attached serially numbered perforated stubs. The ballot cards are blank and do not have a facsimile of the signature of the members of the county board printed on the ballot card stub.

The ExpressVote XL is designed such that a voter does not handle the ballot after the completion of her vote. The voter cannot leave the voting booth with the ballot card to return it to an election officer. The election officer does not have an opportunity to remove the stub. The election officer is not able to verify that the stub has not been detached from the ballot card in order to mark it as spoiled.