Testimony of Verified Voting
Marian K. Schneider, President
Contact: marian@verifiedvoting.org
Pennsylvania State Senate
Senate State Government Committee

Voting System Technology and Security in Pennsylvania
December 12, 2017

Thank you for the opportunity to submit written testimony in connection with the hearing of the Pennsylvania State Senate State Government Committee, held jointly with the Transportation Committee. This testimony will address cybersecurity issues in elections.

Verified Voting is a national non-partisan, non-profit research and advocacy organization committed to safeguarding elections in the digital age. Founded by computer scientists, Verified Voting's mission is to advocate for the responsible use of emerging technologies to ensure that Americans can be confident their votes will be cast as intended and counted as cast. We protect the fundamental right to vote where voting intersects technology. We promote auditable, accessible and resilient voting for all eligible citizens.

The security of election infrastructure has taken on increased significance in the aftermath of the 2016 election cycle. During the 2016 election cycle, a nation-state conducted systematic, coordinated attacks on America's election infrastructure, with the apparent aim of disrupting the election and undermining faith in America's democratic institutions. Intelligence reports that have been published in 2017 demonstrate that state databases and third-party vendors not only were targeted for attack, but were breached.[1] Regardless of the success of hacking attempts in 2016, the consensus among the intelligence community is that future attacks on American elections are inevitable.[2] The inevitability of attacks is a key concept in cyber security, that is, it's not whether a system will be attacked, but when.

The existence and national significance of this threat have escalated the priority of securing Pennsylvania's elections infrastructure. Two primary areas that require immediate and sustained attention are 1) securing both the state and county networks, databases and data transmission infrastructure that touch elections; and 2) instilling confidence in election outcomes by replacing legacy voting systems with new systems that permit reliable recounts and audits.

---

[1] "Illinois election officials say hack yielded information on 200,000 voters," *Chicago Tribune,* Aug. 29, 2016, http://www.chicagotribune.com/news/local/politics/ct-illinois-state-board-of-elections-hack-update-met-0830-20160829-story.html; "Russian hackers targeted Arizona election system," *The Washington Post,* Aug. 29, 2016, https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.de487f1d4b90.

[2] *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, Office of the Director of National Intelligence, 2017 at iii; *Securing Elections from Foreign Interference,* Brennan Center for Justice, June 29, 2017 at 4.

During the time that I served the Commonwealth as Deputy Secretary for Elections and Administration and Special Advisor to the Governor on Election Policy, I worked with the Office of Administration-Office of Information Technology to protect the Commonwealth's networks that touch elections and to implement procedures to recover from any potential attacks. These efforts complied with cyber security best practices to monitor, detect, respond and recover. OA-OIT's experienced staff is continuing this effort, and along with the Department of State, they have engaged county CIOs and technology staff to coordinate similar efforts at the counties working through the Commonwealth's relationship with the County Commissioners Association of Pennsylvania (CCAP). Assuming the administration receives support from the General Assembly, the Commonwealth is on the right track to taking the necessary steps to monitor, detect, respond and recover from cyber attacks.

Electronic voting systems deployed in Pennsylvania are another story. The single biggest driver of the narrative suggesting election results could be hacked is the use of direct recording electronic (DRE) voting systems. DRE systems directly record the voter's choices to computer memory. The voter may interface with the voting machine in one of several ways, such as a touchscreen or push buttons, but the voter's selections are recorded directly to memory stored in the machine. DRE machines retain no trustworthy evidence of the voter's choices, such as a voter verified or voter verifiable paper record. Research by the National Institute of Standards and Technology (NIST) has concluded that a voting system that does not provide a voter-verified paper record will be vulnerable to undetectable errors in the vote count.[3] If the digital records are corrupted, either by benign error or malicious attack there is no way to know the votes have been corrupted because of the lack of paper records.

Pennsylvania is one of only a handful of states in which a majority of voters vote on unverifiable voting systems. 83% of Pennsylvania's voters in 50 counties use these kinds of systems. The other 17% of Pennsylvania voters use voter-marked paper ballots as the primary voting method. Not only does the lack of a voter-verified paper record prevent an audit or recount, but paperless DREs are also more susceptible to undetected errors, failures and crashes because of their age.[4] The lifespan of voting machines has been estimated at 10-15 years.[5] Since the widespread deployment of electronic voting machines in the early 2000s, states have moved away from paperless electronic voting systems, driven by mounting research establishing these machines' security flaws and some high profile and costly machine failures.[6] Most of the nation has adopted voting systems that rely on a voter-marked paper ballot, an election safeguard recognized as essential by election officials and computer scientists alike.

---

[3] "Report of the Auditability Working Group," National Institute of Standards and Technology, Jan. 2011

[4] *Securing Elections from Foreign Interference,* Brennan Center for Justice, June 29, 2017 at 9.

[5] Norden, Lawrence, Famighetti, Christopher, "America's Voting Machines at Risk," The Brennan Center for Justice, Sept. 15, 2015

[6] In 2004 a voting system failure in North Carolina caused the loss of more than 4,500 votes. Because a state-wide contest had a margin fewer than 4,500 votes, the election had to be run again. "More than 4,500 North Carolina votes lost because of mistake in voting machine capacity," *Associated Press,* Nov. 4, 2004. As a result, North Carolina switched to paper ballots that are optically scanned.

Pennsylvania's aging voting systems, especially its aging DRE machines, need replacing as soon as possible. But replacement for replacement's sake should not be the standard. Currently, the best practice requires trustworthy evidence of voter intent in the form of voter-verified or verifiable paper records and a method of checking that the electronic vote tally matches those paper records. A contemporaneous voter-verified or voter-verifiable paper record prevents an undetected change in system software from producing an undetectable change in the voting results. The presence of such a record renders the system "software independent" and is the current best practice. Seventeen Pennsylvania counties already use such system, but that represents only 17% of the registered voters in Pennsylvania.

The system works like this – once the voter is authenticated and checked in, the voter is given a paper ballot. (The ballot is similar to the absentee ballot you would receive in the mail if you needed to vote absentee.) The ballot lists the candidates and ballot questions and beside each one is a small circle or bubble. The voter is given a ballot and a "privacy sleeve" (this is essentially a folder to protect ballot secrecy after the ballot is marked). The voter takes the ballot to a table or desk that affords a private place to mark the ballot and the voter then marks his/her choices by filling in the bubbles with a pen. The voter brings the ballot, in the privacy sleeve, to an optical scanner which is fitted on top of a secure ballot box. The voter feeds the ballot into the scanner. If the voter over-voted, the scanner will reject the ballot and return it to the voter so a poll-worker can spoil the ballot and the voter can correct the over-vote on a new ballot. The scanner can also be set to alert voters if they under-vote. After the ballot is accepted by the scanner, the ballot drops into the secure ballot box. For voters with disabilities, an accessible ballot marking device is provided at each polling location. These devices are ADA compliant and provide a variety of assistive devices but do not tally votes. The voter's selections are printed and scanned in the same manner as voter-marked paper ballots.

Recently, the Advisory Committee on Voting Technology to the Joint State Government Commission released its final report and recommended amending the election code to require paper records of voter intent. The Advisory Committee stated:

> The purpose of this recommended amendment is to make clear the Advisory Committee's commitment to secure elections that inspire confidence in the voters. The national conversation surrounding elections, especially regarding the possibility of voting machine hacking, has made it clear to the Advisory Committee members that implementing technology that reduces the possibility of hacking, and that facilitates post-election audits and recounts, is the best means of maintaining voter confidence.[7]

Justifications for continued reliance on aging DREs are, for the most part, based on myths that are easily debunked. A common misconception is that since the precinct-level devices are not connected to the internet, they cannot be hacked. While precinct devices may very well not be connected to the internet, other pathways for tampering with the software exist and can be

[7] "Voting Technology in Pennsylvania" Report of the Advisory Committee on Voting Technology, December, 2017, at 66, available here: http://jsg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463

exploited.[8] Election management systems (EMS) run on a regular Windows PC. Although counties are directed not to connect those PCs to a network or the internet, DOS has not undertaken any efforts to make sure that counties comply with recommended security configurations. Even more alarming, many counties contract with vendors to do the work of setting up the election. The program files are frequently transmitted to the counties via the internet. Unless counties are scrupulous in their attention best practices, this is another method of possible intrusion. Given recent revelations about voting system vendor ES&S' exposure of passwords and voter data on an unprotected Amazon Web Services (AWS) server, [9] the possibility of intrusion is a significant risk.

Additionally, all voting systems use removable media to transfer files from the EMS computer to the precinct devices. The use of removable media is itself a security vulnerability and provides a vector for attack. The presence of access ports for peripheral devices and memory cards presents an opportunity to attack the system either by connecting a malicious device to the system or by inserting fraudulent code via an unauthorized memory card.

Another common misconception is that attackers would need physical access to voting machines to compromise them and they are unable to gain such access. First, as explained above, an attack can be transmitted over the internet if the computers used to program the election were exposed to the internet.[10] ***The attacker could insert code that would then be replicated on each removable memory card and then spread to other election devices***. We know this is a possibility because of the documented attacks on voter registration systems and election support vendors during the 2016 election cycle.[11] Second, physical access to voting machines is more than a theoretical possibility. Many jurisdictions, including those in Pennsylvania, deliver precinct voting systems up to one week in advance of an election. Despite guidance that DOS reissued in 2016, many times, those precinct machines are left in an unsecured location. The length of time necessary to bypass "tamper evident seals" and insert a malicious cartridge is less than 10 minutes. [12]

Other well-documented vulnerabilities include the ability to disrupt a machine with an ordinary smart phone in the voting booth, the ability for a voter, using a specific type of machine,

---

[8] On September 12, 2017, the Presidential Advisory Commission on Election Integrity ("Pence Commission") held a hearing during which three respected computer scientist and security advisors testified: Dr. Andrew Appel Professor of Computer Science, Princeton University, Dr. Ronald Rivest Professor of Computer Science, Massachusetts Institute of Technology, Harri Hursti, Co-Founder of Nordic Innovation Labs. Their presentations are available here: https://www.whitehouse.gov/presidential-advisory-commission-election-integrity-resources and a summary of the materials is available here: https://medium.com/@max.hailperin/presidential-advisory-commission-on-election-integrity-september-12-2017-meeting-materials-4512dd139ee6

[9] "1.8 million Chicago voter records exposed online", CNN Tech, Aug. 17, 2017 http://money.cnn.com/2017/08/17/technology/business/chicago-voter-records-exposed-upguard/index.html

[10] Appel, A., "Which voting machines can be hacked through the Internet?" *Freedom to Tinker blog*, Sept. 20, 2016, Princeton University, Center for Technology in the Public Interest, https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

[11] "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny," *The New York Times*, Sept. 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html?mcubz=3&_r=0

[12] "Security Seals on Voting Machines: A Case Study", by Andrew W. Appel, *ACM Transactions on Information and System Security (TISSEC)* 14, 2, pages 18:1--18:29, September 2011

to obtain administrator status by inserting the card into the machine twice, the fact that ES&S hard coded the same password into its firmware ***nationwide*** (meaning it cannot be changed and the password has been publicized).[13]

Another myth commonly used to defend DREs is that vote tallies produced by DRE systems are capable of being audited. To the contrary, DRE systems cannot be audited to check that the electronic tabulation is correct because they do not retain trustworthy evidence of the voters' choices. The only evidence that is retained is the unverified interpretation of the voters' choices written to computer memory. That interpretation could be impacted by errors, bugs, or malicious code. No original data exists as a reference against which to check what is stored in computer memory. DREs can print out what was recorded onto their memory after the fact. If there was an error, or a malicious program that altered that choice on its way to the memory, then the copy of the data on the memory is incorrect. You can print out as many copies of the recorded data as you want but you will have no way of ***detecting the error because no trustworthy version of the voters' choices exists.***

Finally, proponents of DREs will point out, correctly, that optical scan tabulators have security vulnerabilities, too. However, jurisdictions can tolerate security vulnerabilities in optical scan systems simply because a paper record of voter intent exists. Thus, optical scan systems with paper ballots (and ballot marking devices for voters with disabilities) provide the ability to detect discrepancies in the electronic tally ***provided that a meaningful sample of ballots are recounted (or audited) to check that tally.*** This feature of optical scan electronic voting systems (and newer digital scan systems) makes those systems ***resilient***, that is, they are able to recover fully from a tampering event or error in the tabulation.

The need to decertify and replace DRE systems is extremely urgent and other states are acting on that urgency. On September 8, 2017, the Virginia Board of Elections voted unanimously to decertify all of the DREs currently deployed in Virginia,[14] most of which are also used in Pennsylvania. There were no abstentions.[15] The Virginia Department of Elections recommended these actions after the Virginia Information Technology Agency (VITA) evaluated the systems for security threats. In the Board's resolution, they noted that "VITA has indicated that based on their testing and analysis of third party reports, it appears there is a reasonable possibility of compromise of the voting machines at issue."[16] The resolution further noted, "the DRE devices analyzed all exhibited a range of demonstrated, documented, or potential

---

[13] As early as 2007, the existence of the hardcoded passwords in the ES&S iVotronics was publicized as well as other backdoors that allow an attacker to bypass passwords altogether. *See* notes from the investigation into the disastrous Florida CD-13 election in 2006: https://josephhall.org/nqb2/index.php/esslett0307

[14] Resolution of The Virginia State Board of Elections Regarding Certain Direct Recording Electronic (Dre) Voting Devices, September 8, 2017 available here: http://www.elections.virginia.gov/Files/Media/Agendas/2017/SBEResolutiondecertifyingDREs09-08-17.pdf

[15]. *See* "Virginia bars voting machines considered top hacking target", *Politico*, Sept. 8, 2017 http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492

[16] Resolution of The Virginia State Board of Elections Regarding Certain Direct Recording Electronic (Dre) Voting Devices, September 8, 2017 available here: http://www.elections.virginia.gov/Files/Media/Agendas/2017/SBEResolutiondecertifyingDREs09-08-17.pdf

vulnerabilities that materially impact the integrity of the voting process, availability of the voting systems, or integrity of election results."[17] Moreover, the lack of recovery from a tampering event, even if tampering could have been detected, was a critical factor in VITA's conclusion.

Verified Voting can provide the Committee with more information about the known vulnerabilities of the DRE systems deployed in Pennsylvania and the inability of these systems to recover from a miscounting event. Setting aside these important considerations, several practical considerations exist that counsel for replacement of DRE systems:

- The application used to program the machines is running on windows XP platform that is no longer supported by Microsoft.
- The legacy systems do not have an easy method of checking whether certified software is actually running on the system.
- It is becoming increasingly more difficult to locate spare parts in the event there are failures with the legacy systems.
- It is becoming harder to begin each election cycle with brand new removable media because deployed systems use outdated cards and cartridges
- Prevention is not 100% effective

The first question most people ask when discussing replacing legacy DRE systems is "How much?" The answer to that question is a moving target, mainly because companies negotiate different deals in different states. For a state like Pennsylvania, if it were to move to voter-marked paper ballots and an accessible device in each precinct, our calculations of the cost, based on actual costs incurred in Michigan from 2016-2017, ranges from $58 million to $91 million for the entire state. This cost is for equipment only and associated service contracts for years 1-5. We would be happy to discuss calculations with you in more detail.

We recognize that county resources in Pennsylvania vary widely. We strongly urge that the General Assembly make a direct appropriation for counties to offset the replacement costs of precinct voting devices. Although several bills are pending in Congress that would provide grants to states for replacement machines, that funding will not cover 100% of costs. Every level of government participates in elections. It is our strong urging that every level of government contribute to the cost of the machinery of democracy.

The success or failure of hacking attempts is, at a basic level, irrelevant. The seeds of doubt sown by the hacking narrative causes distrust in our democracy and skepticism about the correctness of the election outcome. Defusing that destructive narrative is the most effective way to instill confidence in the election result. The best way to defuse the hacking narrative is to deploy precinct voting systems that provide trustworthy evidence of elections results. This evidence allows jurisdictions to confirm that the electronic voting system reported the correct results. Today, given the known vulnerabilities and inability to perfectly safeguard any computer system from attack, the best evidence of the voter's choices is evidence from voter-marked paper ballots. Jurisdictions can leverage technology to tally those paper ballots, but they

[17] *Id.*

can also use them to conduct an audit, or a spot check of the results and the provide the ability for candidates in close races, to have a meaningful recount of the contest.

Thank you very much for your consideration. We welcome the opportunity to provide any additional information and hope to work with the General Assembly in the future on these important issues.