

TESTIMONY for Senate State Government Committee Hearing on Decertification of Machines, March 26, 2019

The Constitution of the Commonwealth of Pennsylvania, Article I, Section 5, begins with an assurance of rights to our citizens that, "Elections shall be free and equal; and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage." The General Assembly has a fundamental duty to ensure free elections. We have a responsibility to our constituents to assure them that their votes are counted accurately, and are not being compromised by miscalibration, malfunctioning voting machines, or illegal attempts to tamper with election outcomes by domestic or foreign criminals. This is one of our highest duties as elected legislators.

The General Assembly should support the Department of State (DOS) directive for counties to have new machines with paper records in place by the 2020 elections, and we should also support funding to assist counties in this essential transition. There are several emergent reasons why we must support their decision:

- 1) DOS has the authority in the Election Code over the certification of voting machines.
- 2) Most of Pennsylvania's voting machines are at the end of their lifespan.
- 3) Most of Pennsylvania voting machines do not allow for independent audits of election results.
- 4) Pennsylvania's voting machines are vulnerable to hacking, despite claims of "not being connected to the internet".
- 5) Officials from the Department of Homeland Security, the Senate Intelligence Committee, and numerous computer science and election security experts have concluded that voting machines must have a voter-verified paper trail and robust election audits to ensure election security. Intelligence officials are unsure of the full impact of Russia's attempted hacks of numerous states and vendors, and have warned that Russians will continue in their efforts to hack U.S. elections.

First, the Department of State acted within its authority under the Pennsylvania Election Code. Article II, Section 201(b), which describes the powers and duties of the Secretary of the Commonwealth, clearly states that the Secretary's has the power and the duty "To examine and reexamine voting machines, and to approve or disapprove them for use in this State, in accordance with the provisions of this act." The General Assembly should not make the mistake of taking away the Secretary's authority at a crucial time when our voting machines are vulnerable. The Secretary needs the ability to act quickly when there are serious flaws or threats to our voting machines. The General Assembly has not demonstrated the will or the ability to act with sufficient speed in critical times, as evidence by the fact that certain flawed parts of the Election Code have not been amended since 1937.

Second, most of Pennsylvania's voting machines are old and showing signs of decay (See Norden, L., & Famighetti, C.). Poll workers and voters complain of buttons that do not work or light up when a voter tries to press certain buttons, and broken locks on machines which leave the results cartridges exposed. There have been problems reported with printers not working, so that Judges of Elections could not

print out vote tallies. However, most vendors are no longer manufacturing direct-recording electronic machines (DREs), so election officials have a hard time finding replacement parts. The problem of malfunctioning machines was recently demonstrated in York and Dauphin counties in the 2018 primary elections when crucial machine functions failed, and voters left the polls without voting (See FOX43.com and WITF.org May 25, 2015). An additional area of concern is the fact that many of Pennsylvania's voting machines, some older than 25 and 30 years, are no longer even supported by software security upgrades, leaving them highly vulnerable to error and manipulation. To ensure "free and equal elections for Pennsylvania voters, the General Assembly has a duty to ensure that the machines in use are resilient in times of crisis and are not outdated.

Third, most of Pennsylvania's voting machines are incapable of being independently audited or recounted, since there is no voter-verified paper record of the individual votes. Fewer than 20% of PA voters have the assurance of a paper record of their individual votes cast (see Verified Voting Testimony...). Pennsylvania lags desperately behind the rest of the nation in protecting our citizens' right to vote with a paper record. By contrast, more than 80% of voters in the U.S. are guaranteed protection of their right to vote with a paper record (See Norden, L., & Famighetti, C.) The problem of inability to audit or recount the votes was poignantly demonstrated in two recent examples. In 2016, several counties received reports from voters of machines that were flipping votes to alternate parties or candidates. Election officials verified the problem, and some were attributed to miscalibration (see WGNTV.com and Lancasteronline.com). The problematic machines were re-calibrated or taken out of service by election officials. That does not address the problem for the voters who had voted previously on the erroneous machines. There would be no way to properly attribute those prior votes, since there was no paper record of the individual votes, and the electronic record had clearly been compromised. In York County's November 2017 election, 600 voting machines were incorrectly programmed, resulting in 2,900 double votes in races where voters were only supposed to vote for one candidate. Election officials later said they had addressed the problem, but there is no way to know that 2,900 people were not disenfranchised, because there was no independent way to go back and check individual records of those votes without a paper record of each vote cast (see WITF.org Dec. 7, 2017). In addition, the Saccone-Lamb special election in Pennsylvania in 2018, Pennsylvania Representative Rick Saccone had considered calling for a recount in a race after voter claims of vote-flipping by machines. No recount or audit was possible due to the lack of individual paper ballots in the DRE voting machines. It is clear that voters need assurance that elections are auditable and verifiable if they are to have faith in the legitimacy of their elected leaders.

Fourth, it is important to restate that the General Assembly has a responsibility under Article I, Section 5 of the Pennsylvania Constitution to ensure that "no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage". That includes a duty to ensure that our voting machines are secure. Several computer scientists and even hacker conventions have demonstrated how easy it is to hack the type of DRE voting machines used in Pennsylvania in just a matter of minutes with materials available to any member of the public. The source list below includes numerous pieces of evidence and testimony from computer experts testifying to the fact, including PhD's such as Appel, Halderman, and Lopresti. Members of the public can easily see how vulnerable our voting machines are by simply walking into a voting precinct a few days or even weeks before an election. Voting machines are often stored for days before the election in unsecured polling places with public access in our public schools, libraries, and town halls for days before an election, often with the results cartridges in the machines.

A common myth argued by public officials is that Pennsylvania's machines are secure because they are not connected to the Internet. This has been disproven. In 2011, voting machines in Venango County, PA were reported to be "flipping votes". An analysis of the machines showed that the machines, which were not "connected to the Internet" had been compromised by remote access software. The software had been installed two years earlier and activated several times, including for 80 minutes the night before an election. A contractor was using the remote access software to work on the system from home. Anyone who could gain access to the contractor's home computer could use that to access the system (see Zetter, Kim, Feb 2018). This is how hackers frequently gain access to systems. They can use phishing emails to install malware on any election official or vendors computer. Anyone who has been compromised by malware can unknowingly download it onto the ballot programming, which can then be downloaded onto every single voting machine with a simple memory device like a flash drive or a memory cartridge. The top voting machine vendor in the country admitted last year in a letter to Senator Wyden (D-OR) that it had installed remote access software on many voting machines, despite prior denials of that installation by a company spokesperson (see Zetter, Kim, July 2018).

Fifth, numerous national officials, intelligence officials, and cybersecurity experts have concluded that there is a high priority for voting machines to have voter-verified paper records of individual votes, and a robust election auditing process (see Senator Burr and Syeed & Edgerton). Federal intelligence officials, agencies, and committees have verified the Russian attempts to hack U.S. elections through both vendors and state databases. They have designated elections as critical infrastructure in order to give it a priority for security. Numerous sources below document this. Even the General Assembly's Joint State Government Commission advised in December of 2017 that Pennsylvania voting machines need voter-verified paper records and audits, and it offered draft legislation to further that purpose (see Joint State Government Commission). The General Assembly must take seriously our responsibility to prevent election interference by criminals. We must support, not hinder, the Department of State in their efforts to bring more secure elections to Pennsylvania citizens.

Pennsylvania's citizens deserve to have confidence that we are protecting their fundamental right to vote. Public and private security experts are in agreement. Pennsylvania's DRE machines are outdated, incapable of being independently audited, and vulnerable to tampering. One of our highest duties is to protect the fundamental right to vote. Senator Gordner's proposed bill would postpone long-needed security upgrades that cannot wait. We must allow the Secretary of the Commonwealth to responsibly perform critical election security upgrades in a timely fashion. We must also impress upon our colleagues the need for General Assembly funding to assist counties in their crucial function of secure elections, upon which local, state, and federal officials are all elected. We must maintain the confidence of Pennsylvania citizens that we are safeguarding their fundamental right to vote.

***Testimony written and submitted by Pennsylvania election integrity groups
from Bucks County and Montgomery County***

Janis Hobbs-Pellechio, president of SAVE Bucks Votes ("Secure, Accurate, Verifiable Elections")
www.SAVEBucksVotes.org

Muna Elshakhs, co-founder of Citizens for Better Elections
www.CoalitionforBetterElections.org

REFERENCES

- Appel, A., Testimony before Congress, (2016, Sep. 28). C-Span.org. <https://www.c-span.org/video/?c4623050/electronic-voting-machines-vulnerable-hacking>; Halderman, J. Testimony before Congress. <https://www.youtube.com/watch?v=3qr67h54VO0>
- Appel, A, Video of Sequoia AVC DRE machine being hacked in minutes by Princeton University Professor of Computer Science Andrew Appel, Oct. 17, 2008, <https://www.youtube.com/watch?v=wzZR5XZ5Cz4>
- Appel, A, "Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine", Oct. 17, 2008, <https://www.cs.princeton.edu/~appel/papers/advantage-insecurities-redacted.pdf>
- Bucks County Courier Times, "Expert: Pennsylvania 'would get an F' on voting machine security", April 25, 2018, <http://www.buckscountycouriertimes.com/news/20180425/expert-pennsylvania-would-get-f-on-voting-machine-security/1>
- Buzzfeednews.com, "The GOP Couldn't Recount the Votes in PA Even if it Wanted. There's no Paper Trail to Audit", March 15, 2018, <https://www.buzzfeednews.com/article/kevincollier/the-voting-machines-in-pennsylvanias-18th-dont-leave-a#.kvndmA47eR>
- FOX43.com, "York Township polling location opens with some problems", May 15, 2018, <https://fox43.com/2018/05/15/york-township-polling-location-opens-with-some-problems/>
- Joint State Government Commission (JSGC). Report of the Advisory Committee on Voting Technology, Voting Technology in Pennsylvania, p. 4 (Pa. Dec 2017). <http://jsg.legis.state.pa.us/resources/documents/ftp/publications/2017-12-11%20FOR%20WEBSITE%20%20VOTING%20FINAL%20REPORT%2011.30.17.pdf>
- Lancasteronline.com, "Voting Machine Error Causes Straight GOP Ticket to Switch to Straight Democratic in Lebanon County", Nov. 8, 2016, https://lancasteronline.com/news/local/voting-machine-error-causes-straight-gop-ticket-to-switch-to/article_bf43f6c0-a5e4-11e6-b1ad-f32a8078dde9.html
- Letter to Congress from 103 Experts on Computer Science, Elections and Security, June 21, 2017, <https://www.electiondefense.org/election-integrity-expert-letter/>
- Letter to EAC and DHS from 30 Cybersecurity, Election Security, and Computer Science Experts, Oct. 2, 2018, <https://www.electiondefense.org/letter-to-eac-and-dhs/>
- Lopresti, Daniel, "The Ticking Time Bomb in Pennsylvania's Election System", Dec. 15, 2016, http://www.philly.com/philly/opinion/20161215_The_ticking_time_bomb_in_Pennsylvania_s_election_system.html?arc404=true
- Newman, Lily Hay, "Voting Machines are Still Absurdly Vulnerable to Attacks", <https://www.wired.com/story/voting-machine-vulnerabilities-defcon-voting-village/>

Norden, L., & Famighetti, C. (2015) America's Voting Machines At Risk, p. 4. Brennan Center for Justice at New York University School of Law.

https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf

Norden, L., & Vandewalker, I. (2017). Securing Elections from Foreign Interference, p.14. Brennan Center for Justice at New York University School of Law.

https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf

NYTimes.com, Mokalla, Jensen and Halderman, "I Hacked an Election. So Can the Russians",

<https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html>

Pennlive.com, "'Pennsylvania elections are at risk': Panel urge funding for new voting machines", Sep. 25, 2018, <https://www.pennlive.com/politics...>

Pittsburgh Post-Gazette, "We Need Voting Machines with Auditable Ballots", March 15, 2018,

<http://www.post-gazette.com/opinion/letters/2018/03/15/We-need-voting-machines-with-auditable-ballots/stories/201803150031>

"Public Citizens Calls on Largest Voting Machine Vendor to Stop Selling Machines that Connect to the Internet, Increase Costs to Taxpayers", July 26, 2018, <https://www.citizen.org/media/press-releases/public-citizen-calls-largest-voting-machine-vendor-stop-selling-machines>

"Russia Wants to Meddle in Midterm Elections, Intelligence Officials Say." Fox News, FOX News Network, 13 Feb. 2018, <http://www.foxnews.com/politics/2018/02/13/russia-wants-to-meddle-in-midterm-elections-intelligence-officials-say.html>

Senator Burr, Press Releases, "Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security", May 8, 2018,

<https://www.burr.senate.gov/press/releases/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security>

Syed, N. & Edgerton, A., Bloomberg.com, "Extent of Election Hacking Is Still Unclear, Says Senate Panel", May 8, 2018, <https://www.bloomberg.com/news/articles/2018-05-09/senate-panel-says-extent-of-election-hacking-is-still-unclear>

<https://www.bloomberg.com/news/articles/2018-05-09/senate-panel-says-extent-of-election-hacking-is-still-unclear>

Thehill.com, "DHS tells 21 states they were Russia hacking targets before 2016 election", Sep. 22, 2017,

<https://thehill.com/policy/cybersecurity/351981-dhs-notifies-21-states-of-they-were-targets-russian-hacking>

Uchill, J. (2017, Sep 22). "DHS Tells 21 States they were Russian Hacking Targets Before 2016 Election".

TheHill.com. <http://thehill.com/policy/cybersecurity/351981-dhs-notifies-21-states-of-they-were-targets-russian-hacking>

Verified Voting Testimony before the Pennsylvania Senate State Government Committee: Voting System Technology and Security, (2017, Dec. 15). VerifiedVoting.org. <https://www.verifiedvoting.org/voting-system-technology-and-security-in-pennsylvania/>

Weise, E. (2017, July 30). "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines" USA Today.com, <https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/>

WGNTV.com, "Pennsylvania voters claim voting machines 'changing' ballots", Nov. 8, 2016, <https://wgntv.com/2016/11/08/pennsylvania-voters-claim-voting-machines-changing-ballots/>
Wines, M. (2017, Oct. 14). "Wary of Hackers, States Move to Upgrade Voting Systems." NYTimes.com. <https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html>

WITF.org, "York County plans changes to elections process after confusion at the polls", Dec. 7, 2017, <http://www.witf.org/news/2017/12/york-county-plans-changes-to-election-process-after-confusion-at-the-polls.php>

WITF.org, "Storm knocks out power, backup batteries at Harrisburg polling place", May 15, 2018, <http://www.witf.org/state-house-sound-bites/2018/05/storm-knocks-out-power-backup-batteries-at-harrisburg-polling-place.php>

Zetter, Kim, "The Myth of the Hacker-Proof Voting Machine" New York Times, Feb 21, 2018, <https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html?mtrref=www.facebook.com&gwh=8CD15702CA0264A04BB081B621EBF11C&gwt=pay>

Zetter, Kim, "Top Voting Machine Vendor Admits it Installed Remote-Access Software on Systems Sold to States", July 17, 2018, https://motherboard.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states