CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony before the Pennsylvania House of Representatives State Government Committee

April 1, 2021

Dr. William T. Adler
Senior Technologist, Elections & Democracy
Center for Democracy & Technology

Chairman Grove, Chairwoman Davidson, members of the committee, thank you for inviting me here to speak with you today about election security in Pennsylvania.

My name is Will Adler. I am the Senior Technologist for Elections & Democracy at the Center for Democracy and Technology, or CDT. CDT has a 25-year history of advocating for individual rights in the digital age. For my work, that means the right to a secure and accessible vote.

As you all know, election infrastructure is complex, with many different digital systems, including the voter registration system, voting machines, and the software and hardware used to tabulate ballots. Making sure these systems are secure is critical for smooth and trustworthy elections.

CDT commends Pennsylvania for the major election security improvements that it has recently made. But there remain a number of things that Pennsylvania can do to make sure it leads the country in election security.

I want to address three possible areas of improvement as this committee takes a look at further improvements to Pennsylvania's election security.

I. Ensure software independence and expand the use of risk-limiting audits

The first is to make sure that voters can be confident that their votes are counted as intended. The elimination of paperless voting systems was a huge step forward in ensuring that Pennsylvania voters can have that confidence. But there's still more to do, such as ensuring software independence, which sets the stage for expanded risk-limiting audits.

In February, the federal Election Assistance Commission adopted the second version of the Voluntary Voting System Guidelines, which were years in the making and will set the standards of voting machine security for years to come. One of the most important new principles is software independence.[1] When a voting system is software independent, that means that an undetected change to its software (such as one that a hacker might introduce), cannot create an undetected change in the election outcome. In other words, if a software independent voting system has been hacked, it won't matter because there will still be an indelible record of voter intent that can be used to confirm the outcome in an audit or a

[1] Election Assistance Commission. (2021). "Requirements for the Voluntary Voting System Guidelines 2.0," p. 179, https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf#page=179.

recount. We spend a lot of time worrying about protecting voting systems, and we should, but wouldn't it be better if we could trust our outcomes even if we didn't have 100% trust in our machines? That's what software independence is about, and it should be possible to take steps to ensure that Pennsylvania's voting systems are software independent even before systems are federally certified as such.

Strong software independence is a key part of ensuring that there is a trustworthy paper record of voter intent. But that paper record is only useful if it's checked, such as through risk-limiting audits. By looking at statistically-driven samples of ballots, risk-limiting audits provide an efficient way to get a high degree of confidence that the outcome was correct. I know that this committee has already held a hearing which covered risk-limiting audits, but I think it's important to reiterate how important they are. Many states are expanding the use of these audits, and it's great to see that Pennsylvania is among them. Continuing to expand and standardize their usage would be a great next step.

II. Prioritize security when procuring election services

Secondly, Pennsylvania should make sure that cybersecurity is front of mind for procurement decisions. Although voting machines do not connect to the internet, many systems used to conduct elections are internet-enabled. We want to avoid the possibility of breaches in which a hacker could copy confidential information, alter the flow of information, or take down a critical Election Day system.[2] I'm aware that Pennsylvania is replacing its voter registration system. As it goes through this process, and as the state and counties continue to work with outside vendors on other services, it should make sure to keep cybersecurity front and center in the process, and ensure that vendors are transparent and follow cybersecurity best practices.[3] As the recent so-called SolarWinds attack illustrated, it's important to ensure confidence in as much of the software supply chain as possible.

III. Help counties follow standard cybersecurity best practices

Lastly, as the primary conductor of elections, counties need assistance in order to run secure elections and follow cybersecurity best practices. County officials are responsible for helping their residents vote, maintaining chains of custody for ballots, and reporting results—a highly technical process that they carry out under a great deal of pressure, and they do very well. But they often don't have the resources they need, which can include cybersecurity training or dedicated IT staff. A report from Pitt Cyber made a few recommendations for ways that the state can secure county operations, such as by funding training, cybersecurity assessments, an ongoing fund for election security upgrades, and more.[4] Any actions taken by the state to ensure a more uniform approach to cybersecurity best practices could make sure that the state isn't blindsided if, say, a small county gets hit with a cyberattack.

---

[2] William T. Adler & Mallory Knodel. (2021). "An Agenda for U.S. Election Cybersecurity," https://cdt.org/insights/cdt-report-an-agenda-for-u-s-election-cybersecurity/.
[3] Center for Internet Security. (2019). "A Guide for Ensuring Security in Election Technology Procurements," https://learn.cisecurity.org/l/799323/2020-06-17/sxs4/799323/32483/CIS_Elections_Procurements_12_April.pdf.
[4] Pitt Cyber. (2019). "The Blue Ribbon Commission on Pennsylvania's Election Security," https://www.cyber.pitt.edu/sites/default/files/final_full_pittcyber_pas_election_security_report.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

For example, one very easy change would be for counties to ensure that they have .GOV domains. Only verified US government institutions can have a .GOV website; it's like having a blue checkmark on Twitter. It builds trust among voters who can know that they are looking at a website that is providing accurate information. But unfortunately, only 11 of Pennsylvania's 67 counties are on .GOV domains;[5] most are on .COM or .ORG domains, which anyone can purchase. For instance, Philadelphia's official elections website is *philadelphiavotes.com*. With that being the official website, it's easy for someone to make a convincing fake website at, say, *phillyvote.com*, and produce fake information about the election or even collect information from unwitting users. And this is a real threat—last year, the FBI found multiple websites that were masquerading as government election websites.[6] Thankfully, .GOV domains are, as of this year, provided free by the federal government, so the state should help counties work with the federal Cybersecurity and Infrastructure Security Agency to move to .GOV domains.

And with that, I look forward to your questions.

[5] Steve Grobman. (2020). "US County Election Websites (Still) Fail to Fulfill Basic Security Measures," https://www.mcafee.com/blogs/other-blogs/executive-perspectives/us-county-election-websites-still-fail-to-fulfill-basic-security-measures/.
[6] FBI & CISA. (2020). "Public Service Announcement: Spoofed Internet Domains Pose Cyber and Disinformation Risks to Voters," https://www.cisa.gov/sites/default/files/publications/PSA_Spoofing_Final-508.pdf.