

Senate Committee on State Government  
Hearing on Senate Bill 48  
March 26, 2019  
Room 8E-A, East Wing  
Commonwealth Avenue, Harrisburg, PA

Written Testimony of  
Lt. Col. Anthony Shaffer

Thank you Chairmen Folmer and Williams, Whip Gordner, and members of the Committee for allowing me to submit written testimony. I write to oppose Senate Bill 48 and to address the national security implications of Pennsylvania's continued use of insecure and vulnerable paperless voting systems. Because of these urgent concerns, it is imperative for the Pennsylvania General Assembly to appropriate adequate funding to assist counties in replacing their systems before the 2020 election.

I have 38 years of experience in national security and cyber security, including operational work with the FBI, NSA, and CIA. As noted in the September 14, 2011, U.S. [Congressional Record](#), I am credited with creating and directed the first undercover offensive Cyber Unit at the Department of Defense in the late 1990s. I continue to advise the Pentagon, the Army War College, key members and committees of the US Congress and members of President Trump's Cabinet on cyber threat, threat mitigation, technology vulnerabilities and related threat intervention issues.

I am here to warn the Pennsylvania General Assembly that the Keystone State's elections are an open target for foreign interference, whether it be from the Chinese, Russians, Iranians, North Koreans, or anyone else seeking to undermine the integrity of our elections. Do not be mistaken, paperless machines can be compromised—this has been proven. Although precinct voting machines in Pennsylvania are generally not connected to the internet while voting occurs, the outdated systems currently in place present numerous opportunities to disrupt the outcome of the election. I know from experience that any computer can be hacked including computers used to count votes like in Pennsylvania. I used to be the one looking to exploit vulnerabilities in the bad guys' computers. Even if a machine is not directly connected to the internet, all machines must accept input files at some point. This is how the machine's software is upgraded and how the new ballots are added to the machine for each election. These input files are added via an internet connection, or via some type of memory device prepared on another computer that might have been connected to an insecure network. Multiple opportunities to enter malware into a voting system exist throughout the chain of custody of these voting systems, and any voting system for that matter.

Unfortunately, since 2006, a majority of Pennsylvania voters cast their votes using paperless machines. When they vote, their choices are recorded directly to computer memory, providing no other record of their selections. If the machine malfunctions or is hacked, there is no way that the records stored to computer memory can be audited or recounted to verify the

accuracy of election results. This uncertainty could destroy voter confidence. We cannot afford to have the results of elections questioned, especially in an important state like Pennsylvania. The other states that have historically determined the outcome of a presidential election, so-called “swing states,” already provide paper records. I know how our foreign adversaries work. They look for the easiest targets to exploit. If Pennsylvania fails to act now, your elections could be the easiest target in 2020.

By way of background, Pennsylvania uses two basic kinds of electronic voting systems: (1) paperless direct-recording electronic (DRE) or (2) optical scan systems. Both types of systems rely on computers, but with a significant difference: optical scan systems incorporate a voter-marked paper ballot, marked either with a pen or pencil or with a ballot marking device. Once a voter marks his selections on the ballot, it is run through an optical scanner, which leverages the speed of the computer to quickly tally unofficial results. That ballot is then retained for an audit or recount. The paper ballots provide a way to check that the computer reported the results accurately either by sampling them in an audit or hand counting the paper ballots if necessary. Seventeen counties in Pennsylvania already benefit from paper ballots – and these machines do not need to be replaced to ensure a secure election.

I am concerned that Senate Bill 48 could slow down Pennsylvania’s current efforts to replace its vulnerable paperless voting systems. It could also hamper the state’s ability to rapidly respond to future security breaches or other emergencies. Under this legislation, if the commonwealth were to decertify voting systems used in half or more of the counties, the Department of State would be required to submit a written plan to the legislature 180 days prior to the decertification taking effect. The legislature would then establish a commission to review the plan, hold at least two public hearings, and issue a written report. Senators, you do not have time for commissions and reports—your paperless systems are in our adversaries’ crosshairs NOW. Election security experts and cyber experts like me all agree that systems that incorporate voter-marked paper ballots (whether marked by hand or device) are necessary to ensure the integrity of elections. I understand that the legislature and counties should inform and participate in the process to replace Pennsylvania’s vulnerable systems, and I encourage the Governor and Secretary of the Commonwealth to include you in a transparent process. But SB 48 is not the answer. Too much is at stake. If Pennsylvania does not act fast, it will be the only swing state without paper records demonstrating the intent of voters for the 2020 election.

That’s why Pennsylvania should support the Trump Administration’s endorsement of paper ballots and answer Homeland Security Secretary Kirstjen Nielsen’s call for “all state and local election officials to make certain that by the 2020 presidential election, every American votes on a verifiable and auditable ballot.”

With that goal in mind, I urge the General Assembly to include adequate funding in this year’s budget to help counties move forward as expeditiously as possible to replace their current aging and vulnerable voting systems. Local election officials and national advocacy groups believe the cost to replace the existing equipment, including training, voter outreach, and logistical needs for deployment could reach \$150 million. The Governor’s budget asks for only \$15 million this year--10% of the actual estimated cost--and would include an additional \$15

million each year over the next 4 years. I am a fiscal conservative, but I view the Governor's proposal as insufficient and too vague to allow counties to adequately plan their budgets to replace vulnerable equipment ahead of the 2020 election. It is vitally important, now more than ever, to invest in protecting our national security. As someone who has spent a career in the trenches of cyber warfare, I understand the threat and I'm here to urge you to stand strong in our national defense.

As has been its history, Pennsylvania is truly the Keystone State. In 2020, the election could be decided by Pennsylvania and its electoral votes. Now 18 years after the election disaster of 2000, with the infamous hanging chads, Florida continues to suffer from a negative reputation. I encourage you to prioritize investing in election security, so that Pennsylvania does not suffer the same fate in 2020.

It is my judgment that Pennsylvania must act prudently to replace all paperless DRE machines with secure optical scan systems in time for the 2020 elections. Once paper ballots are in place, Pennsylvania can conduct mandatory routine post-election audits that use statistical methods to verify the accuracy of the reported results. If these paper ballot and audit safeguards are implemented, Pennsylvania will be able to uncover machine malfunctions or election interference and use the paper ballots to ensure the correct results, so your constituents can be confident that their votes are cast as intended and counted as cast. Without these steps, our elections will continually be dogged by legitimacy questions.

This is not a political or partisan issue. This is an issue of national security. The threat of election interference is known and real. The solution to this problem is known and achievable: voter-marked paper ballots and robust audits. I urge you to take necessary action to protect our democracy from outside interference and stand with me in calling for adequate funding to ensure that all Pennsylvanians cast their votes on secure paper ballots in 2020.