Senate State Government Committee
Public Hearing on Senate Bill 1249 and Voting Machine Demonstration
September 25, 2018
9:30 am 2 South Second Street Harrisburg, PA

Written Testimony of Verified Voting.org
Marian K. Schneider, President
September 21, 2018

Thank you Chairman Folmer, Minority Chair Williams, and members of the Committee for allowing Verified Voting to submit written testimony in connection with the Senate State Government Committee hearing. We write to address the security risks presented for Pennsylvania's counties and the need to expeditiously replace aging and vulnerable electronic voting systems. We urge the Committee to recommend that the Commonwealth appropriate adequate funding to permit counties to replace their aging electronic voting systems as soon as possible.

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 promote auditable, accessible and resilient voting for all eligible citizens. Our board of directors and board of advisors include some of the top computer scientists, cyber security experts and statisticians working in the election administration arena as well as former and current elections officials. Verified Voting has no financial interest in the type of equipment used. Our goal is for every jurisdiction in the United States to have secure and verifiable elections.

There are two basic kinds of electronic voting systems in use in Pennsylvania: Direct recording electronic (DRE) or optical scan systems. Both types of systems are computers, and both are prepared in similar ways. The primary difference is that an optical scan system incorporates a voter-marked paper ballot, marked either with a pen or pencil or with a ballot marking device and that ballot is retained for recounts or audits. Optical scan systems leverage the speed of the computer to report unofficial results quickly. The presence and availability of that paper ballot provides a trustworthy record of voter intent and allows jurisdictions to monitor their system for problems, detect any problems, (either hacking or error), respond to them and recover by, if necessary, hand counting the paper ballots. ***Seventeen counties in Pennsylvania already benefit from the security protection of paper ballots.***

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. There is no software-independent record of voter intent provided with a DRE system.

A printout of election results from the memory card after the fact or a printout of "cast vote records" does not provide any additional verification of the election results. Those printouts simply call up the data that is stored on the computer's memory. If the data was not stored correctly, whether because of malware or malfunction in the voting system, a printout of incorrect data is meaningless. Without a contemporaneous software independent record of voter intent, there is no way to verify, audit or recount DREs.

I refer the committee to Verified Voting's written testimony dated December 12, 2017 and available on the Committee's website here: http://pasenategop.com/stategovernment/wp-content/uploads/sites/30/2017/12/schneider.pdf As explained in that testimony, 50 out 67 Pennsylvania counties use DRE systems. Since December, no counties that use direct recording electronic voting systems have replaced their systems. The persistent barrier to replacement is the cost of doing so. For the past several years, counties have expressed their desire to replace their aging and vulnerable equipment. Without financial assistance from the Commonwealth, that replacement will either occur more slowly or not at all.

The urgency of replacing DREs is because, by design, it is impossible to verify that the computer correctly captured the voter's choices. The committee has likely heard that the precinct voting devices are "unhackable." That statement is untrue. Each precinct voting device is programmed by a regular laptop or desktop computer. The program files are then loaded onto the precinct voting device via some kind of memory card, cartridge or USB stick. This is true for every kind of computer that counts votes in Pennsylvania. An error or malware on the computer that programs the voting devices could infect the entire county. If that computer is connected to a network, a phishing attack, for example, in which the attacker obtained login credentials could provide a pathway for the attacker to modify the ballot definition file. Alex Halderman, Professor of Computer Science at the University of Michigan has demonstrated numerous times how this could be done including in the New York Times video available here: https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html

The chorus of voices calling for the security measure of voter marked paper ballots has grown louder even in the past few days.

On September 17, 2018, a federal court in Georgia issued a decision in *Curling v. Kemp* finding that the persistent vulnerabilities in the Georgia's paperless voting system raised profound constitutional issues that require urgent action from state officials. The plaintiffs in *Curling* are Georgia voters challenging the constitutional adequacy of Georgia's DRE electronic voting systems that produce no paper record. The plaintiffs presented the court with unrebutted evidence regarding the security flaws and vulnerabilities in the state's DRE system. Although the court was troubled by the short amount of time between the date of its ruling and early voting in Georgia, it nevertheless held that plaintiffs were likely to succeed on the merits of their claims. In explaining its ruling, the court outlined the constitutional imperative to secure election systems against modern cyberthreats.

Specifically, the court found that "[p]laintiffs have shown that their Fourteenth Amendment right to Due Process and Equal Protection have been burdened" because "the State's continued reliance on the use of DRE machines in public elections likely results in 'a

debasement or dilution of the weight of Plaintiffs' votes,' even if such conduct does not completely deny Plaintiffs the right to vote." The court began from the premise that "[p]laintiffs shine a spotlight on the serious security flaws and vulnerabilities in the State's DRE system – including unverifiable election results, outdated software susceptible to malware and viruses, and a central server that was already hacked multiple times." The court also noted the "rapidly evolving cybertechnology changes and challenges [that] have altered the reality now facing electoral voting systems." Although the court decided not to order Georgia to change its voting system in advance of the November elections, it "advise[d] the Defendants that further delay is not tolerable in their confronting and tackling the challenges before the State's election balloting system."

The Georgia court's conclusion underscores the stakes associated with ensuring secure and reliable election systems: "The 2020 elections are around the corner. If a new balloting system is to be launched in Georgia in an effective manner, it should address democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote."

The Georgia decision follows the publication of a Consensus Report by the National Academies of Science, Engineering and Medicine dated September 6, 2018. The full report is available for download here: https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

In its report, the Committee specifically recommended, as a security measure, paper ballots and audits:

> 4.11 Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.[1]

The Committee also analyzed the cyber security threats that exist for electronic voting systems and detailed those threats. These threats are exacerbated when an electronic voting system has no voter-marked and inspected paper artifact to check the software. Key findings on cyber security include:

- all digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists—is subject to malicious alteration;
- there is no technical mechanism currently available that can ensure that a computer application—such as one used to record or count votes—will produce accurate results;
- testing alone cannot ensure that systems have not been compromised; and

[1] *Securing the Vote: Protecting American Democracy* (2018) at 7, 80, The National Academies of Sciences, Engineering, And Medicine

- any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.[2]

Throughout 2018, current and former leaders of the U.S. Intelligence agencies have publicly warned that the threat of interference in U.S. elections continues this year and into the future. Director of National Intelligence Dan Coats and other intelligence chiefs laid out two central challenges for the United States: the flow of Russian misinformation and "shoring up the defense of electoral systems, which are run by individual states and were seen as highly vulnerable in 2016."[3] U.S. Homeland Security Secretary Kirstjen Nielsen, has stated several times (as recently as August 22, 2018) that she wants "all state and local election officials to make certain that by the 2020 presidential election, every American votes on a verifiable and auditable ballot."[4] These statements are consistent with the findings of the U.S. Senate Select Committee on Intelligence Report summarizing its findings on election security.[5] Specifically, the Committee, chaired by Senator Richard Burr (R-NC), recommended that "States should rapidly replace outdated and vulnerable voting systems. At a minimum, any machine purchased going forward should have a voter-verified paper trail and no WIFI capability." Furthermore, the Committee recommended that states implement "widespread, statistically sound audits of election results."

The two recent descriptions of the serious risks associated with paperless DRE systems and the intelligence community consensus belief that cyber intrusion into US elections will continue highlight the need for Pennsylvania to adequately fund the replacement of DRE systems before the 2020 election. Historically, Pennsylvania has been a key swing state in national elections. Other swing states either already use voter marked paper ballots or have replaced their systems to include a voter marked paper ballot. Virginia, Florida, Ohio, Wisconsin, Michigan and North Carolina are among the swing states that have paper records available for recounts or audits.[6] Pennsylvania should not lag behind other critical states in its efforts to secure our democracy.

Thank you for the opportunity to submit this testimony and for your consideration. We would welcome the opportunity to address the Committee and are available to provide any assistance to it as it considers these important issues.

---

[2] Id. at 90

[3] Matthew Rosenberg et al., *Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn*, New York Times (Feb. 18, 2018) available here: https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html

[4] Olivia Beavers, *DHS chief calls on officials in all 50 states to have 'verifiable' ballots by 2020 election*, The Hill, Aug. 22, 2018 available https://thehill.com/policy/cybersecurity/403148-dhs-chief-calls-on-election-officials-in-all-50-states-to-have

[5] https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated

[6] Verified Voting provides information on voting equipment used in the United States in its Verifier available here: https://www.verifiedvoting.org/verifier/#year/2018/