Allegheny County Board of Elections
Public Meeting on Purchase of Voting Systems
June 7, 2019 11:30 a.m.
Allegheny County Council, 436 Grant Street, Room 119, Pittsburgh, PA

Written Testimony of Verified Voting.org
Marian K. Schneider, President
June 5, 2019

Thank you, Chairman Baker and members of the Board, for allowing Verified Voting to submit written testimony in connection with the Public Meeting on the Purchase of Voting Systems. We hope to provide background on the security needs that counsel for the adoption of a new voting system with a verifiable and auditable paper ballot, and provide some high-level recommendations for consideration by the Board as it deliberates the purchase of new voting equipment for Allegheny County.

About Verified Voting

Verified Voting is a national, non-profit non-partisan organization. Verified Voting's mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections. Since our founding in 2004, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology experts who comprehend the risks associated with election technology. We have provided direct assistance to election officials in implementing the most efficient post-election audits to verify election results. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.

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.

In addition to our expertise and reputation in the field, Verified Voting has assets developed over years of monitoring election administration practice. These include the most complete, accurate and up-to-date publicly-accessible database of voting and tabulation systems in use, and comprehensive archives of news and publications on election technology. Our dataset on voting equipment is used and relied upon by organizations in need of reliable historical and current data on the election equipment. Further, we assist researchers, the press and the public by providing custom datasets for their use.

The Scope of the Problems with Election Security and Current Election Infrastructure

Election administration depends on computers at multiple points in the election process. Equipment for *voting* is but one part of a broad array of election technology infrastructure that supports the conduct of elections today. Some of that technology infrastructure includes voter registration databases, internet facing applications such as online voter registration and polling place lookup, network connections between state government and local jurisdictions, the computers that program the voting devices that record and count votes in addition to the voting devices themselves. Some jurisdictions also use electronic poll books to check voters in at polling sites and most states and localities report election night returns via a website.

To the extent that any of these can be compromised or manipulated, can contain errors, or can fail to operate correctly—or at all—this can potentially affect the vote. Election system security requires not only efforts to prevent breaches and malfunctions, but also fail-safes that address breaches or malfunctions that do occur and procedures to confirm the correctness of election outcomes.

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 and recent investigations demonstrate that state databases and third-party vendors not only were targeted for attack, but were breached.[1]

The intelligence community agrees that future attacks on American elections are inevitable.[2] The inevitability of attacks is a key concept in cyber security: it's not whether a system will be attacked, but when. Moreover, cyber security experts now agree that it is impossible to thwart all attacks on computer systems. Rather, best practice demands a multi-layered approach built around the concept of resiliency. Systems are resilient if owners can ***monitor, detect, respond and recover*** from either an intentional attack or a programming mistake or error. The capacity to recover from even a successful attack is integral to the security of U.S. elections.

---

[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.

The Board's immediate attention is focused on replacing Allegheny County's legacy paperless direct recording electronic (DRE) voting systems. Two basic kinds of electronic voting systems are used in the United States: Direct recording electronic (DRE) and optical scan systems. Both types of systems are computers, and both are prepared in similar ways. Currently, Allegheny County voters vote on DREs. Direct recording electronic 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[3] record of voter intent provided with a DRE system.

Because DRE systems lack a paper ballot that was separately marked by the voter and then tabulated, errors or malware on the software could result in an undetectable change in the election outcome. All DREs are vulnerable, even those with a "voter verifiable paper audit trail" (VVPAT) present security risks and verification challenges that are difficult to overcome.[4] A printout of election results from the memory card of a DRE 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.

Replacing DREs is urgent because, by design, it is impossible to verify that the computer correctly captured the voter's choices. Thus, DRE systems are not *resilient*. This inherent design flaw of DRE systems is why Governor Wolf has directed the counties to replace paperless DRE systems by the 2020 elections.

Mitigating Voting System Risks

Fortunately, for voting systems, a general consensus has formed on the steps necessary to provide a secure, resilient and verifiable election:

---

[3] Software independence in voting systems was described by Ron Rivest (MIT) and John Wack (NIST) as follows: "*A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome*." *See* Rivest, R. and Wack, J. "On the Notion of Software Independence in Voting Systems." Available at https://people.csail.mit.edu/rivest/RivestWackOnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[4] The Board may have 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. 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 (which is not a best practice but may occur anyway), 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

- A paper ballot (marked by pen or computerized ballot marking device) that voters can verify before casting;
- Tabulation of the marked ballot separately by an optical scanner;
- Routine, robust post-election audits to either confirm that reported outcomes are accurate or identify problems for further investigation before vote counts are finalized; and
- The ability to carry out full manual recounts if needed.

Optical scan systems leverage the speed of the computer to report unofficial results quickly. The difference between DRE and optical scan systems 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. The paper ballots provide a trustworthy record of voter intent and allow jurisdictions to monitor their system for problems, detect any errors, (whether due to hacking or accident), respond to them and recover by, if necessary, hand counting the paper ballots.

For technology used for marking and counting votes, voters must be able to confirm first-hand that their ballots were indeed marked as they intended, and election officials must be able to use those ballots to demonstrate that all the votes were included and were counted as cast. This process is crucial to defuse the narrative that our elections can be hacked.

This bridge between the voter and correctly reported outcomes requires a physical artifact as evidence of the voter's intent, and a process for checking. That artifact is typically the **paper ballot** that is voter-marked, either with a pen or pencil or through the use of an accessible interface such as a ballot marking device. Voting systems, especially ballot marking devices, should make it as easy as possible for voters to verify their ballots.

Post-election tabulation audits provide the crucial check of vote counts against voters' ballots. It is important to check the ballots themselves, not relying upon software-generated images or other artifacts that voters themselves could not verify. Effective audits manually inspect enough of the voter-verified paper ballots to provide strong evidence that the reported election outcomes match the ballots. The most robust tabulation audits, called **risk-limiting audits**, provide a large, statistically guaranteed minimum chance of correcting outcomes that are wrong due to tabulation errors. Colorado and Rhode Island have passed laws to require risk-limiting audits before election results are certified. Many other states require some other form of tabulation audit, which may or may not provide evidence that outcomes are correct -- and, in some states, is conducted too late to correct wrong outcomes. Pennsylvania requires a flat percentage (2%) audit but Allegheny County currently has no ability to conduct a meaningful audit with its current equipment.

Tabulation audits do not stand alone. Other compliance procedures ensure that all ballots are accounted for and the numbers of ballots cast reconciles with the number of voters who

signed in, and that important chain of custody security procedures have been followed each election. Put together, these practices provide assurance that voters' ballots determine the election results. Other election processes also should be routinely audited.

Full manual recounts must be available, when necessary, to correct election outcomes. Risk-limiting audits, by definition, require full manual recounts when audit samples do not find strong evidence that the reported outcome is correct. The best recount provisions allow for full recounts of elections with very close margins, and for full or partial recounts at candidate expense (unless errors are found) in other contests, all conducted by hand.

Consensus Support for Change

The chorus of voices calling for the security measure of voter marked paper ballots plus robust post-election audits has grown louder since 2016. 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. In explaining its ruling, the court outlined the constitutional imperative to secure election systems against modern cyberthreats, thus protecting voters' due process and equal protection rights.

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."[5]

In September 2018, the National Academies of Science, Engineering and Medicine (NASEM) issued a Consensus Report that, among other recommendations, emphasizes the importance of paper ballots and post-election audits.[6]:

> 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.

[5] *Curling v. Kemp,* No.1:17-CV-02589-AT, at 46

[6] National Academies of Science, Engineering, and Medicine, 2018, *Securing the Vote: Protecting American Democracy*, available for download at https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

5.6 Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election reporting, etc.) after each election….

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results…. [When fully implemented, risk]-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.[7]

The Committee also analyzed and detailed the cyber security threats that exist for electronic voting systems and other election systems. 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
- any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.

In Pennsylvania, PittCyber's Blue Ribbon Commission on Pennsylvania's Election Security Study and Recommendations echoes NASEM's recommendations and specifically calls for the replacement of vulnerable legacy DRE systems in Pennsylvania and the adoption of risk-limiting audits.[8]

Ballot Marking Devices

Allegheny's current precinct voting device, the ES&S iVotronic, is a DRE system and must be replaced because of its high susceptibility to an undetectable error or tampering in its programming. Under federal law, jurisdictions are required to provide a voting method so that voters with disabilities can privately and independently cast their ballots. DRE systems incorporate some accessibility features in all devices, allowing jurisdictions to provide a single device for all voters.

The new generation of proprietary commercially available voting systems address the problem of ensuring an auditable paper record and accessibility through the use of a ballot-

[7] *Securing the Vote* at 7-9.

[8] "The Blue Ribbon Commission On Pennsylvania's Election Security Study And Recommendations," Jan. 2019, *University of Pittsburgh Institute for Cyber Law Policy and Security*, available for download https://www.cyber.pitt.edu/report

marking device. These devices provide an electronic user interface and presentation of the ballot, permit the voter to mark their ballot and then print the voter's selections either on a ballot that is identical to one marked with a pen or pencil or a summary of the ballot choices. Ideally, the paper is presented to the voter for verification – an important step to ensuring a trustworthy record for audit. After verification, the paper ballot or summary ballot is scanned for tabulation and retained for recounts and audits.

Some of the new crop of ballot marking devices are similar to paper-based legacy systems that have been used in 13 counties in Pennsylvania since 2006. These systems use a uniform full-size ballot for all voters, which most voters mark by hand, and other voters mark using a ballot marking device with assistive interfaces. Usually these ballots are tabulated by scanners at the polling place but several counties in Pennsylvania tabulate the ballots centrally at the county offices.

Ballot marking devices provide undeniable benefits that may improve the voting experience for some voters. For example, they include assistive technologies such as read-aloud audio function to assist with marking and then verifying the ballot, can allow voters to adjust the text size, are able to present a variety of ballot styles on a single device and make it easier to present multilingual ballots.[9] Because not all voters can mark a ballot using a pen, and because not all voters can use screens, it is imperative that a variety of options for marking a ballot are available in the polling place for all voters.

A growing number of jurisdictions nationally and in Pennsylvania are adopting a new type of ballot marking device that do not produce ballots that are indistinguishable from those marked by hand. Instead, these systems produce summary ballots that show, for each contest that the voter could vote in, only the name of the contest and the voter's selection(s) – or show that the voter did not make a selection in that contest. Summary ballots may be the same size as the hand-marked ballots (although very different in appearance), or they may be substantially smaller. Many of these summary ballots also encode the voter selections as barcodes, which are easier to tabulate than the human-readable text of the selections. Even if the barcodes are non-proprietary and can be read by barcode readers, it may be difficult for a voter to discern whether a printed bar code properly reflects the voters' choices.

Some BMDs include an embedded scanner within the hardware. Such "all-in-one" devices present additional security challenges because they allow the ballot to pass through the printer after the voter has already viewed and ostensibly verified the ballot. Because the printer

[9] Brennan Center for Justice, Common Cause, National Election Defense Coalition, Verified Voting Foundation, *Securing the Nation's Voting Machines: A Toolkit for Advocates and Election Officials,* at 3 (May 31, 2018), available for download at https://www.brennancenter.org/publication/securing-nations-voting-machines

function and the tabulation function are both controlled by software, an attacker could exploit this hardware design to alter ballots after a voter has reviewed the ballot.[10]

Considerations in Selecting new Systems

As Allegheny County considers its voting system choice, Verified Voting urges the Board to consider a variety of issues relating to security, resiliency and verifiability. Because we count votes by computers, certain security risks and vulnerabilities are present and will always be present. The policy considerations involve reducing those risks as much as possible and deploying a system that allows Allegheny County to recover from any event that could interfere with the integrity of the election. In addition, the choice of voting system should ensure that voters have an available and appropriate voting method and that they can deliberately verify their choices before casting their ballots. Allegheny County should also ensure that any system it chooses facilitates the adoption of robust post-election audits, such as risk-limiting audits. An audit has value when it relies on a trustworthy record of voter intent, that cannot be undetectably altered by software, and has arrived at the end of the electoral process through a system that has rigorous chain of custody procedures.

All of the voting systems that have been certified in Pennsylvania incorporate a paper record but there are significant differences in how the systems are deployed and function in the field. Moreover, significant differences exist among the systems with regard to the ease of verification of the voter's choices and whether the voter has actually verified the paper record.

In light of the pervasive security vulnerabilities of all electronic voting systems, including Ballot Marking Devices (BMDs), the considerable cost of BMDs, the necessity for a deliberate verification of the paper record, Verified Voting endorses the use of voter-marked paper ballots, marked primarily with a pen or pencil, and supplemented with BMDs, as the best method for recording votes in public elections. Verified Voting believes that voters should have the opportunity to choose the method that best suits their needs while offering voters the opportunity to deliberately verify their ballots. BMD usage should not be limited to voters with identified disabilities; nor should all in-person voters be compelled to use BMDs. For several reasons, most precinct-based polling places are well served by one BMD and a separate tabulator. In this configuration, election procedures must assure that a critical mass of voters use the BMD. For instance, if necessary, some fraction of voters (such as every 20th voter) can be explicitly invited, but not required, to use the BMD. Such a process has several benefits: it preserves the secrecy of the ballot for voters who use the BMD and it ensures that poll workers and voters alike are familiar with the operation of the BMD to guarantee a smooth election.

[10] Appel, A., "Design flaw in Dominion ImageCast Evolution voting machine," *Freedom to Tinker*, Oct. 16, 2018, retrieved from https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine/

When deciding which system to choose, Verified Voting cautions against choosing ballot marking devices for all voters. This would, in essence, entail swapping one existing DRE for one ballot marking device. Allegheny County currently has 1,332 precincts and at least 2 DREs, if not more, in each precinct. Costs for a single ballot marking device can range from $6,200-$10,000 per device just for the purchase. Service contract pricing can be tied to the number of devices so annual costs could also be higher. Consequently, choosing BMDs for all voters could be the most expensive option.

Moreover, it is necessary to purchase enough of these expensive machines to accommodate all the voters who need them especially during peak election turnout. An inadequate number of BMDs, either because too few were allocated, or because some fail to work, can easily generate long lines, disenfranchising voters who are unable to wait for the machines and no emergency paper ballots are available. Pittsburgh has a history with long lines at the polls, even during the 2018 midterm elections.[11]

As described above, several options for purchase include "all-in-one" systems that combine marking of the ballot and tabulating of the ballot. The design flaw that allows a paper ballot to pass through the printer (controlled by software) after the ballot leaves the possession of the voter presents an unacceptable risk that the ballot could be altered in undetectable ways. Not only that, these devices present a risk that the election could be disrupted in a way that makes it impossible to recover the correct votes as intended by the voter. Such systems are neither "software independent" nor resilient. Verified Voting recommends BMDs that either separate the marking of the ballot from the tabulation function, or are designed in such a way that prevents the system from altering any ballots or voiding any ballots after the ballot has left the possession of the voter.

Voter-marked paper ballots can provide a trustworthy verification bridge from voter intent to vote tabulation: voters can verify that their marks reflect their intended choices, and election officials can verify, through audits and recounts, that the vote counts accurately reflect the voter marks. Both parts of the bridge are necessary. If a voting system does not provide a ballot that voters can verify, it is fatally insecure. If the system produces a marked ballot that in principle the voter *can* verify, then the system's security and trustworthiness depend in significant part on how many voters verify their ballots, how carefully, and what happens if they note discrepancies. Consequently, it is important to design all voting systems and procedures to strongly encourage as many voters to verify their ballots as possible.

BMDs raise voter verification concerns because voters who use them cannot verify their ballots until after entering all the selections. (In contrast, a voter who hand-marks a ballot can verify each selection as it is marked, then review the entire ballot before finally casting the

[11] *See e.g.,* Delano, J. "Reporter Update: Murrysville Voters Tired Of Long Lines At Polls". *KDKA2 CBS Pittsburgh* https://pittsburgh.cbslocal.com/video/4071328-reporter-update-murrysville-voters-tired-of-long-lines-at-polls/

ballot.) When verification cannot begin until late in the voting process, voters may tend to rush past it. As a result, voters can easily overlook errors, unintended choices, and even malicious changes in their selections, or even in which contests are listed on their ballots. With the proper attention to the verification process, including good ballot design, good system design, proper allocation of devices, and a process to encourage voters to deliberately verify their choices, a jurisdiction such as Allegheny County can create an environment to encourage deliberate verification of ballots for voters who vote on ballot marking devices.

A comprehensive system that uses a separate, single tabulation device for all ballots, regardless of whether they are marked by hand or marked by a ballot marking device, is preferable from a security and verifiability standpoint.

The availability of hand-marked paper ballots as an option for voters has other advantages. First, hand-marked paper ballots are significantly less expensive than BMDs. Most paper ballots, whether hand-marked or machine-marked, are tabulated by scanners, and typically a polling place will require only a single scanner unless the precinct is unusually large and then likely only one additional scanner. If, however, a scanner breaks down, voters can deposit their marked paper ballots in a ballot box for later scanning. No additional wait time is required. A voting system that incorporates hand-marked paper ballots for most voters is scalable and can easily handle a spike in voter turnout on election day. Either additional privacy booths may be added or voters can mark ballots in any convenient spot.

We do not believe that compelling all in-person voters to use BMDs is an effective way to protect the rights of voters with disabilities – especially when those BMDs have poor or questionable security and verification properties for all voters. At the same time, BMD use should not be restricted to voters who are unable to hand-mark their ballots. For several reasons, including ballot anonymity, quality assurance, and voter dignity, it is best to have a critical mass of voters using polling place BMDs throughout election day, assisted by pollworkers who are trained to help all voters appropriately. Crucially, to support this objective, the BMDs and election processes should meet the verifiability standards we have discussed.

Conclusion

Verified Voting is grateful for the opportunity to participate in this hearing today. Allegheny County, as Pennsylvania's second largest jurisdiction, can demonstrate its commitment to the integrity of elections by selecting a secure, verifiable and resilient voting system that serves the citizens of Allegheny County well.