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

United States House Committee on House Administration
hearing on "Election Security."

May 8, 2019

10:00 a.m. 1310 Longworth House Office Building, Washington, DC

Chair Lofgren, Ranking Member Davis and members of the Committee, thank you for the invitation to submit testimony to the Committee on House Administration hearing on "Election Security." We urge the Committee to move expeditiously to support state and local jurisdictions in strengthening their election systems and provide upfront and sustained investment in election infrastructure and security. Since 2016, it is clear that the threat to our democratic institution of voting is not theoretical, but real and persistent. We must, as a nation, adopt the clear solutions that will allow us to defuse the destructive narrative of election hacking that undermines the very fabric of our democracy.

About Verified Voting

Verified Voting's mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004 by Stanford computer science professor David Dill, 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 and malfunctions that do occur.

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 consensus among the intelligence community is 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.

Despite considerable progress in the last few years, much work must be done to secure our nation's elections infrastructure. Two primary areas that require immediate and sustained attention are 1) securing both the state and county networks, databases and data transmission infrastructure that touch elections; and 2) instilling confidence in election outcomes by replacing

---

[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.

older, vulnerable legacy voting systems with new systems that permit reliable recounts and post-election audits.

Voting System Infrastructure Risks

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. 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 paper ballots provide a trustworthy record of voter intent and allow 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.

Direct recording electronic (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[3] record of voter intent provided with a DRE system. In some states, the DRE systems produce a contemporaneous printout of the voter's choices known as a "voter verifiable paper audit trail" (VVPAT). That paper output cannot be handled by the voter, is usually viewed through a plastic window and may or may not be checked before the voter's choices are directly recorded onto computer memory. There is a risk that the choices saved onto the memory and tabulated may not match the paper record; alternatively, the paper record may not correctly reflect the voter's choices and the voter may not notice the error.

Because DRE systems lack a paper ballot that was separately marked by the voter and tabulated separately, errors or malware on the software could result in an undetectable change in the election outcome. Replacing DREs is urgent because, by design, it is impossible to verify that the computer correctly captured the voter's choices. Even those with VVPAT present security risks and verification challenges that are difficult to overcome.[4] A printout of election results

---

[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 committee 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

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.

Mitigating Voting System Risks

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

- A paper ballot (marked by pen or computerized ballot marking device) that voters can verify before casting;
- 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.

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. An inferior alternative, to be replaced as soon as possible, is the "Voter-Verifiable Paper Audit Trail" provided by some DRE machines. Whatever the physical record, it must have been available to the voter for his or her review prior to casting in order to serve as a record of voter intent. 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 weaker 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.

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. Many recount laws allow ballots to be re-tabulated by machine, inherently a poor response to cybersecurity concerns.

Consensus Support for Change

The chorus of voices calling for the security measure of voter marked paper ballots 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 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.[8]

Ongoing Improvements

Many savvy election officials throughout the country, at state and local levels, have always taken election security seriously, but after breaches of voter-registration sites were initially reported in mid-2016 the subject has risen to a top-level priority nationally. At many conferences for state and local election officials, security now is a topic of keynotes and workshops, and at some conferences has dominated the discussion. Speaking for myself, as the Deputy Secretary for Elections and Administration in Pennsylvania in 2016 and later as Special Advisor to Governor Tom Wolf on Election Policy, we implemented several steps in the runup to the 2016 election to protect election infrastructure, including issuing guidance to counties about implementing best practices to harden their voting systems, engaging with the United States Department of Homeland Security to conduct penetration testing and assessment of the PA Department of State's networks, engaging a security firm to also conduct penetration testing of those networks, evaluating and strengthening the voter registration database backup protocol, and planning for attacks on the Election Night Return website to foil any attempts to undermine it.

Election administration is generally run at the local level, complicating coordinated efforts to bolster election security. Approximately 8,000 jurisdictions administer elections in the United States, and many of those are small county or municipal government entities that serve a

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

[8] *Id*. at 90

few voters.[9] This decentralized structure causes variability in both election administration processes and cyber security readiness. While some view this decentralization as protective, the existence of such variability in resources can actually be more problematic as attackers seek to attack the weakest link. The existence of such variability in processes, equipment and best practices underscores the need for enough funding to reach those local jurisdictions.

Beginning in 2017, federal, state and local governments have engaged in concerted efforts to improve election cybersecurity. First, in January, 2017, the Department of Homeland Security designated elections as critical infrastructure. As a result, the Elections Infrastructure-Information Sharing Analysis Center (EI-ISAC) was created to provide information sharing and resources to states and localities involved in elections. Additional work on information sharing and dissemination of best practices occurs through the Elections Government Sector Coordinating Council established in October, 2017. Similarly, a private sector counterpart made up primarily of voting system vendors also works towards the information sharing goal.

Election officials in at least 36 states have engaged with the Center for Internet Security to place network monitoring services on their networks. Moreover, several organizations have researched and published guidelines for securing election computer assets, mostly focused on networks and network connected components.[10] Federal agencies including the Election Assistance Commission and the Department of Homeland Security, among others, have been working to disseminate this information as widely as possible.

On the voting system front, in 2016, 70% of voters voted on systems that had some kind of paper record. Currently, more voters, approximately 77% will likely vote on systems that have a paper record in 2020. Since March 2018, the states with the most vulnerable unverifiable equipment have made progress in moving towards replacing those systems. For example, Delaware plans to deploy new ballot marking devices for all voters and Georgia passed legislation appropriating the funding for new voting systems. Pennsylvania has directed all counties to replace their voting systems by the 2020 primary and all new systems must have a voter-marked paper ballot. Louisiana and South Carolina still use 100% paperless DRE systems, and in another 8 states, a significant number of voters still use paperless DRE systems as their primary voting method.[11]

---

[9] Kimball, D., Baybeck, B. "Are all Jurisdictions Equal? Size Disparity in Election Administration," *Election Law Journal,* Vol. 12, No. 2 at 131.

[10] *See, e.g.* Securing Voter Registration Data" National Protections and Programs Directorate, Department of Homeland Security, June 26, 2018 Retrieved from:https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_0.pdf; "A Handbook for Elections Infrastructure Security, Version 1.0." the Center for Internet Security, February 2018, Retrieved from: https://www.cisecurity.org/elections-resources/; "The State and Local Election Cybersecurity Playbook," Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2018. Retrieved from: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#practices. The extent to which jurisdictions adhere to these recommendations will determine the level of integrity they are perceived to have.

[11] Arkansas, Indiana, Kansas, Kentucky, Mississippi, New Jersey, Tennessee and Texas.

Only three states conduct routine, mandatory robust post-election audits and the remaining states vary widely in the effectiveness of post-election audit processes. Many states have worked to improve their post-election audits, either by strengthening their existing audit requirements or by moving toward implementation of risk-limiting audits. For the first time in 2018, Wisconsin conducted its mandatory post-election audits (which are not risk-limiting) before the final results were certified. Six states currently provide, in statute or rule, for mandatory or optional risk-limiting audits (RLAs), and several states are presently considering new RLA requirements. At least seven states have conducted pilot risk-limiting audits. Verified Voting has provided advice to legislators and others seeking to improve their states' audit requirements. We, along with other organizations, also provided crucial technical assistance in the first pilot RLAs in Virginia (conducted by the City of Fairfax in cooperation with state officials) and Rhode Island (conducted by the state board of elections in cooperation with local officials). These and other pilots have helped to model not only best election practices, but broad collaboration to address a national threat.

Although all of the steps that have occurred since 2016 are useful, and long overdue, it's clear that more work needs to be done. Historically, elections and election infrastructure have been woefully underfunded, and more resources are necessary to properly equip local jurisdictions to manage and lessen the risks associated with computerized voting.

Preparations for 2020 and Recommendations

Our discussion above has highlighted the steps necessary to secure our elections. To prepare for 2020, those best practices must be adopted more widely by as many jurisdictions as possible. For that to occur, adequate financial investment in cyber security best practices, replacement equipment and post-election audit processes needs to occur immediately and continue at a sustainable level moving forward.

Adoption of voting systems with voter marked paper ballots and risk-limiting audits would certainly be an important goal in advance of the 2020 election. We note, however, that some of the commercially available ballot marking devices sold today present some risk that voters will not intentionally verify that the device correctly captured their choices. The lack of intentional verification can weaken the effectiveness of a post-election audit as a tool to verify election outcomes. In the short term, in jurisdictions that have purchased ballot marking devices intended for use by all voters, we strongly urge an evaluation of voting processes to incorporate a separate step that reduces the risk that voters will neglect to verify their choices.

Equally important is the need for research into voters' verification of their ballots is funding to support science-based improvements to secure systems in the public interest. That research should endeavor to balance security and accessibility needs and reduce the tension between these two principles.

We see an urgent and ongoing need for investment to bolster national election security for 2020 and beyond. Here we briefly state some of the important focus areas:

- Unverifiable Direct Recording Electronic voting systems should be replaced with voter-verifiable systems with paper ballots as soon as possible. The replacement systems should make it as easy as possible for voters to verify their ballots and for officials to audit the tabulation.
- Rigorous post-election audits, preferably risk-limiting audits, should be adopted as soon as feasible, prioritizing federal and statewide contests. Such audits are possible wherever voter-marked paper ballots are used, Both technical and material support is needed to conduct these audits and by implication, increased funding.
- Funding to support audits and where necessary recounts of close contests in the nature of "recount insurance" when close contests require more scrutiny.
- Jurisdictions that have purchased ballot marking devices intended for use by all voters should urge voters to verify their ballots before casting, and should adopt procedures that support voters in verification. Current ballot marking devices raise concerns that voters will fail to check their ballots, undermining the ballots' value as evidence of voter intent.
- Research is needed into how effectively voters verify their ballots -- especially ballots printed by ballot marking devices – and how to enhance voter verification. This research should proceed in tandem with other usability research to ensure that all voters can vote independently and accurately.
- Continued investment in securing all aspects of election infrastructure – at all levels – from cyber attack remains essential. Voter registration databases, electronic pollbooks, voting systems and election reporting systems are among the targets that must be protected.
- Any legislation with funding should include the following:

    - Incentives for development of open source voting systems
    - Incentives for development of open source software to assist jurisdictions with implementing risk-limiting audits
    - Prohibition on direct recording electronic voting systems.
    - Prohibition on return of voted materials via the internet or mobile phone
    - Incentives for legal public testing of election systems to identify possible security vulnerabilities before systems are deployed in the field.
- Congress should consider expanding testing or certification requirements for election systems that do not specifically tabulate ballots. For example, electronic poll books are widely used but no federal oversight or testing occurs. In the short term, we recommend some method of examining those systems to identify key issues for correction before deployment.

Our nation's elections infrastructure is vitally important to our democracy. We must continue the progress that has begun in the last two years to ensure that our election systems and voting processes are resilient in the face of attack or disaster. With additional resources from Congress, the goal is within our reach.