VerifiedVoting

Statement of Verified Voting.org
Marian K. Schneider, President

United States House Committee on Science, Space, and Technology
Joint Investigations & Oversight and Research & Technology Subcommittee Hearing on
“Election Security: Voting Technology Vulnerabilities”
Subcommittee on Investigations and Oversight
Subcommittee on Research and Technology

June 25, 2019

2:00 pm Rayburn House Office Building, Washington, DC

Chairwoman Sherrill, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird and committee members, thank you for the invitation to submit a written statement in connection with the Joint Investigations & Oversight and Research & Technology Subcommittee Hearing on “Election Security: Voting Technology Vulnerabilities.” Our statement will focus on 1) a brief overview of technologies in use for election administration; 2) describe some of the risks associated with those technologies as well as solutions for mitigating those risks; 3) review the role that NIST and other agencies have played in developing technologies for secure elections; and 4) suggest regulatory changes necessary to address advances in voting technology and the changing threat model facing our elections.

The scale and scope of threats to U.S. elections go far beyond what the current federal policy framework can address. Since the Help America Vote Act was passed, technology has advanced and the security threat landscape has also evolved. It’s time to re-think the regulatory framework to align it with the current environment. Your committee plays a crucial role in shaping our collective response. We urge the committee to take the steps necessary to enact mandatory security measures for all technology that touches election administration, to ensure that the foundation of our democracy is protected from ongoing threats.

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. 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. 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.

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 the actual act of 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 but may also affect the public perception of a fair and accurate election. Election system security requires not only efforts to prevent breaches and malfunctions, but also fail-safes that remedy breaches and malfunctions that do occur.

Limitations of the Current Federal Policy Framework

The U.S. federal policy framework is not designed to ensure -- or even address -- the security of this complex and varied election infrastructure. U.S. elections are administered by state, county, and in some cases municipal officials. The Help America Vote Act of 2002 (HAVA) broke new ground by establishing the Election Assistance Commission. The EAC has very little regulatory authority, but it is tasked (inter alia) with adopting Voluntary Voting System Guidelines (VVSG), developed in collaboration with the National Institute of Standards and Technology (NIST), and with certifying systems under those standards. Although the VVSG is voluntary, many states require their own voting systems to be certified under the standards. The VVSG applies only to voting systems. The EAC can address other parts of election infrastructure in its role as a clearinghouse for election administration information, but has limited resources for doing so. Neither the EAC nor any other federal agency or department has ever been given clear responsibility and resources directed toward countering persistent and coordinated cyber attacks on election systems. In the past, state and local officials have not been trained or funded to thwart cyber attacks on our election system let alone attacks coordinated by another nation state. Yet that is the threat our nation confronts.

Since the 2016 election, and as a result of the national security community warnings that the potential for attacks against our election infrastructure is real and ongoing, federal agencies have launched new initiatives to work with state and local governments and election officials to increase the understanding of cyber security threats to elections, to prepare election offices to address the threat and provide the tools to recover from breaches should they occur.[1] The DHS-funded Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has facilitated timely communication about threat mitigation. Other organizations and groups have also worked to provide best practices for security of election assets by publishing handbooks and guides.[2] State and local election offices have also engaged in "table top" exercises to simulate real-time election day incidents and practice incident response process in advance of a cyber security event. These efforts are a welcome change of relatively recent vintage. But, for local election officials to be better prepared, they need resources to continue the existing efforts and ongoing training, even with the support that DHS currently offers. As we discuss below, technology touches election administration in numerous places and the use of technology requires additional resources to ensure the validity of the election.

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

Voter Registration Databases

Under the Help America Vote Act, states were required to adopt "a single, uniform, official, centralized, interactive computerized statewide voter registration list defined,

[1] *See e.g.*, Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA), for a summary of its work with Elections Officials, through its program "#Protect2020" available here: https://www.dhs.gov/cisa/protect2020

[2] 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.

maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State."[3] Those databases are usually stored on the state's network and are accessed by the local jurisdictions who have authority to register voters.

These systems face substantial security threats. Statewide voter registration databases are connected to localities and other agencies via networks, potentially exposing them to attack. Likewise, internet-facing applications and tools that touch voter registration present their own set of risks to the integrity of the voter registration rolls because they are connected to the Internet. Finally, complete and accurate voter registration lists must be available at the polling place. When jurisdictions choose electronic pollbooks to check voter registration status and sign voters in, these e-pollbooks become another target. We further discuss this threat below.

The cybersecurity risks presented by network-connected voter registration databases are no different than similar risks presented by other databases that contain mission critical data and personally identifying information. According to the U.S. Department of Homeland Security, voter registration databases are vulnerable to a variety of attacks using an equal variety of methods. These can include direct web-based attacks that seek to inject or send commands to enable the attacker to gain unauthorized access to information; denial of service attacks that prevent legitimate users from being able to use election information or services; ransomware attacks that block legitimate users' access to a system until a ransom is paid; and more. Phishing attacks involve forged emails or other messages designed to get the recipient to click on malicious links or otherwise provide an entry point for stealing credentials such as passwords, spread malware or disrupt voting operations.[4]

Although the Help America Vote Act required states to centralize voter registration databases, mainly to provide a more uniform experience for voters rather than relying on a patchwork of systems that varied widely within a state, that statute did not contemplate the advances in technology or the evolving threats directed to those technologies. For example, HAVA does not regulate online voter registration applications or automatic voter registration systems but those are becoming increasingly widespread. Moreover, the creation and deployment of voter registration systems varies from custom-created in-house, to vendor-supplied, to commercial software packages that can be configured.

[3] Help America Vote Act, 52 U.S. Code § 21083.

[4] "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;

In the consensus study report "Securing the Vote" the National Academies of Sciences, Engineering and Medicine found that voter registration databases are subject to cybersecurity vulnerabilities and attacks. In addition, because such databases contain personally identifying information, significant harm could occur if such databases were breached.[5] The National Academies recommended routine assessment of voter registration databases that would allow jurisdictions to detect any tampering or interference with the database. We support that recommendation. To implement it, states and localities need the appropriate resources to conduct such assessments. Federal support is warranted to address these threats to national elections. Moreover, it is imperative that a regulatory framework or guideline be developed by NIST or an agency with cyber security expertise, against which such voter registration systems could be examined or audited.

Electronic poll books

Electronic poll books (EPBs) are computerized and usually networked devices that substitute for paper lists of voters in a polling place. These EPBs serve several useful functions for checking voter status, checking voters in to vote, enabling poll workers to guide voters to a different location if needed, and more. The spread of electronic poll books has been significant in recent years; 34 states are currently using EPBs in some or all jurisdictions.

The correct functioning of such devices is crucial and can affect voters' ability to cast an effective ballot. Because electronic poll books rely on communications connectivity that must function in real-time on Election Day, failure of such devices can result in late-opening polling places and disenfranchisement of voters who cannot wait for a paper back-up to arrive, or who may not be offered a failsafe provisional ballot. In their Preliminary Report on the 2018 Midterm Elections, the Election Protection Coalition reported that among other technology issues affecting voters, there were numerous instances of "broken voter check-in machines or e-poll books which prevented or slowed the voting process[.…] In the most severe cases, faulty or insufficient equipment caused hours-long delays and resulted in many voters being unable to vote."[6] Recently the Department of Homeland Security announced it would conduct forensic investigation of EPBs that caused significant problems in North Carolina in 2016[7], after it was revealed that systems of the company providing the EPBs had been breached in another state.

[5] "Securing the Vote: Protecting American Democracy." The National Academies of Sciences, Engineering and Medicine, Consensus Study Report, September, 2018 at 63.

[6] https://lawyerscommittee.org/wp-content/uploads/2018/12/Election-Protection-Preliminary-Report-on-the-2018-Midterm-Elections.pdf

[7] https://www.washingtonpost.com/investigations/federal-investigators-to-examine-equipment-from-2016-north-carolina-election-amid-renewed-fears-of-russian-hacking/2019/06/05/b70402e6-7816-11e9-b7ae-390de4259661_story.html?utm_term=.93292ced5c5b

Despite the risks inherent in using computerized networked systems for checking in voters, there are no national standards for electronic poll books, and most states using them do not require a certification process. Some states conduct testing and certification, yet even those standards vary from state to state and may not be sufficient.

An important mitigation where EPBs are deployed is to provide paper poll books in case of EPB system failures, and a sufficient quantity of provisional ballots to issue when needed, so that the flow of voters at the polling place will not be unduly interrupted. Election officials also may avail themselves of risk and vulnerability assessments (RVA), remote penetration testing and vulnerability scans, provided by the Cybersecurity and Infrastructure Security Agency (CISA) of DHS.

However, additional structural fixes are needed if such systems are to be used safely. In the consensus report "Securing the Vote," the National Academies found that "Congress should authorize and fund the National Institute of Standards and Technology, in consultation with the U.S. Election Assistance Commission, to develop security standards and verification and validation protocols for electronic pollbooks in addition to the standards and verification and validation protocols they have developed for voting systems."

The report further found that "election administrators should routinely assess the security of electronic pollbooks against a range of threats such as threats to the integrity, confidentiality, or availability of pollbooks. They should develop plans that detail security procedures for assessing electronic pollbook integrity."

Both are sound recommendations. As with voting registration databases, we recommend ensuring that election officials have the necessary resources to carry out these assessments.

Electronic Voting Systems

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.

Since 2016, the percentage of states with some form of paper record has increased from 70% to 77%. While that progress is laudable, the movement towards effective post-election tabulation audits that would confirm that the software-reported results are correct has occurred much more slowly. In addition, there has been no comprehensive regulatory oversight of whether commercially available options actually facilitate effective post-election audits. Are the voting devices on the market designed to ensure that voters verify that their choices are correct? Are all voters able to verify their votes without relying on the voting system itself? Is the record that is preserved a trustworthy artifact of voter intent? To the extent that system design, software configuration, hardware design or other factors interfere with the preservation of a trustworthy record, the utility of post-election audits is undermined.

The Role of Science Agencies in Standards-Setting, Research and Development

Under the Help America Vote Act, the National Institute of Standards and Technology (NIST) functions as an independent team of expert advisors, giving technical guidance to the Election Assistance Commission in particular for the development of the Voluntary Voting System Guidelines (VVSG). NIST further has published guidance on topics relevant to electoral systems, including several on security best practices for remote electronic voting and materials transmission for military and overseas voters.[8] Those publications contain crucial information about best practices in the use of various computer and communications technologies to support secure elections. However, this work has insufficient impact. None of NIST's guidance is mandatory. NIST's recent collaboration with EAC and with stakeholders in the development of the newest VVSG draft helped to profoundly change and improve how those principles and guidelines are generated, thinking beyond just voting systems to the broader election context, but the guidelines nonetheless are limited to the narrow focus of voting systems.

With additional funding, NIST has the potential and technical expertise to provide much more than it does today, whether independently or in collaboration with the EAC. For example, it could readily develop guidelines against which voter registration systems, electronic poll books and even election night reporting systems should be tested, even absent EAC oversight of such a testing function. Such guidelines would help states' election administrators to ensure they are taking all the steps necessary to safeguard those critical systems and reduce the likelihood

[8] https://www.nist.gov/itl/voting/publications

and impact of foreign interference or other tampering, as well as problems caused by malfunctions. Congress could make such guidelines mandatory, or at a minimum, create incentives for states to adhere to them.

NIST could also assist in developing standards for post-election audits and the emerging systems used to support the conduct of audits. The conduct of rigorous audits is essential to ensuring reliable election outcomes and voter confidence; no amount of voting system testing or certification can substitute for this process. While NIST has provided valuable insight through its Auditability Working Group[9], it could further support this critical process. These additional tasks for NIST can succeed because NIST has the ability to leverage its considerable scientific expertise to tackle these problems.

Two other science agencies, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF), have a significant impact on electoral systems and security by funding research and development of systems and methods that can improve election security, and could do more with directed initiatives and sufficient funding. The Defense Advanced Research Projects Agency (DARPA) has granted an award of $10 million to Galois, Inc. for open source development of two demonstration voting systems on a secure software platform, one a ballot marking device and the other a ballot scanning device that counts votes from the scanned ballots.[10] Such initiatives are crucial because election system vendors, operating in a niche market, have not demonstrated the ability to innovate for excellence in election security and usability. Federal research and development support can produce new designs and software solutions that vendors can incorporate in their systems or pave the way for publicly-owned open source solutions that might have significant cost savings for governments. All of this work supporting the sound science behind election security should proceed in coordination with DHS' own efforts in this regard and with EAC's work on election administration.

The National Science Foundation (NSF) engagement in funding studies and investigations into various aspects of voting system security has been extremely valuable, but not constant. Some past examples include a 1999 study on Internet voting[11]; a multi-year initiative starting in 2005 for "A Center for Correct, Usable, Reliable, Auditable and Transparent Elections" (ACCURATE)[12]; a 2007 grant for developing an open source system called Prime III[13]; grants in 2014 for studying open audit voting systems and protocols[14]; and a grant starting

[9] https://www.nist.gov/document-7152
[10] https://defensesystems.com/articles/2019/03/18/darpa-secure-voting.aspx
[11] https://www.nsf.gov/od/lpa/news/press/01/pr0118.htm
[12] https://www.nsf.gov/news/news_summ.jsp?cntn_id=111660
[13] https://www.nsf.gov/awardsearch/showAward?AWD_ID=0738175
[14] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1421373

in 2015 for studying the threats to election integrity deriving from poor ballot usability[15], among others. These examples illustrate the potential for scientific initiatives to support improvements in U.S. voting technology. Election security is not a one-time challenge; it warrants ample and sustained research investment.

Recommendations for Modernizing the Regulatory Framework around Election Security

In summary, we see both immediate needs to bolster public investment in the science of election security, and a broader need to rethink the policy framework that shapes our national response to election security threats.

- Standards-setting must extend beyond voting systems to other election technologies, including voter registration databases, electronic pollbooks, and election reporting systems. With statutory support and funding, NIST is well positioned to lead these efforts as it has led the ambitious effort to update the Voluntary Voting System Guidelines.
- NIST and other agencies should receive ample funding to add additional highly qualified staff, to support standards-setting work and to inform policymakers and election administrators.
- NSF and other agencies should be fully funded to invest in research and development into election security threats and mitigations.
- Broader deliberation is needed on how best to adapt the HAVA framework to today's election security challenges. The various roles of DHS, EAC, NIST, DARPA, NSF, and other agencies are not always clearly defined, and nothing in current law addresses many of the threats we have discussed here. It is easy to recommend that all these agencies should receive more funding for their election protection work -- but how should the work be divided and coordinated? We would like to see a blue-ribbon panel specifically study the policy questions of interagency coordination on election security, taking into account the need for cooperation with state and local policymakers and officials.

[15] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1550936