COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

HEARING CHARTER

Election Security: Voting Technology Vulnerabilities

Tuesday, June 25, 2019
2:00 p.m.
2318 Rayburn House Office Building

PURPOSE

The purpose of the hearing is to review the security of US election system technologies, such as e-poll books, voter registration systems, and voting machines, and the maintenance and operations activities that support them. The Subcommittees will discuss research and other activities being carried out under the Help America Vote Act (HAVA), which directed the National Institute of Standards and Technology (NIST) to develop voluntary voting systems guidelines in collaboration with the Election Assistance Commission (EAC). The Subcommittees will also explore policy strategies for protecting the full technology enterprise associated with election systems and recommendations from the 2018 National Academies report, *Securing the Vote: Protecting American Democracy*.

WITNESSES

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Neal Kelley**, Registrar of Voters, Orange County, California
- **Dr. Latanya Sweeney**, Professor of Government and Technology in Residence, Department of Government, Harvard University, Institute for Quantitative Social Science
- **Mr. Paul Ziriax,** Secretary, Oklahoma State Election Board
- **Dr. Josh Benaloh**, Senior Cryptographer, Microsoft Research

KEY QUESTIONS

- What are the technology components associated with conducting a secure election?
- What types of voting technology vulnerabilities were seen during the 2016 and 2018 election cycles?
- What are the roles of NIST and other science agencies in developing technologies and best practices for secure elections?
- What are some of the barriers that election officials face as they seek to enhance the security of their systems?
- Are legislative changes needed to adapt existing programs to modern technology issues?

BACKGROUND

Help America Vote Act (HAVA 2002) and Voluntary Voting System Guidelines (VVSG)

In October 2002, Congress passed the Help America Vote Act,[1] which (among other things) created the US Election Assistance Commission and authorized election-related activities at NIST.[2] Under HAVA, NIST carries out research to inform the development of the voluntary voting systems guidelines to be recommended to the EAC. This research includes security of computers used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting.

HAVA also established the Technical Guidelines Development Committee (TGDC).[3] TGDC is the forum where voluntary voting system guidelines are developed, with NIST serving as the technical and administrative lead. The other members of TGDC include representatives of the EAC, representatives of the National Association of State Election directors (NASED), and outside experts.[4] The purpose of TGDC[5] is to develop voluntary voting system guidelines which states and counties in the U.S. can use to enhance the security, functionality, usability, accessibility, auditability, privacy etc. of their election systems.

The EAC Commissioners then vote to recognize the recommendations that TGDC promulgates. EAC also provides technical assistance and grants to states that support implementation of election system improvements according to TGDC guidelines. For example, in March 2018, the EAC awarded a grant to the New Jersey Secretary of State that would be used in part to implement secure Automatic Voter Registration at the NJ Motor Vehicle Commission and to pilot voting systems with a voter verified paper audit trail.[6]

HAVA 2002 does not establish any compulsory voting system security requirements for states; the Constitution grants states wide latitude in how to administer elections.[7] Any compulsory federal requirements would likely be issued by the Department of Homeland Security.

In 2004 NIST and the EAC released their first set of election administration protocols., the Voluntary Voting System Guidelines 1.0.[8] In March 2015, NIST and the EAC released an update, VVSG 1.1.[9] States have discretion whether to adopt some of all of the VVSG recommendations. As of 2019, 12 states require full federal certification of their election systems under VVSG.[10] Eight states have no federal testing or certification requirements.[11]

---

[1] Public Law 107–252
[2] https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/
[3] https://www.nist.gov/itl/voting
[4] https://www.eac.gov/about/tgdc-roster/
[5] https://www.eac.gov/assets/1/6/TGDC2019Charter.pdf
[6] https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/
[7] https://www.whitehouse.gov/about-the-white-house/elections-voting/
[8] https://www.eac.gov/assets/1/28/VVSG.1.0_Volume_1.PDF
[9] https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf
[10] DE, GA, ID, LA, NC, ND, OH, SC, SD, WA, WV, WY
[11] http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

On February 15, 2019, the EAC Commissioners voted unanimously to publish a new VVSG promulgated by NIST, VVSG 2.0. The comment period closed on May 29, 2019. NIST is working now to resolve outstanding questions from the EAC and stakeholder process.

National Science Foundation Research

Another element of the U.S. election system within the Committee's purview is relevant research at NSF. As part of its own broad science mission, the National Science Foundation (NSF) carries out fundamental computer science research activities with relevance to election technology and social science research with relevance to voter interface with elections technology.

Technology Elements of the Voting System

Before The Vote

Voting registration portals/interfaces. There are more than 10,000 election jurisdictions in the United States. Depending on the jurisdiction, voters can register in person at election offices, at Departments of Motor Vehicles, or other public agencies.[12] Thirty-seven states and the District of Columbia allow for online voter registration, which can be conducted through state election board websites or within another public agencies' websites. Fifteen states allow same-day voter registration and 9 states and DC have automatic voter registration, where voters must "opt-out" when they interact with a government agency for another purpose (e.g. the DMV).[13]

Voter registration databases (VRDs). HAVA 2002 requires states to create a "single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level[14]" where voter registration data is stored. States use a variety of software products, with varying levels of cybersecurity controls, for the database platforms that aggregate and store this information. VRDs are then used to populate poll books.

Location election websites. Voters frequently use local and state election websites to seek information about where to cast their vote. Many jurisdictions' websites will allow voters to input their home address in order to be matched with their polling place.

Poll books. Poll books are the resource that poll workers use on election day to verify voters are who they say they are, and that they are eligible to vote in that location.[15] A transition from paper to "e-poll books" on computers or tablets has been underway for several years. Some e-poll books contain electronic data that was pre-loaded onto the device in static form and do not maintain an internet connection on election day, while others allow access to VRDs via a live internet connection.[16]

[12] Ibid.
[13] Ibid.
[14] http://uscode.house.gov/view.xhtml?req=(title:52%20section:21083%20edition:prelim)
[15] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy
[16] Ibid.

Casting Votes

Direct recording electronic (DRE) voting machines. These devices are the voting machines themselves – where voters record their choices directly at a digital interface and a computer counts the (paper-free) vote. Voting machines with a mechanical lever are no longer in use.

Ballot-marking devices (BMDs). Some jurisdictions that do not use DREs use ballot-marking devices, where the voter selects candidates from an electronic interface and the electronic device physically marks a paper ballot accordingly. BMDs are one method of improving accessibility for blind and handicapped voters. These ballots are usually counted by optical scanners.

Optical scanners. In jurisdictions where voters hand-mark a paper ballot or use a BMD to cast their votes, ballots are usually fed into a scanning device to be "read" and counted. Scanning devices may be available on-site at each polling place, but some jurisdictions will bundle up their paper ballots and deliver them to a central location where they are scanned.

Counting, Reporting and Verifying the Vote

After the polls close, paper ballot votes may be counted manually; paper ballots may be scanned and counted digitally; and votes cast using electronic systems may be counted digitally.[17]

Voting tabulator machines. These devices are deployed at election precinct headquarters to aggregate the votes cast across the polling stations in a jurisdiction after the polls have closed. Administrators at a polling station will extract a removable media device (e.g., a flash drive) from their voting machines after polls have closed and physically deliver the device to the precinct headquarters so its data can be aggregated on the voting tabulator.

Election night reporting systems. The process by which election administrators transmit the county and state level totals to government websites. For example, in precincts using electronic DRE voting machines and centralized tabulators, administrators at a polling station will extract a removable media device (e.g., a flash drive) from their DREs after polls have closed and physically deliver the device to precinct headquarters so its data can be aggregated on the tabulator. The information from the tabulator is then exported to a reporting website.

Ballot reconciliation. Election officials use a variety of methods at the end of election day to ensure the various technology components of the election system see "agreement" as a check for system malfunctions or interference. For example, a polling station will compare the number of voters that signed in at the poll book with the number of votes cast as recorded by the tabulator.

Ongoing

Maintenance and programming activities. Private vendors of election technologies will use a variety of strategies to program the hardware and software before the point of sale and to maintain those systems with upgrades once they are in circulation. For example, vendors will

[17] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

program an electronic DRE voting machine in advance of an election to display the candidates for that particular race.

What HAVA 2002 does not address

HAVA 2002 establishes federal responsibilities for testing, certification, training, technical assistance, grant-making and other activities related to voting systems. In turn, Section 301(b) of HAVA 2002[18] defines "voting system" as follows:

> (b) VOTING SYSTEM DEFINED.—In this section, the term "voting system" means—
> (1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—
> (A) to define ballots;
> (B) to cast and count votes;
> (C) to report or display election results; and
> (D) to maintain and produce any audit trail information; and
> (2) the practices and associated documentation used—
> (A) to identify system components and versions of such components;
> (B) to test the system during its development and maintenance;
> (C) to maintain records of system errors and defects;
> (D) to determine specific system changes to be made to a system after the initial qualification of the system; and
> (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

Under this definition, the legal mandate for NIST to assist in creating standards extends to only some of the election components described above.

Authorized by HAVA 2002

- Direct recording electronic (DRE) voting machines
- Ballot-marking devices
- Optical scanners
- Tabulator machines
- Voting machine upgrades
- Voting system testing laboratories

No legal mandate to test and certify

- Voter registration portals
- Voter registration databases
- Local election websites
- E-poll books
- Election night reporting systems
- Ballot reconciliation methods
- Maintenance, programming activities conducted by election vendors

[18] https://www.eac.gov/assets/1/6/HAVA41.PDF

Recent Incidents of Insecure Voting Infrastructure

In September 2017, the Department of Homeland Security contacted **21 states** to notify them that their election systems had been targeted by Russian hackers during the 2016 cycle.[19] A Senate Select Committee on Intelligence report that followed in May 2018 found that in at least six of the 21 states, "the Russian-affiliated cyber actors went beyond scanning and conducted malicious access attempts on voting-related websites."[20]

In May 2019, Special Counsel Robert Mueller released the *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.*[21] The Mueller Report describes how Russian GRU officers "targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities."[22] Russia also targeted "private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations." Special Counsel Mueller noted that this interference continued through the November 2016 elections.[23]

Special Counsel Mueller concluded his only public speech about the report by made emphasizing, "**there were multiple, systematic efforts to interfere in our election. That allegation deserves the attention of every American**.[24]"

Some of the incidents described below are presumably captured in the DHS count of 21 states.

- Two counties in **Florida** experienced breaches in their election networks during the 2016 election using spearfishing emails. Malware was also planted in systems at a manufacturer of election equipment, later identified as VR Systems.[25]

- In 2018 in **Johnson County, Indiana**, internet connections between e-poll books faltered, preventing e-poll books from tapping voter registration data and from communicating with one another. The lapse stopped voting entirely for four hours, with no extension of polling hours, and created an opportunity for a voter to vote twice in Johnson County.[26]

- In 2018, **Riverside County, California** saw unauthorized changes had been made to registered voters' party affiliations via internet access. Election officials were unable to identify the source of the changes as their systems did not track the IP addresses responsible.

[19] https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.31f42a3824a5
[20] https://www.intelligence.senate.gov/publications/russia-inquiry
[21] Full text of the Mueller Report: https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf.
[22] Ibid page 50
[23] Ibid page 50
[24] https://www.justice.gov/opa/speech/special-counsel-robert-s-mueller-iii-makes-statement-investigation-russian-interference
[25] https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016
[26] https://cha.house.gov/sites/democrats.cha.house.gov/files/documents/JLH%20CHA%20Election%20Security%20Testimony%20190508-FINAL%20%28002%29.pdf

- During the 2018 general election, **New York City** saw unprecedented lines to vote at numerous polling places as a result of jammed optical scanning equipment. It was later determined that high-humidity weather likely caused the machines to malfunction.[27]

- In June 2016, the **Illinois** Board of Elections network was hacked and intruders spent several weeks exploring the network, downloading the voter registration database and data about individual voters. The attackers then crashed a server, alerting officials of their presence.

- In 2016 the **Arizona** state elections website was breached by the same agent who attacked the Illinois Board of Elections. The intruders installed malware in the website.[28]

- During early voting for the 2018 general election in **Texas,** some electronic DRE voting machines deleted votes for Democratic candidates or switched them to Republican candidates. The machines in question were used in 78 of 254 Texas counties.[29]

- Early voters in **Georgia** in 2018 saw DRE machines deleting votes and switching them to other candidates. The machines where voters saw this occur were purchased in 2002.[30]

- In May 2018, the **Knox County, Tennessee** election website was hit with a distributed denial-of-service (DDoS) attack that crashed the website that displays election results.[31]

- In 2016, a vendor serving **Durham County, North Carolina** inadvertently created a pathway for attackers to breach the State Board of Elections' records by running an insecure remote-access software to service the county's voter registration database and e-poll books.[32]

- In September 2019, a researcher found an unlocked online repository containing what he said were "master passwords" for touchscreen voting machines in **North Carolina**. The repository also contained serial numbers for machines that had modems. State officials admitted the file should not have been publicly available online.[33]

- In late 2018, independent investigators found that the computer servers that provide the platform for **Wisconsin**'s reporting of elections results were running a service called FTP that enables access to sensitive information without a password.[34]

- The Wisconsin investigation also discovered that the servers powering **Kentucky**'s online voter registration were similarly exposed to tampering or exploitation via an FTP.[35]

---

[27] https://www.propublica.org/article/new-york-city-polling-places-midterms-2018-humidity
[28] Ibid..
[29] https://subscriber.politicopro.com/article/2018/11/voting-machine-errors-already-roil-texas-and-georgia-races-916984
[30] Ibid
[31] https://www.knoxnews.com/story/news/2018/05/02/knox-county-officials-investigating-election-night-cyberattack/572236002/
[32] https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582
[33] https://www.politico.com/newsletters/morning-cybersecurity/2019/06/10/cisa-budget-data-brokers-on-congressional-slate-this-week-648194
[34] https://www.propublica.org/article/file-sharing-software-on-state-election-servers-could-expose-them-to-intruders
[35] Ibid