BRENNAN CENTER FOR JUSTICE

House Committee on Science, Space and Technology
Subcommittee on Investigations & Oversight
Subcommittee on Research & Technology
United States House of Representatives

Statement for the Record
Brennan Center for Justice at NYU School of Law

"Election Security: Voting Technology Vulnerabilities"

June 24, 2019

The Brennan Center thanks the House Committee on Science, Space and Technology for holding this hearing.

Our country has made significant progress to secure our elections infrastructure from cyber-attack since 2016. The designation by the Department of Homeland Security ("DHS") of election infrastructure as critical infrastructure means state and local election offices have priority access to needed resources, including cybersecurity advisors and risk assessments. As a result, election officials have participated in thousands of hours of cybersecurity trainings and table-top exercises to prevent, detect, and recover from intrusions into critical election infrastructure.[1] DHS and the Election Assistance Commission ("EAC") have facilitated much better information sharing between election system vendors, the states, and the federal government. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Finally, in 2018 Congress provided $380 million in Help America Vote Act ("HAVA") funds to help states bolster their election security. Based on information provided by the EAC, we know that roughly 90% of this money will be spent prior to the presidential election on such critical measures as strengthening election cybersecurity, purchasing new voting equipment, and improving post-

[1] John V. Kelly, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, Office of Inspector General, Department of Homeland Security, February 18, 2019, https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf.

election audits, all essential steps in protecting our elections from foreign interference.[2]

Nevertheless, significant security gaps remain. We should be doing more to secure our election infrastructure in the following areas, several of which are particularly relevant to the jurisdiction of the House Committee on Science, Space and Technology: (1) replacing paperless voting systems and requiring robust post-election audits; (2) adding electronic poll books to the federal certification process; (3) conducting penetration testing and nationwide threat assessments of the nation's election infrastructure; (4) requiring election system vendors to report cyber incidents; (5) requiring the National Institute of Standards and Technology ("NIST") to create an Election Profile to guide adoption of the Cybersecurity Framework nationwide for elections infrastructure; and (6) providing additional funding to state and local election officials to secure election systems nationwide.

Replace Paperless Voting Systems and Robust Post-Election Audits

The Brennan Center has long supported both a complete, nationwide transition to paper ballot voting machines and the implementation of risk limiting audits ("RLAs") to ensure security and confidence in electoral results.

In the event a virus or other malicious software is introduced into a voting machine, voter-marked paper ballots can be used to detect and recover from that attack. The National Academy of Sciences, Engineering, and Medicine is just one of the latest authorities to examine paperless voting systems and conclude that they should be "removed from service as soon as possible" to ensure the security and integrity of American elections.[3] They have been joined in this conclusion by the U.S. Senate Select Committee on Intelligence, as well as security experts around the country, all of whom have argued that continued use of these systems presents an

---

[2] *Discussion on Recommendations from the ODIHR Observation of the 2018 Mid-Term Congressional Elections,* OSCE Office for Democratic Institutions and Human Rights (June 18, 2019) (statement of Benjamin Hovland, EAC Commissioner); *Grant Expenditure Report, Fiscal Year 2018*, The U.S. Election Assistance Commission, April 4, 2019, https://www.eac.gov/assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf.

[3] *Securing the Vote: Protecting American Democracy*, The National Academies of Sciences, Engineering, and Medicine, 2018, 5, https://www.nap.edu/read/25120/chapter/1.

unnecessary security risk.[4]

Today, 11 states still use paperless electronic machines as the primary polling place equipment in at least some counties and towns (Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee and Texas). Three (Georgia, Louisiana, and South Carolina) continue to use such systems statewide.[5] There is still time for these jurisdictions to transition to paper-based voting systems before the 2020 presidential election. Approximately $300 million is still needed to replace the remaining paperless voting systems in use throughout the country.[6] Congress should act to ensure that every vote in 2020 is supported by a secure and verifiable record of voters' decisions, in the form of a paper back up, to help guard against electronic manipulation.

Of course, without robust election audits comparing paper records to software totals, the value of that paper record is more theoretical than actual. For this reason, we support robust post-election audits that will

---

[4] *Securing the Vote: Protecting American Democracy*, The National Academies of Sciences, Engineering, and Medicine; *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, U.S. Senate Select Committee on Intelligence, May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/; *Study and Recommendations*, The Blue Ribbon Commission on Pennsylvania's Election Security, 2019, 21, https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf.

[5] "The Verifier — Polling Place Equipment — November 2018," Verified Voting, accessed June 24, 2019, https://www.verifiedvoting.org/verifier/; Delaware rolled out new machines with paper backups on May 14 of this year. See Amy Cherry, "Delawareans to get 1st look at new voting machines in upcoming school board elections," WDEL, May 6, 2019, https://www.wdel.com/news/video-delawareans-to-get-st-look-at-new-votingmachines/article_7d625346-6ddd-11e9-a2c7-4f6dfafa74af.html.

[6] Relying mainly on Verified Voting data from November 2018, we estimated that approximately 37,232 precincts
are using paperless DREs as the primary polling place equipment (this number excludes precincts in Delaware which replaced machines in May 2019). We multiplied this number of precincts by $8,000, our estimate for per-precinct machine replacement cost, to arrive to our $300 million estimate.

provide voters with confidence they can trust the electronic totals provided on election night. Unfortunately, only 22 states that have paper records of every vote require post-election audits of those votes before certifying their elections.[7] This is only two more than did so in 2016.[8] Even in states where post-election audits are required, in most cases they could be far more robust. Currently, only two states, Colorado and Rhode Island, will require post-election risk-limiting audits (RLAs) in 2020 which provide "strong statistical evidence that the election outcome is right and ha[ve] a high probability of correcting a wrong outcome."[9]

Add Electronic Pollbooks to the Federal Certification Process

The existing testing and certification process put in place under the Help America Vote Act (HAVA) has significantly increased the quality and reliability of voting systems. However, over the past several years, the limitations of the current testing and certification program have become evident.

One of the biggest shortcomings has been the inability to regulate electronic pollbooks due to their lack of inclusion in HAVA. Electronic poll books (EPBs) are electronic versions of the voter rolls that are used to process voters at the polls instead of using paper-based lists. Use of EPBs

---

[7] These twenty-two states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Mexico, New York, North Carolina, Ohio, Oregon, Rhode Island, Utah, Washington, and West Virginia. Although Ohio conducts post-election audits after certification, the Election Board must amend its certification if the audit results in a change of the vote totals reported in the official canvass; See "POST-ELECTION AUDITS," National Conference of State Legislatures, last modified February, 1, 2019, http://www.ncsl.org/research/elections-and-campaigns/post-electionaudits635926066.aspx; Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall, *Election Security in All 50 States: Defending America's Elections*, Center for American Progress, February 12, 2018, https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.

[8] 17 R.I. Gen Laws §17-19-37.4 (2017); 2017 Iowa Acts 256.

[9] Jerome Lovato, "Defining and Piloting Risk-Limiting Audits," U.S. Election Assistance Commission, accessed May 6, 2019, https://www.eac.gov/defining-and-piloting-risk-limiting-audits-/.

has spread rapidly in the last decade, and at least 34 states as well as the District of Columbia currently use some form of EPBs to process voters at the polls.[10] One of the major benefits of EPBs is that they can make it easier to set up "vote centers" during early voting or on Election Day. Vote centers are "an alternative to traditional neighborhood-based precincts."[11] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing cost savings, and encouraging increased voter turnout.[12] If a county uses multiple vote centers, the electronic pollbooks can automatically sync up during the day to ensure that once someone has voted in a particular location, they cannot vote in another location on the same day.

Despite these advantages, EPBs also pose significant risks. Someone who gains unauthorized access to these pollbooks could delete names, mark individuals as felons prohibited from voting, mark individuals as having already voted, or change individuals' party affiliation to keep them from voting in a party primary.[13] Unlike voting machines, there are currently no national security standards for electronic pollbooks. Of the 34 states that have adopted them, only 13 have statewide procedures for certification requirements, or certify systems statewide, according to NCSL.[14]

HAVA's current structure limits EAC's ability to create requirements for, test, and certify EPBs in the same way they do for voting machines. The Brennan Center supports updating HAVA to allow the EAC to create a certification program for all electronic pollbooks, as they do for voting systems, in order to encourage secure EPB systems nationwide. These

---

[10] "VRM in the States: Electronic Poll-books," last modified February 6, 2017, Brennan Center for Justice, http://www.brennancenter.org/analysis/vrm-states-electronic-poll-books.
[11] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[12] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[13] Lawrence Norden and Ian Vandewalker, *Securing Elections From Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[14] "Electronic Poll Books," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

Conduct Penetration Testing and Nationwide Threat Assessments

In addition to including EPBs in the testing and certification process, the Brennan Center recommends creating an additional requirement of penetration testing for each EAC-vetted system. Penetration testing proactively identifies vulnerabilities in critical infrastructure, often by launching real-world attacks on the system. Once vulnerabilities are discovered, they are able to be addressed before malicious actors become aware of them.[15]

Periodic penetration testing of both new and existing EAC-vetted election systems should be made a routine part of the EAC certification process. This process could leverage the skills and expertise of technology companies and white hat hackers to find potential system vulnerabilities. This would ensure that our election systems are prepared to meet the challenge of defending against a landscape of new and changing cyber threats.

The Brennan Center also supports a requirement that the federal government conduct regular, nationwide threat assessments to help state and local governments understand where the vulnerabilities to cyberattack are. As cyber threats evolve, it is critical to conduct ongoing threat assessments of election infrastructure such as voter registration databases and voting systems. Conducting threat assessments on a regular basis would help state and local governments implement mitigation strategies where weaknesses are identified. In a 2017 Brennan Center report, *Securing*

---

[15] Meredith Berger, Charles Chretien, Caitlin Conley, Jordan D'Amato, Meredith Davis Tavera, Corinna Fehst, Josh Feinblum, Kunal Kothari, Alexander Krey, Richard Kuzma, Ryan Macias, Katherine Mansted, Henry Miller, Jennifer Nam, Zara Perumal, Jonathan Pevarnek, Anu Saha, Mike Specter and Sarah Starr, *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School and Defending Digital Democracy, 2018, 53, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

Elections from Foreign Interference, we noted a consensus among experts that many states were unlikely to have completed this kind of risk assessment in the last few years, even though the cost of completing a threat assessment was likely to be manageable. In the Commonwealth of Virginia, for example, Edgardo Cortés, former Commissioner of the Virginia Department of Elections and current Brennan Center Election Security Advisor, estimates that his department could have conducted a comprehensive threat assessment or audit for just $80,000 annually.[16]

Require Private Election System Vendors to Report Cybersecurity Incidents

Private companies are contracted to perform everything from building and maintaining election websites that help voters determine how to register and where they can vote, to printing and designing ballots, to programming voting machines before each election, to building and maintaining voter registration databases, voting machines, and electronic poll books. Congress should consider additional steps to protect our elections from attacks that target these private election system vendors. Unlike other sectors that the federal government has designated "critical infrastructure," there is currently almost no federal oversight of the private vendors who build our election systems. In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal elections infrastructure.[17]

The Brennan Center recommends that Congress adopt a mandatory reporting system for all cyber security incidents for election vendors. While this may seem like a small step, it will have a large impact on the overall security position of election officials around the country. Election vendors have stated that such requirements are unnecessary and burdensome, and that they are somehow different from vendors in other critical infrastructure sectors. This is simply not true. We know that the lack of transparency in vendor security is a significant vulnerability to election

[16] *Securing Elections From Foreign Interference*, Brennan Center for Justice.
[17] Compare, for example, 16 C.F.R. §§ 1500.14, 1500.48, 1500.83, 1700.14, with 11 CFR §§ 9405.1 et seq.

security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[18] In fact, reporting requirements for cyber security incidents are a bare minimum, and we should be considering additional requirements such as vendor employee background checks and other lessons learned from similar critical infrastructure sectors.[19] The Brennan Center has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[20]

Applying Cyber Security Framework to Election Systems

NIST is responsible for creating and maintaining the Cybersecurity Framework (CSF) which "consists of standards, guidelines, and practices to promote the protection of critical infrastructure."[21] The CSF assists industries, governments, and businesses in managing cybersecurity risks. In addition to the CSF, NIST creates implementation profiles that give voluntary guidance on how to adapt the CSF to particular critical infrastructure sectors. For instance, the CSF Manufacturing Profile "can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices."[22]

NIST should prioritize the development of a CSF Elections Profile. This would be done in collaboration with other federal partners like the EAC and DHS, state election officials, local election officials, and other entities

---

[18] *Securing Elections from Foreign Interference*, Brennan Center for Justice.
[19] Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, Roisin, *A Handbook for Elections Infrastructure Security*, Center for Internet Security, February 2018, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf.
[20] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.
[21] "New to Framework," Cybersecurity Framework, National Institute of Standards and Technology, updated April 23, 2019, https://www.nist.gov/cyberframework/new-framework#background.
[22] Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Joshua Lubell Jeffrey Cichonski, John McCarthy, *Cybersecurity Framework Manufacturing Profile*, National Institute of Standards and Technology, September 8, 2017, https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile.

involved in elections like election technology vendors. Implementing the Cybersecurity Framework can be a daunting task, and this profile would provide clear and direct guidance to election officials for how to best secure their systems. State and local election offices could use a CSF Elections Profile to guide prioritization of spending cyber security funds, including identifying deficiencies that need to be addressed to prevent foreign interference. This would require additional resources for NIST to develop and for the EAC to use its clearinghouse role to encourage state and local election officials to utilize the roadmap in their cybersecurity planning.

Ensuring Sufficient Funding to Protect State and Local Election Offices

Congress took an important first step in 2018 by allocating $380 million to states for election security activities. However, it is clear there is an ongoing need for federal funding to help protect our elections infrastructure from foreign threats. Congress should build on last year's efforts and provide additional funding to states to continue improving election security. Any funding should ensure that some of it is designated for use at the local level. In addition to funding for state and local election offices, Congress should ensure that federal agencies involved in this important work, including EAC, DHS, and NIST, have sufficient resources to carry out their mandates.

Conclusion

Election officials around the country need appropriate tools and resources to meet the on-going challenge of protecting our democracy from hostile nation states. We are encouraged by the great progress we have made in securing our elections since 2016, but our work in defending against cyber threats is far from complete. We urge you to consider legislative changes that will help tackle these problems head on. We appreciate this committee's leadership in continuing to strengthen our nation's election infrastructure.