MICILLINE FOR THE OFFICIAL RECORD

BRENNAN CENTER FOR JUSTICE

House Committee on the Judiciary
United States House of Representatives

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

"Securing America's Elections"

September 27, 2019

The Brennan Center thanks the House Committee on the Judiciary for holding this hearing on the critical issue of election security. The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to provide detailed information about election infrastructure vulnerabilities and important remedial policies and procedures we have identified in our extensive studies and efforts to ensure our nation's election systems are more secure and reliable in today's complex threat environment. We are deeply involved in the effort to ensure accurate and fair voting for all Americans.

Our country has made significant progress to secure our election infrastructure from cyber-attack since 2016.[1] Federal, state and local officials continue to implement fundamental systemic and infrastructure improvements.[2] Yet, significant security gaps

[1] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[2] Ibid; Election Security Hearing, Before the Comm. on House Administration, 116th Cong. (2019) (statement of Lawrence Norden) ("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. 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 85% of this money will be spent prior to the presidential election on such critical measures as strengthening election cybersecurity, purchasing new

remain, many on a patchwork basis across the country.[3] This landscape is largely the result of our decentralized electoral system. While this structure is a strength in many ways, as a nation, we are only as strong as our weakest link. Successful attacks against our infrastructure in any county in any state can have a ripple effect that impacts the balance of power at the federal level and the daily lives of American citizens.

Additional, and urgent, action is required to ensure that our country's election infrastructure is sufficiently resilient to withstand future attacks. In the testimony below, we identify five risks to our election infrastructure, as well as steps that can be taken to reduce their potential harm: (1) the continued use of paperless and antiquated voting systems; (2) the lack of a federal certification program for electronic pollbooks; (3) the rapid evolution of cyber threats; (4) the lack of federal oversight of election system vendors; (5) the limited resources of state and local election officials.

Too Many Jurisdictions Still Use Paperless and Antiquated Voting Systems. We Must Replace Them and Implement Robust Post-Election Audits.

Millions of voters will go to the polls to cast their ballot on Election Day 2020. They will encounter a variety of different voting machines at their polling place and we estimate at least some voters in as many as 38 states will cast their ballot on equipment that is more than 10 years old.[4] In November 2018, we estimate that 34 percent of all local election jurisdictions were using voting machines that were at least 10 years old as their primary polling place equipment (or as their primary tabulation equipment in all vote-by-mail jurisdictions)[5] and 20 years old in at least one state.[6]

These aging voting systems are a security risk and less reliable than voting equipment available today. Older systems are generally "more likely to fail and are increasingly

---

voting equipment, and improving post election audits, all essential steps in protecting our elections from foreign interference.")

[3] DHS National Risk Management Center, July 2018, https://www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-risk-management-fact-sheet.pdf.

[4] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary (41 states minus Alaska, California, and North Dakota).

[5] Ibid.

[6] "Proposed Recommendation Regarding Acquisition of a New Voting System," Alaska Election Policy Work Group, http://www.elections.alaska.gov/doc/info/180718%20DRAFT%20Proposition.pdf.

difficult to maintain."[7] Many are no longer manufactured so finding replacement parts will be increasingly difficult over time.[8] This problem exacerbates the reported system-specific security concerns with some widely used older systems, such as the AutoMARK, including inconsistent vote tallying and reboot times of 15 to 20 minutes.[9] Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.[10]

More troubling, we estimate that, absent additional federal assistance, at least some voters in 8 states (Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Tennessee and Texas) will cast their ballots on paperless voting systems in 2020.[11] Voter-marked paper ballots are a critical election security measure[12] and, in the event a virus or other malicious software is introduced into a voting machine, can be used to detect and recover from that attack.

Paper-based systems also provide better security because they create a paper record that voters can review before casting their ballot and election officials can audit after the

---

[7] *Election Security Hearing*, *Before the Comm. on House Administration*, 116th Cong. (2019) (statement of Lawrence Norden); Josie Bahnke (Elections Director, Office of the Lieutenant Governor, Alaska), Letter to Election Policy Work Group Members, July 18, 2018, http://www.elections.alaska.gov/doc/info/180718%20EPWG%20Research.pdf ("Today the DOE is at a critical juncture: Alaska's voting equipment and technology are outdated, difficult to repair and prone to failure").

[8] Lawrence Norden and Andrea Cordova, "Voting Machines at Risk: Where We Stand Today," *Brennan Center for Justice*, March 5, 2019, https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today.

[9] Ruth Johnson (Oakland County clerk/register of deeds), Letter to Rosemary Rodriguez (chairperson, Election Assistance Commission), October 2, 2008, https://www.eac.gov/assets/1/6/Oakland_County_Michigan_letter_regarding_ES_S_M-100_voting_machine_tabulators.pdf (stating that 8 percent of M-100 fleet in Oakland County "reported inconsistent vote totals during their logic and accuracy testing"); "Election Systems and Software (ES&S) AutoMARK," Verified Voting (listing AutoMARK security concerns), accessed May 4, 2019, https://www.verifiedvoting.org/resources/voting-equipment/%20ess/automark/.

[10] Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, Rachael Dean Wilson, *Defending Elections*, Brennan Center for Justice, 2019, https://www.brennancenter.org/sites/default/files/publications/2019_07_EACFunding%20Report_FINAL.pdf.

[11] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.

[12] *Securing the Vote*, The National Academies of Sciences, Engineering, and Medicine, 2018, https://www.nap.edu/read/25120/chapter/1; *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.

election. However, these paper records will be of little security value unless they are used to check and confirm electronic tallies of election results. In 2020, we estimate that only 24 states and the District of Columbia will have voter verifiable paper records for all votes cast and require post-election audits of those paper records before certifying election results.[13]

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

Encouragingly, multiple states have made significant progress in replacing their aging and paperless systems in recent years. Arkansas, Georgia, Pennsylvania and South Carolina have either completed the replacement of their paperless voting machines or are transitioning now.[14] Alaska, California, North Dakota and Ohio are currently working to replace their aging systems.[15] In addition, at least 12 states are experimenting with risk-limiting audits, the "gold-standard" of post-election audits.

There Are No Federal Security Guidelines for Electronic Pollbooks. They Should Be Included in the Federal Certification Process.

As of July 2019, 41 states and DC use or authorize the use of electronic pollbooks in at least some polling places.[16] Electronic pollbooks (EPBs) are laptops or tablets that poll workers use instead of paper lists to look up voters. Most EPBs can communicate with other EPBs in the same polling location to share real-time voter check-in updates.[17] In addition to an expedited check-in procedure, shorter lines, lower staffing needs, and cost savings, one major benefit 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

[13] Lawrence Norden and Andrea Cordova, "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary," *Brennan Center for Justice*, August 13, 2019, https://www.brennancenter.org/analysis/voting-machine-security-where-we-stand-six-months-new-hampshire-primary.
[14] Ibid.
[15] Ibid.
[16] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx; Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.
[17] Edgardo Cortés, Liz Howard, and Lawrence Norden, *Better Safe than Sorry: How Election Officials can Plan Ahead to Protect the Vote in the Face of a Cyberattack*, Brennan Center for Justice, 2018, https://www.brennancenter.org/sites/default/files/publications/2018_08_13_ElectionSecurity_V4.pdf.

neighborhood-based precincts."[18] Anyone in a particular jurisdiction can vote there, regardless of where they live, possibly making voting more convenient, providing additional cost savings, and encouraging increased voter turnout.[19] If a county uses multiple vote centers, the electronic pollbooks can automatically sync 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. In a worst-case scenario, hackers could alter or delete voter data, even causing voters to appear as if they have voted when they have not. EPBs that require access to the Internet can also pose problems in rural counties that lack reliable connectivity.[20] Unlike voting machines, there are currently no national security standards for electronic pollbooks. 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.

In the absence of federal certification standards, states have developed a patchwork system of e-pollbook regulation and certification. Only 12 states certify systems statewide, according to NCSL.[21] Many states using EPBs do not mandate important election security measures that can mitigate risks associated with EPB use in precincts. In 2018, when 34 states used EPBs, only half required printed backup paper pollbooks to be present in the polling place at the time voting began and, in 32 of the 34 states, we found no requirements in state law or regulation mandating a minimum number of provisional ballots.[22]

The Brennan Center supports updating the Help American Vote Act 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 additional responsibilities will require increased funding and staffing levels for the EAC to effectively test and certify EPBs.

---

[18] "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.
[19] Ibid.
[20] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.
[21] "Electronic Poll Books," National Conference of State Legislatures, July 15, 2019, http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.
[22] Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," *Brennan Center for Justice*, October 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper.

Cyberthreats Evolve and Change Over Time. It Is Critical to Conduct Penetration Testing and Nationwide Threat Assessments to Keep Up.

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 can be cured before malicious actors become aware of them.[23]

Penetration testing is a critical addition due to the limitations of the current federal certification process, which only ensures compliance with baseline security requirements created using information available before the time of certification. Unlike the static certification process, penetration testing protocols can be updated on an ongoing basis in response to the ever-evolving threat environment. 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 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

[23] 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.

could have conducted a comprehensive threat assessment or audit for just $80,000 annually.[24]

Election System Vendors Are Another Point of Vulnerability. They Should be Required 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 and to regulate vendor conduct. Unlike other sectors that the federal government has designated "critical infrastructure," there is currently almost no federal oversight of the private vendors who design, build and maintain 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.

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 security. Private vendors were targeted in the 2016 election and are likely to be targeted again.[25] 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.[26] The Brennan Center

[24] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[25] Lawrence Norden and Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, 2017, https://www.brennancenter.org/publication/securing-elections-foreign-interference.
[26] 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.

has documented some of the additional reasons for mandating such reporting in the 2010 report, *Voting System Failures: A Database Solution*.[27]

Election Officials Have Limited Resources. Congress Should Ensure That They Have Sufficient Funding to Protect Our Election Infrastructure.

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

With significant risks threatening our election infrastructure, effective risk mitigation measures and policies should be uniformly implemented to create a resilient election administration system. 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. 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 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.

[27] Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice, 2010, https://www.brennancenter.org/publication/voting-system-failures-database-solution.