BRENNAN CENTER FOR JUSTICE

Defending America's Election Infrastructure

Democracy in America is under serious threat. A bipartisan report from the Senate Intelligence Committee concluded that in 2016 all 50 states were likely targeted by Russian operatives seeking access to election infrastructure, at least one major election vendor was successfully breached, and that future attacks should be expected. Indeed, since 2016, we have seen continued cyberattacks against political campaigns tied to both Russia and Iran.

American elections are decentralized, with state and local election officials retaining primary authority for administering them. This means, among other things, that they bear considerable responsibility for defending our infrastructure against concerted attacks from sophisticated nation state actors. Fortunately, election officials take this duty seriously, and the federal government has recently provided some overdue assistance, in the form of minimal funding to improve election security and better coordination with agencies such as the Department of Homeland Security. Many states are in the process of replacing antiquated and paperless voting machines with more secure systems, while others have sought out risk assessments to identify security vulnerabilities in important infrastructure such as registration databases.

Much more can be done, however, to strengthen election security and increase public confidence in elections. Below, we detail our top policy recommendations for doing so.

Conduct Assessments and Testing

Discussions of election security often focus on individual aspects of election systems, such as voting machines or registration databases. While such focus is important, it is also critical to look at the election process as a whole, understand the interaction of election systems and personnel, and assess the vulnerabilities that exist in each facet that could be exploited by malicious actors looking to undermine elections. Below we detail steps the federal government could take to ensure more comprehensive security.

Conduct periodic state and nationwide threat assessments. As cyber threats evolve, it is essential to assess the security of our election infrastructure regularly, to understand where new vulnerabilities may crop up. Congress should provide resources for state and federal agencies to conduct regular threat assessments and help state and local governments implement mitigation strategies to address the identified weaknesses.

Establish a bug bounty program for election systems. Bug bounty programs provide a mechanism for independent security researchers to identify potential vulnerabilities and responsibly report them. This provides a legal method to actively search out vulnerabilities in election systems and financial incentives for appropriately reporting them. Disclosures through a bug bounty program would allow manufacturers the ability to fix the issue before the discovery is made public and allow election officials to appropriately plan mitigation strategies for existing vulnerabilities. Several federal agencies, including the Department of Defense, have established successful bug bounty programs in recent years as part of ongoing efforts to strengthen cyber security. Congress should authorize and provide funding for the Election Assistance Commission (EAC) to certify and monitor a broader range of election systems (explained more below), and create an additional requirement for establishing a bug bounty program for each of these EAC-vetted systems.

Develop a CSF Elections Profile. The National Institute of Standards and Technology (NIST) is responsible for creating and maintaining the Cybersecurity Framework (CSF), a set of standards, guidelines, and practices that help entities manage cybersecurity risks. Along with the CSF, NIST creates implementation profiles that give voluntary guidance on how to adapt these guidelines and practices to particular critical infrastructure sectors. Consistent with the recognition of election systems as critical infrastructure, NIST should prioritize the development of a CSF Elections Profile to provide clear and direct guidance to election officials on how to best secure their systems.

Secure Voting Equipment and Registration Databases

Even though election jurisdictions across the country have made significant progress in updating their election infrastructure since 2016, significant security gaps remain. But steps can be taken to reduce the likelihood of equipment failure, recover more quickly from failures when they do occur, and ensure that every legitimate voter has an opportunity to cast a ballot and have their vote counted. We recommend the following actions be taken to achieve these goals.

Require paper ballots. Paper ballots create a tangible record of a voter's choices that the voter can review, prior to casting the ballot, to ensure it accurately captures their intent. These records can then be used by election officials to discover any errors in the voting tabulation system, and ultimately ensure that total election results were recorded correctly. All voting systems should use paper ballots in order to make effective auditing and confirmation of results feasible.

Ban wireless components. Wireless components that permit connections to WiFi networks, cellular networks, or other devices, via Bluetooth or other protocol, pose an unnecessary risk of malware being implanted in this equipment, unbeknownst to election

administrators. Wireless components should be prohibited in voting systems that record and tabulate votes. Voting system components that do not tabulate votes should limit wireless connectivity only to instances necessary for accessibility.

Implement robust post-election audits. Replacing paperless voting machines is not enough on its own to ensure accurate election results—election officials must use these paper ballots to conduct rigorous and routine post-election audits that are designed to provide a high level of statistical confidence of the correct outcome. We recommend the regular use of risk-limiting audits. Risk-limiting audits provide confidence in election outcomes because they limit the risk that a voting system error or hack significant enough to affect the outcome of an election will go undiscovered. A sample of ballots is examined by hand and compared to the results recorded by the voting system to look for discrepancies. For contests with large reported margins of victory, a smaller sample is required to reduce the risk of error than for contests with small reported margins of victory. Therefore, risk-limiting audits can be performed on a regular basis, unlike costly full hand recounts.

Back up voter registration databases regularly. In the run-up to the 2016 elections, Russian agents sought to access election systems in many states, and successfully breached records in the voter registration database of at least one state. Such attacks on statewide voter registration databases present a serious risk of electoral disruption, as malicious actors could interfere with the ability of voters to cast ballots by deleting them from lists of registered voters, changing their recorded address, or changing party affiliation to keep them from voting in their party's primary. If backup registration lists are available, election officials should be able to quickly reconstruct accurate lists when improper changes are discovered. To ensure that no manipulation of a state registration database prevents legitimate voters from casting a ballot or having their votes counted, backup registration lists should be created regularly on removable media isolated from internet connections, as well as on paper.

Establish election day failsafes. Backup registration lists can allow election officials to reconstruct accurate lists, but that may not ensure eligible voters can cast ballots if the problems are discovered only after Election Day is over. An undetected change to the voter list could incorrectly show that a voter had already cast a ballot, or that she had recently moved. For this reason, election officials should also put in place failsafe measures to ensure that legitimate voters can still cast a ballot that will be counted, such as having sufficient numbers of provisional ballots at every polling place. In addition, states should adopt election day registration procedures that allow voters to register at their polling places if they are unregistered, improperly removed from the lists, or if there are other problems with their registration in the database.

Create a certification program for e-pollbooks. Under the Help America Vote Act (HAVA), the EAC is tasked with developing voluntary voting system guidelines (VVSG) that set standards for voting systems and certifying voting systems that meet these

standards. While participation in the certification program is voluntary under HAVA, many states have formally adopted the VVSG and require all voting systems used in the state to be certified by the EAC. But the VVSG and corresponding certification process is limited to voting systems upon which votes are cast and counted, failing to account for the numerous other systems that are necessary for the broader election process. The EAC's authority should be expanded to certify not just voting systems, but also e-pollbooks, in order to ensure that other components of election infrastructure are more secure, incorporating appropriate access controls, and providing backup and recovery mechanisms. Several proposed bills in Congress—including the Election Security Act, the SAFE Act, and the For the People Act—have recommended adding e-pollbooks to the voting system certification regime.

Regulate Election Vendors

Security measures in response to the attacks on America's elections in 2016 have largely focused on instituting best practices for state and local officials to prevent, detect, and recover from cyberattacks. Yet private vendors, not election officials, build and maintain much of our election infrastructure. These companies are involved at every stage of the election process—creating voter registration databases, programming ballots, providing electronic pollbooks and voting machines, building election night reporting websites, and checking equipment and procedures post-election. Despite this prevalent role, there is almost no federal regulation of private vendors in the election space. A forthcoming Brennan Center report will focus on this problem and propose a series of solutions, including the following:

Create a certification regime for election system vendors. While the EAC runs a federal certification system for voting machines, it does not certify vendors selling voting machine equipment or vendors that provide other election services. There is no federal oversight to ensure that private vendors have properly screened employees who may program voting machines and conduct other sensitive functions, or have engaged in the best supply chain management and cybersecurity practices when manufacturing and replacing their equipment. We need a federal certification program so that election officials and the public can have greater confidence in the companies that provide critical election products and services, and to engage in routine monitoring of such vendors to ensure ongoing compliance. The For the People Act and the SAFE Act have both proposed these kind of programs.

Require vendors to report cyber incidents. Both the public and government officials are often in the dark about security incidents affecting election vendors. This state of affairs can undermine faith in the vote and leave election officials unsure about vendor vulnerabilities. To address these concerns, Congress should require election vendors to report cyber incidents to all relevant election authorities. Recent bills in Congress have

proposed similar mandatory reporting requirements, including the Secure Elections Act and the Election Vendor Security Act.

Centralize Information

While the EAC has taken significant steps in recent years to improve information sharing among election officials when problems with voting systems occur, we believe more can be done to ensure that state and local officials can address system vulnerabilities and prevent the same problems from occurring in multiple jurisdictions. Because of this, we recommend that the federal government take a greater role in monitoring voting system failures and promoting the spread of information across the country.

Create a national database of voting system failures. The establishment of a new, national information hub is needed to ensure that voting system defects are caught early, disclosed immediately, and corrected quickly and comprehensively. Specifically, the nation needs a publicly available, searchable online database that includes data about voting system failures and defects discovered across the country. Such a database could be used to prevent the same system failures from occurring in multiple jurisdictions across many years, and would assist election officials as they look to purchase new voting machines with critical information about system performance.

Provide Long Term Support and Funding

A lack of financial resources presents the most significant obstacle to election security improvements in local jurisdictions. Congress took an important first step in 2018 by allocating $380 million to states for election security activities, and there are promising signs of more funding coming in 2019. But these one-time investments are not enough to address the significant problems facing election systems or provide long-term stability for future election security planning. It is clear there is an ongoing need for federal funding to help protect our election infrastructure from foreign threats. Accordingly, we recommend that Congress take the lead to ensure that all levels of government provide sufficient long-term funding for election security and invest in innovative approaches toward making elections more secure, accessible, and efficient.

Provide robust, consistent funding for election resources. Because the threats to election security evolve over time, effective election security requires an ongoing commitment of resources, as opposed to a one-time expenditure. Companies in the private sector have departments and budgets dedicated to security generally, and often to cybersecurity specifically, precisely for this reason. Congress should provide a steady stream of funding for the periodic replacement of outdated voting systems, upgrading of database and other election infrastructure, and the purchasing of ongoing technical and security support for all these systems. But federal funding alone is not enough—state and

local governments should make election security a budget priority and develop long-term plans to fund regular equipment upgrades, training, and cybersecurity staff to assist local officials.

The Brennan Center has estimated the nationwide five-year cost for several critical election security items to be approximately $2.2 billion. This total includes:

- Providing additional state and local election cybersecurity assistance
- Upgrading or replacing statewide voter registration systems
- Replacing aging and paperless voting machines
- Implementing rigorous post-election audits

Establish an innovation fund. Congress should establish an innovation fund for the purpose of promoting advancements in the security, accessibility, and efficiency of elections. This fund would award grants on a competitive basis to entities for research and development in election modernization. The Election Security Act, which is currently pending before Congress, would provide for such a fund.

Make the "critical infrastructure" designation for election systems permanent. The federal government has provided important election security support to state and local governments through its "critical infrastructure" designation for election systems, adopted by the Department of Homeland Security in January 2017. However, this designation could be withdrawn by the executive branch at any time. Congress should make the critical infrastructure designation permanent though legislation to guarantee states are provided with priority access to tools and resources available from DHS and greater access to information on cyber vulnerabilities.

Adequately fund the EAC. In recent years, despite the increased threat of cyberattacks against our nation's election infrastructure, funding for the Election Assistance Commission -- the federal agency charged with adopting election security guidance and certifying voting systems -- has dropped sharply. The agency's budget in fiscal year 2019 was just $9.2 million, slightly more than half the funding it received in fiscal year 2010. Congress should ensure this agency has the resources, staff and leadership it needs to properly perform its critical election security functions.