



# Defending Elections

## Federal Funding Needs for State Election Security

**Christopher R. Deluzio**, Policy Director, University of Pittsburgh Institute for Cyber Law, Policy, and Security

**Liz Howard**, Counsel, Brennan Center for Justice

**Paul Rosenzweig**, Senior Fellow, R Street Institute

**David Salvo**, Deputy Director, Alliance for Securing Democracy

**Rachael Dean Wilson**, Head of External Affairs, Alliance for Securing Democracy

PUBLISHED JULY 18, 2019

## Introduction

---

State and local election officials are on the front lines of a cyberwar with sophisticated nation-state rivals and other malevolent actors. As Robert Brehm, co-executive director of the New York State Board of Elections, recently put it, “It is not reasonable” to expect each of these state and local election offices to independently “defend against hostile nation-state actors.”<sup>1</sup> State and local election systems have already been breached. In 2016 Russian hackers penetrated computer networks in two counties in the swing state of Florida, using information they had gleaned from a software vendor.<sup>2</sup> That same software vendor may have opened a gap for hackers to alter the voter rolls in North Carolina, another swing state, on the eve of the election.<sup>3</sup> Episodes like these undermine faith in our democratic system, and steps must be taken to prevent them from occurring again.

Critically, in 2018 Congress provided \$380 million in Help America Vote Act (HAVA) grant funds to help states bolster their election security. Grant recipient states had to submit a grant narrative—a list of specific election security projects (and estimated costs) that the state planned to fund with grant money—and provide a 5 percent state match within two years. Based on information that the states submitted to the Elections Assistance Commission (EAC) as part of the grant process, recipients are using the vast majority of this money to strengthen election cybersecurity, purchase new voting equipment, and improve postelection audits — all pressing needs around which there is broad bipartisan consensus.<sup>4</sup> The EAC has estimated that 85 percent of the money Congress has provided will be spent ahead of the 2020 election.<sup>5</sup>

Unfortunately, given the myriad security challenges

faced by these states, the \$380 million is not enough to address the needs of state and local offices; many have substantial election security needs that likely will not be met absent additional federal support.

This paper examines six key states (Alabama, Arizona, Illinois, Louisiana, Oklahoma, and Pennsylvania) that represent different regions of the country, varied population sizes, and the full range of election security needs. It investigates how they have allocated their share of the

2018 federal election security grants and documents their needs for additional election security funding. States' use of HAVA funds is tailored to their specific requirements and reflects the nature of the state and local governments that oversee elections. Likewise, their unfunded election security needs vary according to state-specific circumstances. While the authors have limited their review to a sampling of six states, it is clear that the other 44 states and the District of Columbia have similar unfunded needs.<sup>6</sup>

## State Spotlights

---

### Alabama

In the wake of unsuccessful cyberattacks against the state voter registration database in 2016, Alabama Secretary of State John Merrill stated, "While it is encouraging that our efforts to protect Alabamians' data have proven to be successful, we must remain vigilant and prepared for the constantly evolving threats to our voting systems and the integrity of those processes. We will utilize every resource available to ensure we are protecting the data of all Alabamians."<sup>7</sup>

As part of these ongoing efforts, Secretary Merrill has welcomed public and private election security partners, such as the U.S. Department of Homeland Security (DHS), into Alabama, taking advantage of a wide range of free resources available to further improve Alabama's election security risk posture.<sup>8</sup> These partnerships are critical to many states that are, in Merrill's words, "not rich when it comes to resources that are available for discretionary purposes or specifically [election security]."<sup>9</sup>

While these partners can help identify vulnerabilities, best practices, and important support functions, they do not fund the personnel, training, and security measures necessary to secure vulnerabilities in Alabama's election system. For these reasons, Secretary Merrill supports federal block grants for funding specific election security projects in the states and believes such grants "would be very helpful" to Alabamians.<sup>10</sup>

#### Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$6,160,383

**State match:** \$308,020

**Total:** \$6,468,413

Alabama has designated the entirety of its federal election security grant and state matching funds toward the following four projects:<sup>11</sup>

- **Voter registration database upgrades and maintenance.** With "more voters registered and more ballots being cast than ever before,"<sup>12</sup> the state is devoting \$3 million to improve the voter registration database and its security features through upgrades, such as two-factor authentication (2FA), to ensure that voter data is secure and reliable.
- **Computer equipment replacement and upgrades.** The state is providing new computers and related equipment to each of the five primary election officials in all 67 counties at an estimated cost of \$300,000. Alabama officials expect to complete this project by September 30, 2019.<sup>13</sup> One of the many cybersecurity challenges faced in Alabama and several other states is related to the security practices of the users of a shared system, such as a statewide voter registration database. By providing computer equipment directly to local officials, the state can ensure that users across the state are implementing basic cybersecurity measures, including antivirus software installation.
- **Postelection audits.** The state designated \$800,000 for postelection audits. This process is an essential election security bookend to the critical election measure already in place, paper ballots. While many of the audit-related costs will be incurred at the local level, the state plans to assume or reimburse all costs associated with implementing robust postelection audits, as local election officials simply don't have the funds to underwrite this project.<sup>14</sup> The state is currently working with election security experts to determine the best options for Alabama, and the first pilots are expected to be scheduled in calendar year 2019.<sup>15</sup>
- **Addressing cyber vulnerabilities.** The state designated \$2.3 million for various cybersecurity

enhancements, improvements, and fixes. Working with a variety of partners, the state plans to “investigate, implement, and identify new technologies” to help reduce or eliminate cyber vulnerabilities. As an example, the state previously fixed an official state elections website vulnerability that had been publicly identified by a private cybersecurity firm.<sup>16</sup>

### Additional Unfunded Security Needs

Alabama election officials identified two unfunded election security projects: legacy voting equipment replacement and development of a “cyber navigator program.”<sup>17, 18</sup>

**Legacy voting equipment replacement.** Alabama election officials in every county except Montgomery use legacy voting systems that are more than a decade old, including AutoMARK voting systems, used in 66 counties, and M100s (precinct count optical scanners), used in seven counties.<sup>19</sup>

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 difficult to maintain.”<sup>20</sup> Specifically, as neither the AutoMARK nor the M100 is currently manufactured, finding replacement parts will be increasingly difficult over time.<sup>21</sup> This problem exacerbates the system-specific security concerns that have been reported to the EAC or by Verified Voting, such as inconsistent vote tallying and reboot times of 15 to 20 minutes.<sup>22</sup> Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.<sup>23</sup>

State and local election officials would consider using additional election security funding to replace these legacy systems.<sup>24</sup> Bullock County Court of Probate Judge James Tatum, the local chief election official, explained, “Our [AutoMARKs] are old and becoming very difficult to maintain . . . I would like to have the most secure equipment, cyber training, and election security [tools], but we simply can’t afford it.”

Judge Tatum further explained that although “Secretary Merrill is a champion of rural counties,” they often must do without the tools and resources available in wealthy counties. “While Huntsville and Birmingham can afford these [replacement] costs, when you’re talking about rural counties, we simply can’t afford these costs no matter how much they would improve our election security. For example, we would be responsible for paying for training. Of course, we have to compensate our poll workers for their time when they come to training. We can’t afford it. Rural counties are all in need of some additional resources.”

**Development of a “cyber navigator program.”** Election officials would like a state program that provides election security and cybersecurity professional services to local election officials.<sup>25</sup>

Illinois recently developed such a system, where cyber navigators with responsibility for geographic zones will work across the state with local election officials to train relevant personnel and lead risk assessments and evaluations, among other things. They will fill a role akin in many ways to that of a chief information security officer for counties. Their assessment and evaluation efforts will help officials identify vulnerabilities and determine where additional resources may be needed to shore up cyber defenses. The program’s other principal components are infrastructure improvement and information sharing.<sup>26</sup>

Without a state resource for cyber assistance, local election officials, such as those in Bullock County who do not have dedicated IT staff, may be at greater risk of a successful cyberattack. Local election officials consider the state a trusted partner and know personnel are available to address all voting equipment technical questions.<sup>27</sup> However, without a cyber navigator-type of program, local election officials may not have sufficient resources to appropriately respond to identified cyber threats to local systems or equipment, such as those risks shared by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

## Arizona

After obtaining stolen log-in credentials of a local election official, cybercriminals attempted to gain access to Arizona’s voter registration database in 2016.<sup>28</sup> Subsequently, state election officials initiated the procurement process for a new, more secure database. They also established private and public partnerships to help identify system vulnerabilities and appropriate steps to mitigate them.

For several reasons, including the decentralized nature of Arizona’s election administration system, state election officials believe that supporting local election officials’ election and cybersecurity improvement projects is a critical component of their efforts to improve election security across the state.<sup>29</sup> While the 2018 grant provides necessary funding for foundational election security projects, some of which will directly benefit local officials, it is simply not enough to also pay for projects that would provide or subsidize cyber services and more secure voting equipment to local election officials.<sup>30</sup>

### Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$7,463,675

**State match:** \$373,184

**Total:** \$7,836,859

Arizona has designated the entirety of its federal elec-

tion security grant and state matching funds toward the following projects:<sup>31</sup>

- **Voter registration database replacement.** The former Arizona secretary of state, Michele Reagan, explained the importance of this project, stating, “When our online database was created, cybersecurity was an afterthought. Now, faced with international threats, we must have a system that implements strong protections and the highest level of security capabilities to protect voter data.”<sup>32</sup> While the total cost of replacing the aging database is estimated at \$7 million to \$10 million, the state has devoted approximately \$2.8 million to the project.<sup>33</sup>
- **Cybersecurity.** The state designated the remaining grant funds, approximately \$5 million, to various cybersecurity projects, including:
  - **Security assessment.** The state partnered with a private vendor to conduct an assessment of the “current IT infrastructure, focusing on critical election systems.” The state expected this assessment to “provide a framework for future spending.” The vendor’s public report was released in late 2018.
  - **Information sharing.** The state is partnering with local election officials to create stable communication channels and build a culture of support between the state and local election officials through routine meetings with interactive cybersecurity discussion topics and curated agendas.
  - **Cybersecurity subgrants to local election officials.** Working in conjunction with local election officials, the state plans to distribute a portion of its federal grant directly to counties to fund mutually agreed-on cyber projects.

### Additional Unfunded Security Needs

Election officials in Arizona noted they do not currently have funds they need to expand cybersecurity assistance to local election officials or replace legacy voting systems.<sup>34</sup>

**Greater cybersecurity assistance to local election officials.** Assisting local election officials with the cybersecurity challenges they face is an important priority for Secretary of State Katie Hobbs.<sup>35</sup> The secretary of state’s chief information officer, Bill Maaske, stated that if Congress provides additional election security funding for the states, then he would support using those funds to implement a state cyber navigator program,

which, as described below, would coordinate cybersecurity resources, information, and trainings for and with local election officials.<sup>36</sup>

Such a state program could provide essential services to local election officials, some of whom lack dedicated IT staff and may be at a greater risk of successful cyberattack. Without a cyber navigator–type of program, these local election officials may not have sufficient resources to appropriately respond to identified cyber threats to local systems or equipment, such as those shared by EI-ISAC.

**Legacy voting system replacement.** Arizona’s legacy voting systems represent a security and availability risk for three main reasons. First, “older systems are more likely to fail and are increasingly difficult to maintain.”<sup>37</sup> Aging voting systems often use outdated hardware, and many of them, including the AccuVote TSX and AVC Edge systems used in multiple Arizona counties, are no longer manufactured.<sup>38, 39, 40</sup> This can make finding replacement parts difficult, if not impossible. Second, aging systems also frequently rely on outdated software, like Windows XP and 2000, which may not receive regular security patches and are therefore more vulnerable to the latest methods of cyberattack. Third, “older systems are less likely to have the kind of security features we expect of voting machines today.”<sup>41</sup>

State election officials estimate the cost to replace the legacy voting equipment in use across the state, including the direct recording electronic (DRE) machines, to be \$40 million.<sup>42</sup> While relatively wealthy and urban counties, like Maricopa County, may be able to fund the purchase of new voting equipment without financial support from the state, Arizona’s more rural counties will likely struggle to find sufficient local resources.<sup>43, 44</sup> Considering this, if Congress allocates additional state election security funding, then state election officials can prioritize assisting counties with new voting system procurement costs.<sup>45</sup>

## Illinois

Former special counsel Robert Mueller’s report on Russian election interference included a troubling finding about Illinois: Russian operatives “compromised the computer network of the Illinois State Board of Elections . . . [,] then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.”<sup>46</sup> Although there is no single panacea to address such threats, the state is devoting a substantial portion of its federal election security funds to a cyber navigator program, which should help identify and address cybersecurity vulnerabilities like those the Russians exploited in 2016.

## Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$13,232,290

**State match:** \$661,615

**Total:** \$13,893,905

Illinois is using all of its federal election security funds to improve its cybersecurity. The hallmark of that effort is the state's cyber navigator program; the state plans to devote at least half of its federal grant toward this program.

Cyber navigators with responsibility for geographic zones across the state will work with local election officials to train relevant personnel and to lead risk assessments and evaluations, among other things. They will fill a role akin in many ways to that of a chief information security officer for counties. Their assessment and evaluation efforts will help officials identify vulnerabilities and determine where additional resources may be needed to shore up cyber defenses. The program's other principal components are infrastructure improvement, through the Illinois Century Network Expansion, and information sharing, through the Cybersecurity Information Sharing Program.<sup>47</sup>

### Additional Unfunded Security Needs

Election officials noted two unfunded election security projects: adoption of countermeasures for security vulnerabilities identified through risk and vulnerability assessments, and legacy voting system replacement.<sup>48</sup>

The cyber navigator program will help Illinois officials identify potential vulnerabilities in election systems and concrete actions to correct those weaknesses. However, as Noah Praetz, the former elections director of Cook County, explained, counties will likely need additional funds to correct any issues that arise during assessments: "The cyber navigators will be a great resource for counties and will go a long way toward helping officials across Illinois improve their cybersecurity. But we'll likely need continued funding support to address any vulnerabilities that the Navigators identify and to carry the cyber navigator program forward after its first few years."<sup>49</sup>

More immediately, Matt Dietrich of the State Board of Elections explained that Illinois needs significant additional funding to undertake a statewide replacement of its aging voting systems. He estimated the likely cost to be \$175 million. "Many of our local jurisdictions used the [original] HAVA grants to modernize their outdated voting systems. But those systems are now 15 years old and in need of replacement."<sup>50</sup> As explained above, such aging systems were not designed to withstand today's threats and can be more prone to equipment and software issues that could affect performance during voting.

## Louisiana

As one of only three states that continue to use paperless voting machines statewide, Louisiana lacks one of the most critical election security measure available today: voter-verifiable paper backups of every vote. Despite warnings by Department of Homeland Security (DHS) officials, cybersecurity experts, and the former Louisiana secretary of state, these paperless machines will likely be used in the upcoming 2019 general election for governor, attorney general, four other statewide elected positions, and all 144 members of the Louisiana Legislature.<sup>51,52</sup>

The ongoing effort by state election officials to replace the paperless voting machines in order to make election results verifiable has faced many setbacks, including bid protests, administration changes, and state budget woes.<sup>53</sup> Most recently, the process to purchase new, paper-based voting machines failed in October 2018 after a bid protest was filed. With this process stalled, state election officials plan to spend \$2 million to rent reliable voting equipment for early voting for the 2019 election.<sup>54</sup> Although Secretary of State Kyle Ardoin wants to get new voting machines "as soon as possible to continue to keep Louisiana at the forefront of election integrity and security," the timeline for replacing the voting machines is somewhat unclear.<sup>55</sup>

### Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$5,889,487

**State match:** \$294,474

**Total:** \$6,183,961

Given the pressing need to replace the state's paperless voting machines, Louisiana officials have allocated the entirety of the state's federal election security grant toward the purchase of new voting systems. However, those funds are insufficient to cover the cost of replacing paperless machines statewide. The original contract awarded for new voting equipment, since rescinded, was \$95 million.<sup>56</sup> Although state officials believe that the ultimate contract price for new voting machines will be lower, federal grant funds may cover less than 10 percent of total costs associated with obtaining and deploying a new, paper-based voting machine fleet across the state.<sup>57,58</sup>

### Additional Unfunded Security Needs

Louisiana has set aside all of its federal money to pay for much-needed new voting machines with paper backups. Even with this funding, **it still faces a multimillion dollar gap to replace its voting machines.** In addition, it has other security needs that have gone unaddressed,

including:

- **Post-election audits.** If paper-based voting systems are deployed across the state, then the essential election security bookend to the use of paper ballots – robust postelection audits to ensure that the ballots were counted as cast – can be implemented.
- **Addressing identified cyber vulnerabilities.** Cyber vulnerabilities are identified on an ongoing basis by the secretary of state’s information technology department.<sup>59</sup> They also may be identified periodically through independent Risk and Vulnerability Assessments available from DHS. Resources may be required to address cyber vulnerabilities discovered during these processes.

## Oklahoma

Although Oklahoma deployed a new statewide fleet of voting equipment in 2012, the state still faces many difficult election security decisions. Recent financial constraints have severely limited officials’ discretionary spending as Oklahoma slowly recovers from one of the most debilitating financial crises in the state’s history. Eight months into the past fiscal year, Oklahoma was forced to reduce state agency budgets, resulting in a \$50,000 cut in funding to the Oklahoma State Board of Elections.<sup>60</sup> The year ended in June 2019 with a \$167 million projected shortfall, and this was considered an improvement. One state official noted, “Last year [FY 2018], our shortfall was around \$800 million. I believe the year before was about \$1.3 billion, so we’re improving.”<sup>61</sup>

### Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$5,196,017

**State match:** \$259,801

**Total:** \$5,455,818

As of July 2018, Oklahoma planned to devote the entirety of its federal grant funds to the following four critical election security projects:<sup>62</sup>

- **Voter registration database upgrades and security enhancements.** The current custom-built state voter registration database relies on architecture designed in 2005 that can be installed only on Windows PCs. Oklahoma plans to spend \$1.65 million on the most critical security and system updates and upgrades.

- **Cybersecurity and physical security improvements.** Working with state and federal partners, election officials have identified multiple discrete projects, such as the relocation of their servers to a secure server bunker, implementation of two-factor authentication for access to the state Virtual Private Network (VPN), and remote antivirus protection management. The aggregate estimated cost of these projects is \$1 million.
- **Training.** The state estimates that developing and providing training for local election officials on the new equipment described above and additional cybersecurity trainings will cost approximately \$300,000.
- **New election system equipment.** The state plans to use \$2.5 million to purchase electronic poll books, which officials say can enhance election security through built-in security features, such as automated notifications in the event of unusual activity, e.g., the addition or deletion of a high number of voter records, by one or more users.<sup>63</sup> The state also plans to purchase document scanners to reduce the need to store hard copies of documents that contain personal private information and to protect against theft and loss of information through accidents and disasters.<sup>64</sup>

### Additional Unfunded Security Needs

According to State Election Board Secretary Paul Ziriach, Oklahoma Cyber Command and the Department of Homeland Security (DHS) may recommend new election security projects that should be given higher priority than those currently planned.<sup>65</sup> These partner agencies routinely provide services that identify cyber vulnerabilities and significant system risks and have been working with the Election Board to explore options “to optimize the board’s physical and cybersecurity and plan for potential election emergency situations.”<sup>66</sup>

If this process leads to recommendations of new election security measures, then Oklahoma would likely revise the current grant narrative to include them, Ziriach stated.<sup>67</sup> If officials designate federal funding for these new projects, then they must reduce the amount of federal funds currently designated for one or more of the projects described above. Depending on the costs associated with the new projects, officials may be forced to delay, partially defund, or abandon currently planned election security projects.

Regardless of the outcome of these assessments, Oklahoma has several additional election security needs, some of which have already been identified by election officials, that are not currently designated for federal funding, including:

- **Robust postelection audits.** Oklahoma is one of only 10 states with no postelection audit process.<sup>68</sup> Robust postelection audits ensure that the ballots were counted as cast and are an essential election security bookend to the state’s use of paper ballots for all elections.
- **Voting equipment hardware and software updates.** Although Oklahoma’s fleet of paper-based voting equipment is relatively new compared with that of several other states, it is already at the approximate “halfway mark of its life span,” and state officials “anticipate that the system may require hardware and/or software updates.”<sup>69</sup> If such updates become necessary for proper voting system fleet maintenance, then officials plan to revise the grant narrative and use federal funds for this project.<sup>70</sup>
- **Virtual Private Network (VPN) upgrades.** Oklahoma election officials are exploring options to upgrade the VPN provided by the Oklahoma State Regents for Higher Education to enhance security and protection of the state voter registration database.<sup>71</sup> This database houses the personal identifying information of more than 2.1 million registered voters in Oklahoma.<sup>72</sup>

## Pennsylvania

Pennsylvania’s election security challenges are substantial: As recently as the 2018 midterm elections, more than 80 percent of Pennsylvania voters were registered in jurisdictions still using paperless voting systems.<sup>73</sup> Yet Pennsylvania officials have taken steps to move away from these vulnerable machines. Those efforts include the Pennsylvania Department of State directing counties to have paper-based systems in place by 2020.<sup>74</sup>

### Allocation of 2018 Federal Election Security Funds

**Federal grant:** \$13,476,156  
**State match:** \$673,808

**Total:** \$14,149,964

Given the pressing need to replace the state’s paperless voting machines, Pennsylvania officials have allocated the entirety of the state’s federal election security grant to the purchase of new voting systems. The state is sharing these funds with counties in the form of a partial reimbursement once they have selected new voting systems, with each county receiving a share proportionate to its

number of registered voters. According to the Department of State, the counties have made great strides toward accomplishing the state’s goal of having new paper-based machines in place across Pennsylvania by 2020, and acting Secretary of the Commonwealth Kathy Boockvar expressed confidence in the state’s ability to meet that timeline.<sup>75</sup>

Unfortunately, those funds (approximately \$14 million with the state match added) are insufficient to cover the cost of replacing paperless machines statewide. The Pennsylvania Department of State estimates that federal funds will cover only 10 to 12 percent of the statewide bill to replace existing machines (approximately \$150 million).<sup>76</sup> In Lehigh County, for example, Tim Benyo, the county’s chief clerk for elections and registration, stated that federal funds will cover only a small portion of the county’s planned spending to procure a new paper-based voting system: roughly \$350,000 of the \$3.5 million that the county had budgeted for upgrades.<sup>77</sup> Zane Swanger, Mifflin County’s director of elections and voter registration, similarly said that federal funds will cover only \$41,000 of a likely \$250,000–\$300,000 total bill for the predominantly rural county’s purchase of a new voting system.<sup>78</sup>

### Additional Unfunded Security Needs

Setting aside the **ongoing funding gap for new voting systems with paper backups**, the urgent need to replace the state’s legacy voting machines has deprived Pennsylvania of the ability to direct federal funds toward other critical election security needs. Examples include:

- **Voter registration system.** The state is embarking on a procurement process to replace its aging statewide voter registration system, which is into its second decade of use. Pennsylvania’s state officials “have regularly maintained and updated its operating system,” but as Benyo explained, “The system is really outdated, and it has gotten Band-Aid after Band-Aid and requires a lot of money to keep it working properly.”<sup>79, 80</sup> Department of State leadership stated that although they remain confident in the security of the current system thanks to multilayered security protections in place, the “voter registration system replacement is absolutely about security,” as well as improving its performance and efficiency.<sup>81</sup> Not only is the current system expensive to maintain, but officials often confront performance costs when weighing security enhancements to the system.
- **Cybersecurity assessments.** County officials also expressed interest in regular, robust county cybersecurity assessments, which can be critical to identifying vulnerabilities and shoring up cyber defenses.

Although DHS has put Pennsylvania through its Risk and Vulnerability Assessment process and the Pennsylvania National Guard has been offering some cybersecurity assessment services to counties, counties tend to lack dedicated funding for regular, periodic assessments. The Department of State mentioned the Center for Internet Security's "Albert" sensors and annual costs, in particular, as something that additional funding could support for counties.<sup>82</sup>

## Conclusion

---

**In administering our elections, states face security challenges of unprecedented magnitude.** They are, in many cases, ill equipped to defend themselves against the sophisticated, well-resourced intelligence agencies of foreign governments. States should not be expected to defend against such attacks alone. Our federal government should work to provide the states with the resources they need to harden their infrastructure against cybersecurity threats. At the very least, each state should develop the ability to verify election results in the case of a breach.

Russia and other malign foreign actors use multiple tools and tactics to interfere in democracies, and cyber

- **Cybersecurity trainings.** There was also interest in cybersecurity training, which can help elections personnel guard against spear-phishing attacks and learn other basics of cybersecurity. Noting that the threat "environment is ever changing," Zane Swanger emphasized the importance of training his staff, poll workers, and others involved in election administration about current security threats and "better election material handling."<sup>83</sup>

threats against election systems are among them. The states included in this study have begun the hard work of upgrading dated infrastructure, setting aside funds for postelection audits, and addressing cyber vulnerabilities. But there is more they can do with additional resources.

Elections are the pillar of American democracy, and, as we saw in 2016 and 2018, foreign governments will continue to target them. States cannot counter these adversaries alone, nor should they have to. But at a time when free and fair elections are increasingly under attack, they can, with additional federal funding, safeguard them.

## Endnotes

---

- 1 Robert A. Brehm, co-executive director, New York State Board of Elections, interview by Brennan Center for Justice, May 6, 2019.
- 2 Pam Fessler, "Mueller Report Raises New Questions About Russia's Hacking Targets in 2016," *NPR*, April 19, 2019, <https://www.npr.org/2019/04/19/714890832/mueller-report-raises-new-questions-about-russias-hacking-targets-in-2016>; Lee Ferran, "Voter Databases in 2 Florida Counties Hacked in 2016, Governor Says," *ABC News*, May 15, 2019, <https://abcnews.go.com/Politics/voter-databases-florida-counties-hacked-2016-governor/story?id=63052842>.
- 3 Kim Zetter, "Software Vendor May Have Opened a Gap for Hackers in 2016 Swing State," *Politico*, June 5, 2019, <https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582>.
- 4 U.S. Election Assistance Commission, *Grant Expenditure Report, Fiscal Year 2018*, April 4, 2019, <https://www.eac.gov/assets/1/6/FY-2018HAVAGrantsExpenditureReport.pdf>.
- 5 *Oversight of the U.S. Election Assistance Commission Hearing, Before the Sen. Comm. on Rules and Administration*, 116th Cong. (2019) (statement of Christy McCormick, Chair, U.S. Election Assistance Commission).
- 6 National Association of Secretaries of State, "NASS Interim Position on Potential Federal Election Funding," <https://www.nass.org/node/1556> ("The emergence of cyber threats to election systems require[s] resources state and local governments may not sustain alone. Election security is equated with national security. Common nationwide threats justify federal assistance in funding individual state efforts to prevent and defend against cyber threats"); *Election*

- Security Hearing, Before the Comm. on House Administration*, 116th Cong. (2019) (statement of Lawrence Norden, director of election reform, Brennan Center for Justice) (documenting, among other things, that 28 states do not yet conduct post election audits of all votes before election certification, 40 states use at least some voting equipment over 10 years old, 41 states rely on voter registration databases created at least a decade ago, and 11 states continue to use paperless electronic machines as the primary polling place equipment in at least some counties).
- 7 Callum Borchers, "What We Know About the 21 States Targeted by Russian Hackers," *Washington Post*, September 23, 2017, [https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?noredirect=on&utm\\_term=.058ac930e61e](https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?noredirect=on&utm_term=.058ac930e61e).
  - 8 John Merrill, Alabama Secretary of State, "Panel 1, Investing in Security — Best Practices" (remarks, U.S. Election Assistance Commission 2018 Election Readiness Summit, October 3, 2018), <https://www.eac.gov/videos/opening-remarks-and-panel-1-investing-in-security-best-practices/>; *Election Security Hearing, Before the Comm. on House Administration*, 116th Cong. (2019) (statement of John Merrill, Alabama Secretary of State).
  - 9 John Merrill, "Panel 1, Investing in Security."
  - 10 *Election Security Hearing* (statement of John Merrill).
  - 11 State of Alabama, "2018 Help America Vote Act (HAVA) Election Security Grant Program Narrative, State of Alabama, Secretary of State," accessed June 5, 2019, [https://www.eac.gov/havadocuments/AL\\_Narrative\\_Budget.pdf](https://www.eac.gov/havadocuments/AL_Narrative_Budget.pdf).

- 12** Andrew J. Yawn, "E-lection Day? Why Online Voting Is Not an Option," *Montgomery Advertiser*, November 12, 2018, <https://www.montgomeryadvertiser.com/story/news/politics/2018/11/02/online-voting-unite-states-voter-turnout-alabama-estonia/1860186002/>.
- 13** John Merrill, "Panel 1, Investing in Security."
- 14** Clay Helms (election director, Alabama Secretary of State) and John Bennett (deputy chief of staff, Alabama Secretary of State), interview by Brennan Center for Justice, May 9, 2019.
- 15** Ibid.
- 16** Clare Malone, "State Websites Are Hackable—and That Could Compromise Election Security," *FiveThirtyEight*, May 31, 2018, <https://fivethirtyeight.com/features/state-websites-are-hackable-and-that-could-compromise-election-security/>.
- 17** James Tatum (judge of probate, Bullock County, Alabama), interview by Brennan Center for Justice, May 2, 2019; Clay Helms and John Bennett, interview by Brennan Center.
- 18** As used in this report, the terms "cyber navigator program" (CNP) and "cyber navigators" refer to the Cyber Navigator Program established pursuant to 10 ILCS 5/1A-55 and CNP personnel, not the Cyber Navigator service offered by Protinuum.
- 19** Clay Helms and John Bennett, interview by Brennan Center.
- 20** *Election Security Hearing* (statement of Lawrence Norden).
- 21** 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>.
- 22** Ruth Johnson, Oakland County clerk/register of deeds, 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](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/ess/automark/>.
- 23** *Election Security Hearing* (statement of Lawrence Norden).
- 24** James Tatum, interview by Brennan Center; Clay Helms and John Bennett, interview by Brennan Center.
- 25** James Tatum, interview by Brennan Center.
- 26** Matt Dietrich (spokesman, Illinois State Board of Elections), interview by Brennan Center for Justice, May 3, 2019.
- 27** James Tatum, interview by Brennan Center.
- 28** Mark Phillips, "Arizona's Brush with Potential Hacker During 2016 Election," *ABC 15*, April 18, 2019, <https://www.abc15.com/news/state/arizonas-brush-with-potential-hacker-during-2016-election>.
- 29** Sambo "Bo" Dul (election services director, Arizona Secretary of State) and Bill Maaske (chief information officer, Arizona Secretary of State), interview by Brennan Center for Justice, May 17, 2019.
- 30** Ibid.
- 31** Arizona Department of State, "Arizona 2018 HAVA Election Security Funds," 2018, [https://www.eac.gov/havadocuments/AZ\\_Narrative\\_Budget.pdf](https://www.eac.gov/havadocuments/AZ_Narrative_Budget.pdf).
- 32** Matt Roberts, "Secretary Reagan Seeks Updated Voter Registration System," *Prescott Valley News*, May 21, 2017, <https://prescottvalleynews.com/index.php/news/current-news/item/10238-secretary-reagan-seeks-updated-voter-registration-system>.
- 33** Election Services Division, Arizona Secretary of State, "Request for Proposal for Voter Registration System," 2017, <https://aset.az.gov/sites/default/files/itac/Exhibit%204%20-%20Meeting%20Packet%20-%20PIJ%20-%20ST18001.pdf>; Arizona State Procurement Office, "Master Blanket Purchase Order ADSP017-186601," 2017, <https://procure.az.gov/bsa/external/purchaseorder/poSummary.sdo?sessionid=C533D16BE1B852F8735B5323D81D4BCF?do-clid=ADSP017-186601&releaseNbr=0&parentUrl=contract>.
- 34** Sambo "Bo" Dul and Bill Maaske, interview by Brennan Center; Tonia Tunnell (state and federal compliance officer, County Recorder's Office, Maricopa County, Arizona), interview by Brennan Center for Justice, April 26, 2019.
- 35** Ibid.
- 36** Ibid.
- 37** *Election Security Hearing* (statement of Lawrence Norden).
- 38** Ibid.
- 39** Verified Voting, "The Verifier — Polling Place Equipment in Arizona — November 2018," accessed May 2019, <https://www.verifiedvoting.org/verifier/>.
- 40** Lawrence Norden and Andrea Cordova, "Voting Machines at Risk."
- 41** *Election Security Hearing* (statement of Lawrence Norden).
- 42** Verified Voting "The Verifier — Polling Place Equipment in Arizona."
- 43** Tonia Tunnell, interview by Brennan Center.
- 44** Sambo "Bo" Dul and Bill Maaske, interview by Brennan Center May 17, 2019.
- 45** Ibid.
- 46** Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, 2019, 50, <https://www.justice.gov/storage/report.pdf>.
- 47** Matt Dietrich, interview by Brennan Center.
- 48** Noah Praetz (former elections director, Cook County, Illinois), interview by Brennan Center for Justice, May 6, 2019; Matt Dietrich, interview by Brennan Center.
- 49** Noah Praetz, interview by Brennan Center.
- 50** Matt Dietrich, interview by Brennan Center.
- 51** Alyza Sebenius, "Trump Cyber Official Warns Voting Machines Need Paper Trails," *Bloomberg*, February 13, 2019, <https://www.bloomberg.com/news/articles/2019-02-13/trump-cyber-official-warns-voting-machines-need-paper-trails>; Melinda Deslatte, "Louisiana Starts Process to Replace 10,000 Voting Machines, but It May Come with Hefty Price Tag," *The Advocate*, March 30, 2018, [https://www.theadvocate.com/baton\\_rouge/news/politics/elections/article\\_70500bb0-345b-11e8-a151-9fe2f4f5bd30.html](https://www.theadvocate.com/baton_rouge/news/politics/elections/article_70500bb0-345b-11e8-a151-9fe2f4f5bd30.html) (in which then-secretary of state Tom Schedler warns, "The day of reckoning is coming").
- 52** Julia O'Donoghue, "Louisiana Won't Have New Voting Machines for 2019 Governor's Race," *Nola*, December 10, 2018, <https://www.nola.com/news/2018/12/louisiana-wont-have-new-voting-machines-for-2019-governors-race.html> (stating, "The secretary of state's office has faith in the older machines, even if it would have preferred to use new machines next fall. 'We haven't had problems with the machines,' Ardoin spokesman Tyler Brey said. 'We have no issues with vulnerability. They work just fine.'").
- 53** Julia O'Donoghue, "Plans to Replace Louisiana Voting Machines Stall," *Nola*, November 30, 2018, <https://web.archive.org/web/20181129033258/https://www.newsobserver.com/news/business/article222332155.html>; Melinda Deslatte, "Louisiana Starts Process to Replace 10,000 Voting Machines" (stating that, including the federal grant, there was approximately \$8 million in state funds available for new voting equipment as of March 2018); Mark Ballard, "Here's Why Louisiana Won't Get New Voting Machines in Time for Next Year's Big Elections," *The Advocate*, December 11, 2019, [https://www.theadvocate.com/baton\\_rouge/news/politics/elections/article\\_2973c230-fda6-11e8-a0da-6bb5e6c765fa.html](https://www.theadvocate.com/baton_rouge/news/politics/elections/article_2973c230-fda6-11e8-a0da-6bb5e6c765fa.html) (stating that the state has approximately \$1.5 million set aside for new voting equipment); Melinda Deslatte, "Decision Upheld to Scrap Louisiana Voting Machine Contract," *Associated Press*, November 28, 2018, <https://>

[web.archive.org/web/20181129033258/https://www.newsobserver.com/news/business/article222332155.html](http://web.archive.org/web/20181129033258/https://www.newsobserver.com/news/business/article222332155.html) (stating, “The voting machine replacement work began under Ardoin’s predecessor and former boss, Republican Tom Schedler”).

**54** Melinda Deslatte, “Louisiana Renting Early-Voting Machines for Fall Election,” *Associated Press*, April 3, 2019, <https://www.wvltv.com/article/news/politics/elections/louisiana-renting-early-voting-machines-for-fall-election/289-a2aa9046-5468-4460-ae2f-9dab84363e6d>; Lani Durio (Louisiana deputy director of elections), interview by Brennan Center for Justice, May 7, 2019.

**55** Julia O’Donoghue, “Plans to Replace Louisiana Voting Machines Stall”; Lani Durio, interview by Brennan Center (stating that state election officials plan to initiate the procurement process “in the near future”).

**56** Benjamin Freed, “Louisiana Cancels \$95 Million Contract for New Voting Machines,” *StateScoop*, October 11, 2018, <https://statescoop.com/louisiana-cancels-95-million-contract-for-new-voting-machines/>.

**57** Melinda Deslatte, “Louisiana Starts Process to Replace 10,000 Voting Machines” (stating, “[Secretary of State] Schedler estimates the entire replacement project, complete with new equipment and computer software, will cost between \$40 million and \$60 million”); Lani Durio, interview by Brennan Center.

**58** Total cost estimates range from \$40 million–\$60 million to \$95 million; see Benjamin Freed, “Louisiana Cancels \$95 Million Contract”; also see Melinda Deslatte, “Louisiana Starts Process to Replace 10,000 Voting Machines” (stating, “[Secretary of State] Schedler estimates the entire replacement project, complete with new equipment and computer software, will cost between \$40 million and \$60 million”). The federal portion of the 2018 grant, \$5,889,487, is 9.8% of \$60 million.

**59** Melinda Deslatte, “Louisiana Starts Process to Replace 10,000 Voting Machines” (stating, “Schedler said Louisiana has upped its security and continues to look for system improvements. ‘We are constantly changing codes and putting up blocks,’ he said”).

**60** Oklahoma State Election Board, “OK Narrative Budget,” 2018, [https://www.eac.gov/havadocuments/OK\\_Narrative\\_Budget.pdf](https://www.eac.gov/havadocuments/OK_Narrative_Budget.pdf).

**61** Lili Zheng, “Oklahoma Faces \$167M Budget Shortfall Next Fiscal Year,” *KFOR*, February 20, 2018, <https://kfor.com/2018/02/20/it-doesnt-look-hopeful-oklahoma-facing-167-budget-shortfall-for-next-fiscal-year/>.

**62** Oklahoma State Election Board, “OK Narrative Budget.”

**63** *Ibid.*

**64** *Ibid.*

**65** Paul Zirix (secretary, Oklahoma Board of Elections), interview by Brennan Center for Justice, May 2, 2019.

**66** Office of Management and Enterprise Services, State of Oklahoma, “State of Oklahoma Executive Budget Fiscal Year 2020,” February 2019, <https://omes.ok.gov/sites/g/files/gmc316/f/publications/bud20.pdf>; Paul Zirix, interview by Brennan Center.

**67** *Ibid.*

**68** National Conference of State Legislatures, “Post-Election Audits,” January 2019, <http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>.

**69** Oklahoma State Election Board, “OK Narrative Budget.”

**70** *Ibid.*

**71** Oklahoma State Election Board, “OK Narrative Budget.”

**72** Oklahoma State Election Board, “Current Registration Statistics by County,” January 15, 2019, [https://www.ok.gov/elections/documents/20190115%20-%20Registration%20By%20County%20\(vr2420\).pdf](https://www.ok.gov/elections/documents/20190115%20-%20Registration%20By%20County%20(vr2420).pdf).

**73** Blue Ribbon Commission on Pennsylvania’s Election Security, Study and Recommendations, 2019, 14, [https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber\\_PAs\\_Election\\_Security\\_Report.pdf](https://www.cyber.pitt.edu/sites/default/files/FINAL%20FULL%20PittCyber_PAs_Election_Security_Report.pdf).

**74** Pennsylvania Department of State, “Department of State Tells Counties to Have New Voting Systems in Place by End of 2019,” May 12, 2018, <http://www.media.pa.gov/Pages/State-Details.aspx?newsid=276>; Pennsylvania Department of State, “Wolf Administration Directs That New Voting Systems in the Commonwealth Provide Paper Record,” February 9, 2018, <https://www.media.pa.gov/Pages/StateDetails.aspx?newsid=261>.

**75** Kathy Boockvar (acting secretary of the Commonwealth, Pennsylvania Department of State) and Jonathan Marks (deputy secretary for elections and commissions, Pennsylvania Department of State), interview by Brennan Center for Justice, May 3, 2019.

**76** *Ibid.*; see also Blue Ribbon Commission on Pennsylvania’s Election Security, *Study and Recommendations*, 24.

**77** Timothy Benyo (chief clerk, registration and elections, Lehigh County, Pennsylvania), interview by Brennan Center for Justice, April 29, 2019.

**78** Zane Swanger (director of elections and voter registration, Mifflin County, Pennsylvania), interview by Brennan Center for Justice, April 30, 2019.

**79** Blue Ribbon Commission on Pennsylvania’s Election Security, *Study and Recommendations*, 34.

**80** Timothy Benyo, interview by Brennan Center.

**81** Kathy Boockvar and Jonathan Marks, interview by Brennan Center.

**82** *Ibid.*

**83** Zane Swanger, interview by Brennan Center.