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.

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."

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. 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]."

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.[10]

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:[11]

Voter registration database upgrades and maintenance. With "more voters registered and more ballots being cast than ever before,"[1] 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.[1] 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.[1] 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.[1]

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.[1]

Additional Unfunded Security Needs

Alabama election officials identified two unfunded election security projects: legacy voting equipment replacement and development of a "cyber navigator program."[1] ,[1]

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.[1]

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." [0] Specifically, as neither the AutoMARK nor the M100 is currently manufactured, finding replacement parts will be increasingly difficult over time. [1] 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. Moreover, these systems simply lack important security features expected of voting machines today, such as hardware access deterrents for ports.

State and local election officials would consider using additional election security funding to replace these legacy systems. 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.

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.

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. 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. 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. 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. [0]

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-

which, as described below, would coordinate cybersecurity resources, information, and trainings for and with local election officials.

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

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. [1],

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. 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. 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.

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 (cf1.1)(le Are

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.

Unfortunately, those funds (approximately $14 million with the state match added) are insufficient to cover the cost of replacing paperless machines statewide. The Pennsylvana 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). In Lehigh County, for example, Tim Benyo, the county's chief clerk for elections and registration, stated(ion, st)12stot2

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.

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."

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 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 A. , , , 6, 2019.

2 , A - 2016, *NPR*, A 19, 2019, // / 01 /0 /1 / 1 0 / - - - - - - 01 ; 2 2016, , *ABC News*, 15, 2019, // / / - - 01 - / 0 .

3 , 2016 , *Politico*, 5, 2019, // / / 01 /0 /0 / - - - - 01 -1 0 .

4 A , *Grant Expenditure Report, Fiscal Year 2018*, A 4, 2019, // . - / /1/ / - 01 A A .

5 *Oversight of the U.S. Election Assistance Commission Hearing, Before the Sen. Comm. on Rules and Administration*, 116 . (2019) (, , A).

6 A , A - , // / /1 (

.9 (0 ( )9 (15(-) -0.0410.1 (/)79 (/)7)10 ( ) 208( )30.1)-5 ,01 - (,-)-20 -2116.1 - (()20 (810)29.1 -(,-

12 A . , - ? -
, *Montgomery Advertiser*, 12, 2018, // -
/ / / / 01 /11/0 / - -
/1 01 00 /.

13 , 1, .

14 (, A)
(, A),
, 9, 2019.

15 .

16 , A
, *FiveThirtyEight*, 31, 2018,
// / / - - -
/.

17 (, , A),
, 2, 2019;
, .

18 A , .
( )
10 5/1A-55 , .

19 , .

20 *Election Security Hearing* ( ).

21 A , *Voting Machines at Risk: Where We Stand Today*, , 5, 2019,
// / / - -
.

22 , / , ,
, A ,
2, 2008, // / /1/ / -
-100 -
(8 -100
);
(&) A A , -
(A A), 4,
2019, // / / - /
/ /).

23 *Election Security Hearing* ( ).

24 , ;
, .

25 , .

26 (,),
, 3, 2019.

27 , .

28 , A '

1 . 1 . 1 . -
A 1 -1 01& 0& .

34 , ;
(,
, , A),
, A 26, 2019.

35 .

36 .

37 *Election Security Hearing* ( ).

38 .

39 , , A -
2018, 2019, // . -
/ /.

40 A ,
.

41 *Election Security Hearing* ( ).

42 .
A .

43 , .

44 ,
17, 2019.

45 .

46 , *Report on the Investigation into Russian Interference in the 2016 Presidential Election*,
, 2019, 50, // - /
/ .

47 , .

48 (, ,),
, 6, 2019; ,
.

49 , .

50 , .

51 A , ,
, *Bloomberg*, 13, 2019, ://
/ / /2019-02-13/ -
- - - ; ,
10,000 ,
, *The Advocate*, 30, 2018, //
/ - / / / /
0 00 0- -11 - 1 1- 0. (
- ,
).

52 , ,
2019 , *Nola*, 10, 2018, //
/ / 01 /1 / - - - - - -
- 01 - - . (
,
, A .
').

53 , , -
, *Nola*, 30, 2018, // - /
/ 01 11 0 / / / /
/ 1 ; ,
10,000 (,
, $8
2018); ,
, *The Advocate*, 11, 2019, //
/ - / / / / -
0- -11 - 0 - . (
$1.5 -
); , ,
, *Associated Press*, 28, 2018, //