Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated July 8, 2022

Election Security: Federal Funding for Securing Election Systems

State and local systems were targeted as part of efforts to interfere with the 2016 elections, according to the U.S. intelligence community. Reports of those activities highlighted the potential for threats to the technologies, facilities, and processes used to administer elections. Congress has responded to such threats, in part, by providing and proposing funding to help secure elections.

This In Focus offers an overview of federal funding for securing election systems. It starts with some background on potential threats to state and local election systems and then summarizes the funding Congress has provided and proposed to help secure those systems.

Background

Elections-related systems in all 50 states were likely targeted in the 2016 election cycle, according to a July 2019 report from the Senate Select Committee on Intelligence. Some attempts to access state and local systems succeeded. Foreign actors reportedly extracted data from the statewide voter registration database in one state, for example, and breached county systems in another.

Multiple techniques were used to target state and local election systems in the 2016 cycle. Attackers tried to access voter registration databases by entering malicious code in the data fields of state or local websites, for example, and to gain access to county systems by sending election officials emails with malware attached.

Election systems may also be vulnerable to other types of attack. Hacked election office websites or social media accounts might be used to disseminate disinformation, for example. Malware might be spread among non-internet-connected voting machines, computer scientist J. Alex Halderman has testified, in the course of programming the machines with ballot designs. Individuals with access to election storage facilities might tamper with ballot boxes.

Some threats to election systems may also be compounded by the structure of U.S. election administration. States, territories, and localities—which have primary responsibility for conducting elections in the United States—use different election equipment and processes and have varying levels of access to security resources and expertise. This decentralization may help guard against large-scale, coordinated attacks, but it also offers potential attackers multiple possible points of entry, some of which may be less well defended than others.

Limited attacks on less well defended jurisdictions might undermine voters' confidence in the legitimacy of the election process or the winners it produces. In some cases, some have suggested, such small-scale attacks might also be capable of changing election outcomes.

Appropriated Funding

States, territories, and localities have primary responsibility for ensuring that election systems are secure, but federal agencies also play a role in helping identify and address election system threats and vulnerabilities. Since the 2016 elections, Congress has provided election system security funding both to states, territories, and the District of Columbia (DC) and to federal agencies.

Funding for States, Territories, and DC

The consolidated appropriations acts for FY2018 (P.L. 115-141), FY2020 (P.L. 116-93), and FY2022 (P.L. 117-103) included $380 million, $425 million, and $75 million, respectively, for payments to states, territories, and DC under the Help America Vote Act of 2002 (HAVA; 52 U.S.C. §§20901-21145). All three sets of payments were available to the 50 states, DC, American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands, and the FY2020 and FY2022 funds were also available to the Commonwealth of the Northern Mariana Islands (CNMI).

Funds for the payments were appropriated under provisions of HAVA that authorize funding for certain general improvements to election administration, which may include security improvements. Explanatory statements accompanying the FY2018 and FY2020 bills also explicitly listed the following as acceptable uses of the funds:

- replacing paperless voting equipment,
- implementing postelection audits,
- addressing cyber vulnerabilities in election systems,
- providing election officials with cybersecurity training,
- instituting election system cybersecurity best practices, and
- making other improvements to the security of federal elections.

Each eligible recipient was guaranteed a minimum payment under each appropriations bill, with some recipients eligible for additional funds based on voting-age population (see **Table 1** for the total amount available to each eligible recipient under all three bills). The 50 states, DC, and Puerto Rico are required to provide a 5% match for the FY2018 funding and a 20% match for the FY2020 and FY2022 funds. All funding recipients are expected to submit plans for use of the payments to the U.S. Election Assistance Commission (EAC) and report on how they spend their funds.

According to the EAC, which is charged with administering the payments, eligible recipients had received all but $7,665 of the available FY2018 and FY2020 funding as of March

31, 2022. Spending plans and budgets for the FY2022 funds were due to the EAC on May 2, 2022.

Table 1. Total HAVA Funding Allocated to Each Eligible Recipient Under the FY2018, FY2020, and FY2022 Consolidated Appropriations Acts

($, rounded in millions)

AL	14.2	**IN**	17.4	**NV**	10.1	**TN**	17.4
AK	7.0	**IA**	10.8	**NH**	7.6	**TX**	53.7
AZ	17.2	**KS**	10.3	**NJ**	22.4	**UT**	9.7
AR	10.5	**KY**	13.3	**NM**	8.9	**VT**	7.0
CA	79.3	**LA**	13.5	**NY**	44.7	**VA**	20.9
CO	14.6	**ME**	7.6	**NC**	23.9	**WA**	18.2
CT	11.9	**MD**	16.2	**ND**	7.0	**WV**	8.7
DE	7.0	**MA**	18.1	**OH**	27.9	**WI**	16.0
DC	7.0	**MI**	24.5	**OK**	12.0	**WY**	7.0
FL	44.2	**MN**	15.2	**OR**	12.4	**AS**	1.4
GA	23.7	**MS**	10.5	**PA**	30.9	**CNMI**	0.8
HI	7.7	**MO**	16.6	**RI**	7.2	**GU**	1.4
ID	7.9	**MT**	7.1	**SC**	13.9	**PR**	8.4
IL	30.3	**NE**	8.4	**SD**	7.0	**VI**	1.4

Source: CRS, based on data from the EAC.

Notes: Figures reflect the total HAVA funds available to each eligible recipient under the FY2018, FY2020, and FY2022 consolidated appropriations acts. They do not include HAVA funds available under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Funding for Federal Agencies

Multiple federal agencies, from the Department of Homeland Security (DHS) to the Department of Justice, are involved in helping secure election systems. For more information about the role of any given agency, see CRS Report R45302, *Federal Role in U.S. Campaigns and Elections: An Overview*, by R. Sam Garrett.

Congress has designated some of the funding it has appropriated to such agencies specifically for helping secure election systems. For example, DHS designated election systems as critical infrastructure in January 2017, and report language for subsequent DHS appropriations measures has recommended funding for the agency's election security initiatives.

Agencies may also spend some of the funding they receive for more general purposes on activities related to election system security. The EAC devotes some of its operational funding to developing voluntary guidelines for voting systems, for example, and the Defense Advanced Research Projects Agency has provided funding to advance development of a secure, open-source voting system.

Proposed Funding

Proposals to provide states with grant funding for election system security have been offered in each appropriations cycle since the 2016 elections. For example, proposed FY2021 appropriations bills and amendments to FY2019 appropriations measures would have provided funding under the same provisions of HAVA and the same or similar terms and conditions as the FY2018, FY2020, and FY2022 bills.

Some Members have also introduced bills to authorize other election system security spending. For example, the For the People Act of 2021 (H.R. 1/S. 1/S. 2093) would authorize grant programs for various election system security purposes, including replacing paperless voting systems, and the 117th Congress's Freedom to Vote Act (S. 2747), Freedom to Vote: John R. Lewis Act (H.R. 5746), and Sustaining Our Democracy Act (H.R. 7992/S. 4239) would provide for ongoing funding for securing election infrastructure and other elections activities.

Such proposals have taken various approaches to securing election systems. Some of the ways in which they vary are:

- **Type of Threat Addressed.** Election systems face multiple threats. Bad actors might target technological, physical, or human vulnerabilities in the system, for example, or more than one of the above. Funding proposals offered since the 2016 elections have aimed to address several types of threat. For example, the FAST Voting Act of 2019 (H.R. 1512) would have authorized funding that could be used for securing the physical chain of custody of voting machines, among other purposes, and the EAC Reauthorization Act of 2017 (H.R. 794) would have authorized appropriations for payments to upgrade the technological security of voter registration lists.
- **Timing of Response.** Efforts to secure election systems can be aimed at mitigating a risk at any point in its lifecycle (e.g., identifying, protecting, detecting, responding, or recovering). Funding has been proposed for interventions at various points. Some of the funding provisions of the SAFE Act (H.R. 2722; 116th Congress) were directed at protecting election systems against attacks, for example, while others would have helped officials respond to them.
- **Specificity of Uses.** Some of the funding provisions of election system security bills have focused on specific activities. Others would authorize appropriations for more general purposes and delegate responsibility for identifying the best uses of the funds to states or other entities. The Election Security Assistance Act of 2019 (H.R. 3412), for example, would have left decisions about how to use its payments largely to states and territories. The 115th Congress's Secure Elections Act (H.R. 6663/S. 2261/S. 2593) would, among other provisions, have established an election cybersecurity advisory panel and authorized a grant program for implementing the panel's guidelines.

Among the proposed bills listed above, an FY2021 consolidated appropriations bill (H.R. 7617), the Freedom to Vote: John R. Lewis Act (H.R. 5746; 117th Congress), the SAFE Act (H.R. 2722; 116th Congress), and a version of the For the People Act of 2021 (H.R. 1) have been passed by the House. None of the other legislative proposals listed above had passed either chamber as of this writing.

Karen L. Shanton, Analyst in American National Government

IF11286

Disclaimer