Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 8, 2019

Election Security: Federal Funding for Securing Election Systems

Russia targeted state and local systems as part of its effort to interfere with the 2016 elections, according to the U.S. Intelligence Community. Reports of Russia's 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, the Senate Select Committee on Intelligence (SSCI) suggested in a July 2019 report. Some attempts to access state and local systems succeeded. Russian actors reportedly extracted voter 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 obtain access to county systems by sending emails to election officials 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 misinformation, 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 voting equipment.

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 able to change 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. Congress has provided election system security funding both to states, territories, and the District of Columbia (DC) and to federal agencies since the 2016 elections.

Funding for States

The FY2018 Consolidated Appropriations Act (P.L. 115-141) included $380 million for payments to the 50 states, DC, American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands (referred to herein as "states") under the Help America Vote Act of 2002 (HAVA; 52 U.S.C. §§20901-21145).

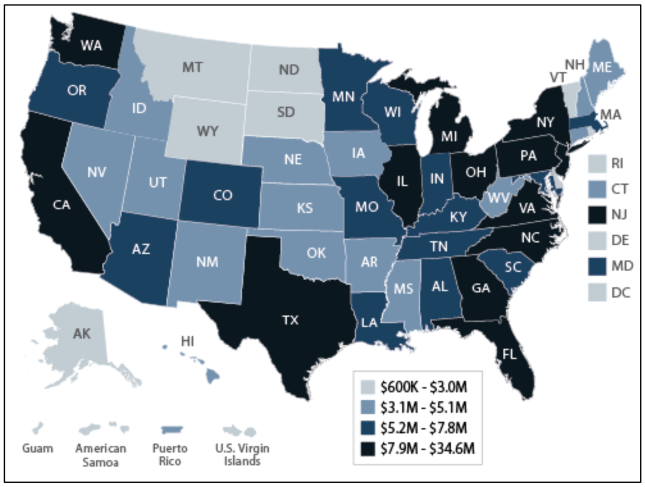
The FY2018 payments were appropriated under provisions of HAVA that authorize payments to states for general improvements to the administration of federal elections. The explanatory statement accompanying the FY2018 bill listed the following as acceptable uses of the funding:

- replacing paperless voting machines,
- conducting 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 state was guaranteed a minimum payment under the FY2018 appropriations bill, with some eligible for additional funds based on voting-age population (see **Figure 1**). The 50 states, DC, and Puerto Rico are required to provide a 5% match for the federal funds they receive, and all funding recipients were asked to submit their plans for the payments to the U.S. Election Assistance Commission (EAC) and report each year on how they spend their funds.

According to the EAC, which is charged with administering the FY2018 HAVA payments, all of the available funds were requested by July 16, 2018, and disbursed to the states by September 20, 2018. States spent at least $108.14 million of the $380 million total by the end of April 2019, the agency reported to the House Committee on House Administration in July 2019.

Figure 1. FY2018 HAVA Election Security Funds



Source: U.S. Election Assistance Commission.

Funding for Federal Agencies

In addition to payments to the states, Congress has provided election system security funding to federal agencies. Multiple agencies, from the U.S. Department of Homeland Security (DHS) to the U.S. Department of Justice (DOJ), 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 the report language for subsequent DHS appropriations measures has recommended funding for the agency's Election Infrastructure Security Initiative (EISI). The explanatory statement for the FY2018 spending bill also directed the Federal Bureau of Investigation (FBI) to use some of its funding to help counter threats to democratic institutions and processes.

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 (DARPA) has provided funding under its System Security Integrated Through Hardware and Firmware (SSITH) program to advance development of a secure, open-source voting system.

Proposed Funding

Proposals to provide funding for election system security have been offered in each appropriations cycle since the 2016 elections. For example, proposed amendments to FY2019 appropriations measures in the House and Senate would have provided $380 million and $250 million, respectively, under the same provisions of HAVA and the same or similar terms and conditions as the FY2018 appropriations bill. The House-passed version of the FY2020 Financial Services and General Government (FSGG) appropriations bill (H.R. 3351) includes $600 million for payments to the states to replace direct-recording electronic (DRE) voting machines and make other election security improvements.

Some Members have also introduced bills to authorize other election system security spending. For example, the For the People Act of 2019 (H.R. 1), which incorporates provisions of a number of other measures, would authorize funding for various election system security purposes, including replacing paperless voting systems and conducting postelection audits. The Election Security Assistance Act (H.R. 3412) would authorize $380 million in payments to the states for purposes such as enhancing election technology and improving election security.

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 authorize grants for securing the physical chain of custody of voting machines, among other purposes, and the EAC Reauthorization Act of 2017 (H.R. 794; 115th Congress) would have authorized funding to upgrade the technological security of voter registration lists.
- **Timing of Response.** Efforts to secure election systems can try to mitigate 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) would aim to protect election systems against attacks, for example, while others would try to help election officials respond to them.
- **Specificity of Uses.** Some of the funding provisions of election system security bills have been directed to specific purposes. Others would authorize more general election security funds and delegate responsibility for identifying the best uses for them to states or other entities. The Election Security Assistance Act of 2019 (H.R. 3412), for example, would leave decisions about how to use its payments largely to the states. The 115th Congress's Secure Elections Acts (S. 2261; S. 2593; H.R. 6663) would, among other provisions, have established an election cybersecurity advisory panel and grants for states and localities to implement the panel's guidelines.

Three of the above proposals—the House's FY2020 FSGG appropriations bill (H.R. 3351), the For the People Act of 2019 (H.R. 1), and the SAFE Act (H.R. 2722)—had been passed by the House as of this writing. None of the other proposals had advanced past referral to committee or committee hearings.

Karen L. Shanton, Analyst in American National Government

IF11286

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.