GAO Highlights

Highlights of GAO-20-267, a report to congressional committees

February 2020

ELECTION SECURITY

DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections

Why GAO Did This Study

In January 2017, the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. The designation allowed DHS to prioritize assistance to state and local election officials to protect key election assets, including voter registration databases and voting equipment.

The Conference Report (H. Rep. No. 116-9) accompanying the 2019 Consolidated Appropriations Act included a provision for GAO to examine how DHS is implementing key responsibilities to help protect the election infrastructure and the reported benefits and challenges of such efforts.

This report addresses (1) DHS's election security efforts and selected election officials' perspectives on them, and (2) DHS's planning for the 2020 elections. GAO reviewed DHS's strategies, plans, and services provided to election officials. GAO also interviewed DHS officials, representatives of the EI-ISAC, a DHS-funded center responsible for sharing threat information nationwide, and election officials from eight states and three local jurisdictions.

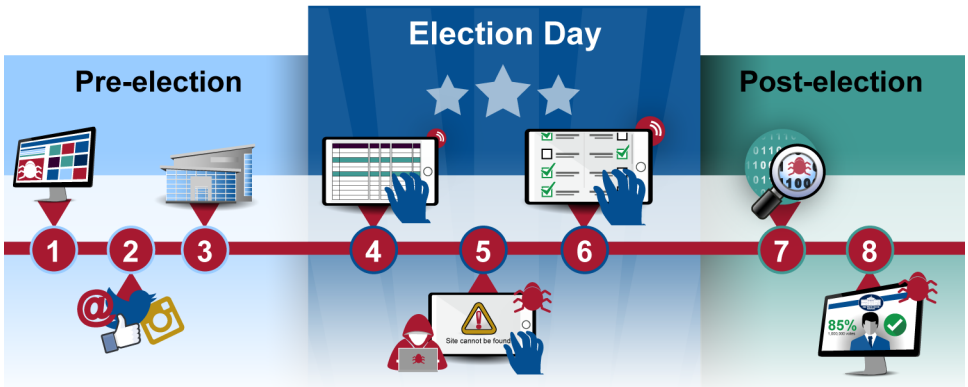
GAO selected the states and local jurisdictions to provide geographic diversity and variation in election administration, among other factors. The results from these states and localities are not generalizable, but provide insight into election officials' perspectives on DHS's efforts.

View GAO-20-267. For more information, contact Vijay D'Souza at (202) 512-6240 or dsouzav@gao.gov or Rebecca Gambler at (202) 512-8777 or gamblerr@gao.gov.

What GAO Found

Since the 2017 designation of election infrastructure as critical infrastructure, the Department of Homeland Security (DHS), through its Cybersecurity and Infrastructure Security Agency (CISA), has assisted state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing. Such efforts help state and local election officials protect various election assets from threats (see figure).

Figure: Examples of Election Assets Subject to Physical or Cyber Threats



1 Online voter registration systems
2 Election office social media accounts
3 Storage locations
4 Electronic poll books
5 Voter registration systems
6 Vote casting devices
7 Election management systems
8 Official websites

Source: GAO analysis based on information reported by the Department of Homeland Security, the Harvard University John F. Kennedy School of Government's Belfer Center for Science and International Affairs, and the Center for Internet Security. | GAO-20-267

In August 2019, the CISA Director identified election security as one of the agency's top five operational priorities. CISA security advisors, who are located throughout the country, consult with state and local election officials and identify voluntary, no cost services that CISA can provide. According to CISA, as of November 2019, 24 cybersecurity advisors and 100 protective security advisors perform and coordinate cyber and physical security assessments for the 16 critical infrastructure sectors, including the Election Infrastructure Subsector. Technical teams at CISA headquarters generally provide the services, once requested.

To further assist state and local election officials, CISA conducted two exercises simulating real-world events and risks facing election infrastructure in August 2018 and June 2019. According to CISA, the 2019 exercise included 47 states and the District of Columbia. In addition, CISA has funded the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). According to CISA officials, the EI-ISAC is the primary mechanism for exchanging information about threats and vulnerabilities throughout the election community. The EI-ISAC director reported that, as of November 2019, its members included 50 states, the District of Columbia, and 2,267 local election jurisdictions, an increase from 1,384 local jurisdictions that were members in 2018. As a result of its efforts, CISA has provided a variety of services to states and local election jurisdictions in the past 2 years (see table).

What GAO Recommends

GAO is making three recommendations to the CISA Director to (1) urgently finalize the strategic plan and the supporting operations plan for securing election infrastructure for the upcoming elections, (2) ensure that the operations plan fully addresses all lines of effort in the strategic plan for securing election infrastructure for the upcoming elections, and (3) document how the agency intends to address challenges identified in its prior election assistance efforts and incorporate appropriate remedial actions into the agency's 2020 planning. DHS concurred with all three recommendations and provided estimated dates for implementing each of them.

Table: Number of Selected Cybersecurity and Infrastructure Security Agency Services Provided to States and Local Election Jurisdictions in 2018 and 2019, as of November 6, 2019

Service	States	Local election jurisdictions
Continuous scanning of internet-accessible systems for known vulnerabilities	40	161
Assessments of potential network security vulnerabilities	26	20
Remote testing of externally accessible systems for potential vulnerabilities	4	44
Assessments of states' and local jurisdictions' susceptibility to malicious emails	10	5
Educational posters on cybersecurity	19	1,202

Source: Cybersecurity and Infrastructure Security Agency. | GAO-20-267

State election officials with whom GAO spoke were generally satisfied with CISA's support to secure their election infrastructure. Specifically, officials from seven of the eight states GAO contacted said that they were very satisfied with CISA's election-related work. Also, officials from each of the eight states spoke positively about the information that they received from the EI-ISAC. Further, officials from five states told GAO that their relationship with CISA had improved markedly since 2017 and spoke highly of CISA's expertise and availability.

To guide its support to states and local election jurisdictions for the 2020 elections, CISA reported that it is developing strategic and operations plans. CISA intended to finalize them by January 2020, but has faced challenges in its planning efforts due to a reorganization within CISA, among other things. In the absence of completed plans, CISA is not well-positioned to execute a nationwide strategy for securing election infrastructure prior to the start of the 2020 election cycle. Further, CISA's operations plan may not fully address all aspects outlined in its strategic plan, when finalized. Specifically, according to CISA officials, the operations plan is expected to identify organizational functions, processes, and resources for certain elements of two of the four strategic plan's lines of effort—protecting election infrastructure, and sharing intelligence and identifying threats. CISA officials stated that CISA was unlikely to develop additional operations plans for the other two lines of effort—providing security assistance to political campaigns, and raising public awareness on foreign influence threats and building resilience.

Moreover, CISA has not developed plans for how it will address challenges, such as concerns about incident response, identified in two reviews—one conducted by CISA and the other done by an external entity under contract—of the agency's 2018 election security assistance. Challenges that the reviews identified include:

- inadequate tailoring of services, which could have made it more difficult for CISA to meet the resource and time constraints of customers such as local election jurisdictions;
- not always providing actionable recommendations in DHS classified threat briefings or making unclassified versions of the briefings available, which may have hindered election officials' ability to effectively communicate with information technology and other personnel in their agencies who did not have clearances;
- the inability of CISA personnel supporting election security operations to access social media websites from situational awareness rooms, which hindered their collection and analysis of threat information;
- few capabilities that CISA field staff could quickly provide on Election Day, which could limit the agency's timeliness in responding to an incident; and
- a lack of clarity regarding CISA's incident response capabilities in the event of a compromise that exhausts state and local resources, which may limit knowledge about agency capabilities that are available.

Although CISA officials said that the challenges identified in the reviews have informed their strategic and operational planning, without finalized plans it is unknown whether CISA will address these challenges.