Report to Congressional Committees

February 2020

ELECTION SECURITY

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

Accessible Version

GAO-20-267

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.

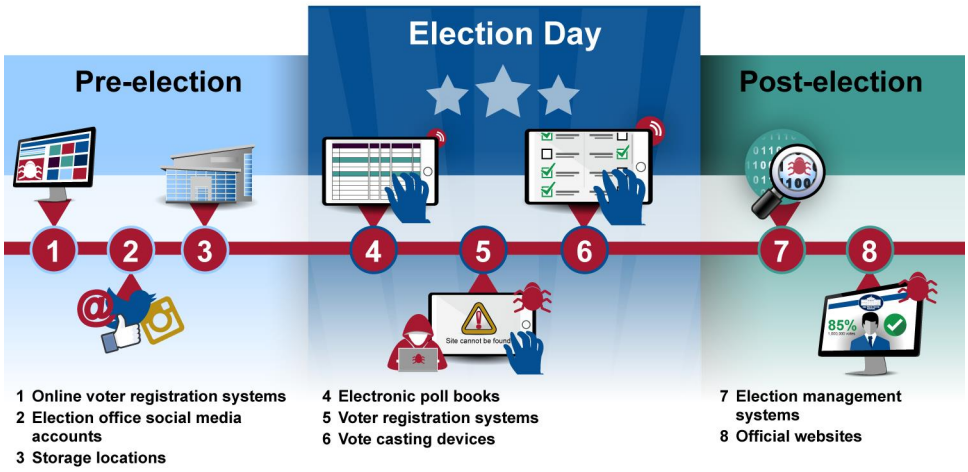
GAO selected the states and local jurisdictions to provide geographic diversity and variation in election administration, among other factors. The results from these states and localities are not generalizable, but provide insight into election officials' perspectives on DHS's efforts.

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



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.

Contents

Tables

Figure

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EAC	Election Assistance Commission
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 6, 2020

The Honorable Shelley Moore Capito
Chairwoman
The Honorable Jon Tester
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable Lucille Roybal-Allard
Chairwoman
The Honorable Chuck Fleischmann
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

In July 2019, the U.S. Senate Select Committee on Intelligence publicly reported that the Russian government had directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level.[1] Further, according to the Department of Homeland Security (DHS), perceived and actual threats to voting equipment as well as computerized (cyber) systems used to support the elections process—such as voter registration databases—may diminish the overall public confidence that elected officials need to perform their public duties and may undermine the integrity of the nation's democratic process.

Given the vital role of elections to American democracy, the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector, known as the Election Infrastructure Subsector,

[1]U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*. https://intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

in January 2017.[2] Following this designation, DHS took steps to establish partnerships with federal, state, and local governments, as well as private sector entities; and to promote and prioritize cybersecurity and physical assistance to state and local election officials who request it.

The Conference Report accompanying the Consolidated Appropriations Act, 2019, included a provision for us to examine how DHS is implementing key responsibilities to help protect the election infrastructure subsector and the reported benefits and challenges of such efforts.[3] This report addresses (1) how DHS helps to protect election infrastructure, and selected states' and local election jurisdictions' perspectives on DHS's efforts; and (2) the extent to which DHS is developing plans to assist states and local jurisdictions in securing election infrastructure in preparation for the 2020 elections and is addressing challenges identified in prior election assistance efforts.

To address both objectives, we reviewed relevant documentation, such as DHS's Election Infrastructure Security Resource Guide. We also interviewed relevant DHS officials regarding the department's key roles and responsibilities for assisting state and local officials in securing the election infrastructure. Specifically, we interviewed headquarters officials from DHS's Cybersecurity and Infrastructure Security Agency (CISA) and CISA officials assigned to regions who work with state and local election officials. We also received written responses to questions from the DHS Office of Intelligence and Analysis.

We also interviewed officials from the Center for Internet Security, which operates the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), a central resource for states and local election jurisdictions to receive cybersecurity services and information. In addition, we attended CISA's national election cyber tabletop exercise in June 2019, which simulated real world events and potential issues facing the election infrastructure in collaboration with federal, state, and local partners.

[2]DHS, *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*. News release, January 6, 2017. Accessed February 25, 2019. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[3]H. Rep. No. 116-9, at 492 (2019), Conf. Rep. accompanying the Consolidated Appropriations Act, 2019, Pub. L. No. 116-6 (Feb. 15, 2019).

In addition, to address the first objective regarding selected states' and local election jurisdictions' perspectives on DHS's efforts, we conducted semi-structured interviews with the election directors or their designated representatives within selected states, and the chief election officials or their designated representatives within selected local election jurisdictions.

To select the states, we considered factors including geographic distribution and variation in election governance systems. Regarding geographic distribution, we ensured that there were no more than two states from a given critical infrastructure protection region established by CISA. With regard to the variation in election governance systems, we considered whether counties or municipalities managed elections and whether states' voter registration systems were managed from a central, state-level platform (known as "top down"), managed at the local level and transmitted to state-wide databases (known as "bottom up"), or managed using a hybrid of the two approaches. Based on these factors, we selected eight states.

The eight states that we selected included at least one state in which counties manage elections and at least one state in which municipalities manage elections. The selection also included at least one state that used each type of voter registration system: top down, bottom up, or hybrid. In addition, for the local election jurisdictions, we randomly chose three of the previous eight selected states and then reached out to the largest local election jurisdiction within each of these. We are providing information on state and local perspectives in the aggregate, due to the sensitivity of state and local interactions with DHS regarding the security of their election infrastructures.

We asked state and local election officials questions about the physical security and cybersecurity services and assessments that they requested and received from DHS; we also asked them to assess how, if at all, DHS helped their states or local jurisdictions secure their election infrastructures. The results from these states and localities are not generalizable, but provide insight into election officials' perspectives on DHS's efforts. We asked officials from states and localities a variety of questions regarding their interactions with DHS. Not all states and localities responded to all questions, and in some cases we asked different follow up questions of officials.

Further, we interviewed officials from the National Association of Secretaries of State and the National Association of State Election

Directors, which represent state election officials, and the Election Center, which represents local election officials. We met with officials from these groups to discuss their relationship with CISA as well as any benefits and challenges members have reported regarding CISA's election assistance efforts.

To address the second objective, we reviewed CISA's draft strategic plan to identify the agency's goals and objectives to assist states and local jurisdictions in mitigating risks and protecting the election infrastructure for the 2020 election cycle. We then assessed CISA's planning efforts against our prior reports that identified leading practices for effective planning[4] and DHS's National Planning System planning guidance.[5]

We also assessed how CISA addressed challenges identified during two reviews of the agency's 2018 election security assistance, as cited in a draft report produced by CISA[6] and another report produced by the RAND Corporation.[7] We compared the agency's efforts to address challenges identified in these reports to DHS's National Infrastructure Protection Plan, 2013,[8] and GAO's Standards for Internal Control in the Federal

[4]GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, GAO-18-562 (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, GAO-17-300 (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, GAO-15-602 (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, GAO-05-372 (Washington, D.C.: Sept. 8, 2005); and *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[5]Department of Homeland Security, *National Planning System* (February 2016).

[6]Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, DRAFT *2018 Midterm Elections Security Operations After Action Report* (Washington, D.C.: April 2019).

[7]Benjamin Boudreaux, Quentin E. Hodgson, Edward Chan, *Quick Look: Elections Security Lessons Learned from the 2017-2018 Election Cycle*, Homeland Security Operational Analysis Center, April 2019. The Homeland Security Operational Analysis Center is a federally funded Research and Development Center operated by the RAND Corporation under a contract with DHS.

[8]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

Government, which, among other things, provides standards on how management should address identified deficiencies.[9]

We conducted this performance audit from February 2019 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Administration of State and Federal Elections Involves Various Roles, Responsibilities, and Processes

In the United States, authority to regulate elections is shared by federal, state, and local officials. Congressional authority to regulate elections derives from various constitutional sources, depending on the type of election. In addition, Congress has passed legislation in major functional areas of the voting process, such as voter registration and prohibitions against discriminatory voting practices.

However, responsibility for the administration of state and federal elections resides at the state level. States regulate various aspects of elections including, for example, registration procedures, absentee and early voting requirements, and Election Day procedures.

Within each state, responsibility for managing, planning, and conducting elections is largely a local process, residing with about 10,300 local election jurisdictions nationwide. Some states have mandated statewide election administration guidelines and procedures that foster uniformity in the way their local jurisdictions conduct elections, whereas other states have guidelines that generally permit local election jurisdictions considerable autonomy and discretion in the way they run elections. The

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

result is that elections can be administered differently across states and local jurisdictions.[10]

Unless states require otherwise, local jurisdictions generally have discretion over activities such as election officials' training and, in most states, the selection and purchase of voting technology. Among other things, local election officials register eligible voters; educate voters on how to use voting technology; provide information on the candidates and ballot measures; recruit, train, organize, and mobilize poll workers; prepare and test voting equipment for use; and count ballots.

The election process is composed of pre-election, Election Day, and post-election activities:

- **Pre-election** activities include providing opportunities for eligible individuals to register to vote, maintaining and updating the voter registration database, recruiting and training poll workers, selecting polling locations, preparing voting materials, testing equipment, qualifying candidates for office, and administering absentee and vote-by-mail voting processes.
- **Election Day** activities include opening and closing polling places, setting up voting machines and voting booths, checking in voters and verifying registration status, and providing opportunities for voters to mark and cast ballots.
- **Post-election** activities include securing equipment and ballots, transferring physical ballots or records of vote counts to a central location for counting, determining the outcome of the election, publishing unofficial results, certifying official election results, and performing recounts, if required.

[10]The state and local offices that administer or oversee elections can be organized in different ways, and in some cases offices with primary responsibility for elections may have responsibility for other areas of government as well. For example, state election offices may include a Board of Elections that is responsible for overseeing elections in the state or a Secretary of State's office that oversees an Elections Division, as well as other divisions and offices responsible for public records, business filings, state archives, and other services. Similarly, local election offices may include a Board of Elections that is specifically responsible for elections, or a county clerk's office that may also have responsibility for public records, licenses, or other activities.

Election Infrastructure Relies on Various Components and Assets and Is Susceptible to Threats

The election process relies on various assets—such as information technology systems, networks, equipment, and facilities. These assets can be broadly categorized as physical, cyber, and human components of the Election Infrastructure Subsector, as described in table 1.

Table 1: Election Infrastructure Subsector Components and Assets

Component	Description	Examples of assets
Physical	Equipment, materials, and facilities that support or provide protection for election activities.	Voting equipment, storage facilities, ballot processing facilities, voting locations, paper poll books[a] and ballots.
Cyber	Hardware and software, including computers, servers, databases, and other information technology systems used in election activities.	Voter registration systems; electronic poll books; election-night reporting systems; election management systems;[b] public websites with voter data; and electronic voting equipment such as direct recording electronic machines, optical scanners, and ballot marking devices.
Human	Personnel with unique training, certification, knowledge, skills, authorities, or roles whose absence could hinder election activities.	State and local election officials, information technology staff, temporary staff such as poll workers, and vendor support staff.

Source: GAO analysis of Department of Homeland Security information. | GAO-20-267.

[a]A poll book is a list of eligible voters assigned to a local election jurisdiction and is commonly organized alphabetically or by the address of the voters. Jurisdictions use either paper or electronic poll books—most often laptops or tablets—to check in voters.

[b]According to the Center for Internet Security, election management systems handle all backend activities for elections and are used to design or build ballots, program the election database, and report results. Center for Internet Security, A Handbook for Elections Infrastructure Security (East Greenbush, NY.: February 2018).

Physical, cyber, and human assets comprising the election infrastructure are susceptible to unintentional and intentional threats.[11] As we have previously reported, unintentional, or nonadversarial, threat sources include equipment failures, software coding errors, or the accidental actions of employees (human errors).[12] Threat sources also include

[11]According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

[12]GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

natural disasters and other events that can cause failure within sectors on which the election infrastructure is dependent, such as power grid failures in the energy sector.

Intentional, or adversarial, threats can involve targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These adversaries vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include seeking monetary gain or pursuing an economic, political, or military advantage. Appendix I lists general cybersecurity threat sources that can impact information technology systems that support the election infrastructure.

Cyber adversaries may make use of various techniques, tactics, and practices—or exploits—to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. These exploits are carried out through various conduits, including websites, email, wireless and cellular communications, internet protocols, portable media, and social media. Further, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, to deliver a threat by embedding malware or other exploits within software files that can be activated when a user opens a file within its corresponding program.

DHS and others have identified general cyber and physical threats that are applicable throughout the election process.[13] For example, voting equipment may be susceptible to a supply chain attack in which the malicious actor may use the voting equipment vendor as a pathway to plant malware to modify or compromise ballot definition files before they

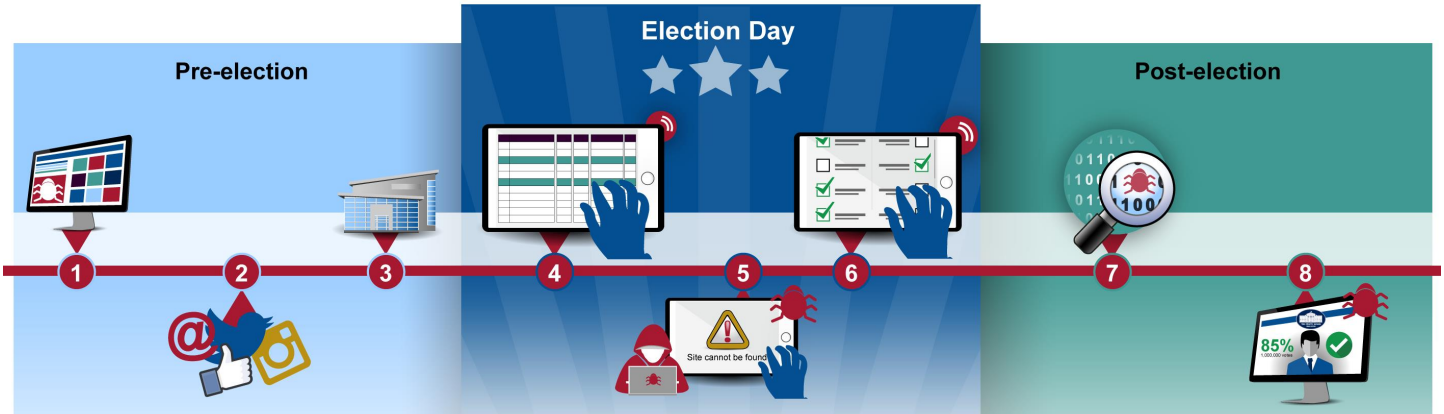
[13]See, for example, Belfer Center for Science and International Affairs, Harvard University John F. Kennedy School of Government, *The State and Local Election Cybersecurity Playbook (*Cambridge, MA.: President and Fellows of Harvard College, 2018); Center for Internet Security, *A Handbook for Elections Infrastructure Security* (East Greenbush, NY.: February 2018); National Conference of State Legislatures, *Voting System Standards, Testing and Certification,* August 2018, accessed December 3, 2019, http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx; and Technical Guidelines Development Committee, *Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission* (August 2007), accessed January 31, 2020, https://www.eac.gov/sites/default/files/eac_assets/1/28/TGDC_Draft_Guidelines.2007.pdf.

reach the hands of election officials.[14] Also, the absence of or lack of consistent physical access controls, auditable chain of custody procedures, or vendor installed countermeasures may allow malicious actors or well-placed insiders to manipulate voting equipment and ballots at any stage of the process through unauthorized physical access.

In addition, there are certain physical and cyber threats that are applicable to individual assets and stages in the election process. Figure 1 provides examples of threats to various assets and stages in the election process.

[14]The ballot definition file is a unique file for each election that records all necessary options for casting and recording votes. It may also enable the supporting software to successfully register ballot images and tabulate votes.

Figure 1: Examples of Physical and Cyber Threats to the Election Infrastructure and Assets by Stage of the Election Process



1 **Online voter registration systems** may be susceptible to website spoofing as attackers can create a malicious copy of the official website to capture sensitive information or give voters the illusion that their information was updated. Targeted denial of service or outage attacks could prevent voter registration.

2 **Internal communication systems or election office social media accounts** could be compromised as attackers may use legitimate accounts from these systems to send out false information—such as false voting locations and inaccurate dates—to election officials, poll workers, or voters.

3 **Storage locations** may be vulnerable to physical tampering or destruction of voting equipment by attackers with malicious intentions.

4 **Electronic poll books** may be susceptible to compromise by malicious attackers who gain access to the poll books either using a wireless connection or because the physical device is not properly secured. A compromise to a poll book could allow attackers to manipulate the voter rolls—either deleting or altering existing voter registration data resulting in confusion when voters show up to vote on Election Day.

5 **Voter registration systems** access could be blocked and its data and backups could be encrypted or erased through ransomware, a type of malicious software, by attackers until a ransom is paid. This could also result in theft or irreversible encryption of voter registration databases and other sensitive records causing disruption to Election Day activities and potential decline in public trust.

6 **Vote casting devices** may be vulnerable to physical tampering using removable media or remotely using a wireless connection. A compromise to a vote casting device could allow a malicious actor to modify a vote on Election Day.

7 **Election management systems** could be compromised due to commercial software and hardware with security weaknesses or configuration errors in network connections. A successful attack could lead to manipulation of results during electronic transmission of vote tallies.

8 **Official websites** may be susceptible to compromise as attackers may replicate the official state or county website and post opposite results than are being reported—for instance, the winner of a particular race is now the loser.

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

Note: A number of examples in the table were taken from the Harvard Belfer Center's The State and Local Election Cybersecurity Playbook and used with permission: online voter registration systems, internal communications systems or election office social media accounts, electronic poll books, vote casting devices, election management systems, and official websites.

Additionally, DHS has analyzed and identified common cybersecurity vulnerabilities[15] associated with enterprise networks[16] and voter

[15]According to the National Institute of Standards and Technology (NIST), a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[16]An enterprise network is the organization-wide communications infrastructure that links the organization's computing devices.

registration systems supporting election infrastructure that could apply to multiple assets at all stages of the election process. Such vulnerabilities include user susceptibility to malicious email, outdated software patches, the use of default system configurations, passwords that are weak or presented in clear text, and the use of operating systems with known weaknesses that have not been properly addressed.

DHS, through CISA, Is the Lead Federal Agency for the Election Infrastructure Subsector

Presidential Policy Directive 21, issued in February 2013, shifted the nation's focus from protecting critical infrastructure against terrorism to protecting and securing critical infrastructure and increasing its resilience against all hazards, including natural disasters, terrorism, and cyber incidents.[17] The directive identified 16 critical infrastructure sectors and outlined roles and responsibilities for protecting these sectors.[18] Further, the directive established sector specific agencies as the federal entities responsible for providing institutional knowledge and specialized expertise to facilitate or support federal, state, and local governments, as well as private sector entities, in protecting critical infrastructure.

The National Infrastructure Protection Plan, updated by DHS in December 2013, further integrates critical infrastructure protection efforts between government and private sectors, among other things.[19] It describes a voluntary partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. As part of the partnership structure, the designated sector-specific agencies serve as the lead coordinators for the security programs of their respective sectors.

[17]White House, *Presidential Policy Directive 21/PPD-21: Critical Infrastructure Security and Resilience* (February 2013).

[18]The 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[19]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

In accordance with the National Infrastructure Protection Plan, the National Protection and Programs Directorate within DHS was designated the sector-specific agency, or lead federal agency, for the Election Infrastructure Subsector.[20] CISA subsequently assumed the role of sector-specific agency upon its establishment as the successor to the Directorate in November 2018.[21]

As the lead agency for the Election Infrastructure Subsector, CISA is responsible for coordinating partnership activities and information sharing and is the primary federal interface with the subsector's stakeholders with respect to security. The Election Security Initiative, part of CISA's National Risk Management Center, is responsible for managing the agency's election subsector partnerships.

To implement the voluntary partnership model, the subsector created two complementary coordinating councils—one for governments and one for private sector partners—to facilitate partnerships to support election infrastructure. Specifically, the Election Infrastructure Subsector Government Coordinating Council, created in October 2017, enables federal, state, and local governments to share information and collaborate on best practices to mitigate and counter threats to election infrastructure. The council is composed of 27 members, which include three voting members from the federal government—specifically one from DHS and two from the Election Assistance Commission (EAC)—and 24 from state and local governments.[22] The Federal Bureau of Investigation (FBI), EAC, and National Institute of Standards and Technology (NIST) coordinate

[20]The Election Infrastructure Subsector is part of the government facilities sector. The government facilities sector is to ensure continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

[21]In November 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 renamed the National Protection and Programs Directorate as the CISA. Pub. L. No. 115-278, § 2(a), 132 Stat. 4168 (Nov. 16, 2018). According to a CISA official, the agency has taken steps to further reorganize and unify using the CISA Act of 2018 as a framework. Specifically, the agency intends to reorganize several of the functions within its headquarters and field operations, including those that support election security, to a new division. The details of the reorganization were not available for this review as they were still under deliberation within DHS, CISA, and the Congress. We have ongoing work examining the reorganization efforts of CISA.

[22]The Government Coordinating Council also includes non-voting members representing DHS, EAC, the National Institute of Standards and Technology (NIST), the Department of Defense, and the Federal Bureau of Investigation (FBI).

with each other, with CISA, and with state and local governments through the Election Infrastructure Subsector Government Coordinating Council.

Additionally, the Subsector Coordinating Council was chartered in February 2018 and includes private sector entities whose services, systems, products, or technology are used by or on behalf of state or local governments in administrating the U.S. election process. The Election Infrastructure Subsector Specific Plan outlines actions that CISA, as the sector-specific agency, the Government Coordinating Council, and the Subsector Coordinating Council will take to support election infrastructure.[23]

Other Federal Agencies Also Have Key Roles in the Election Infrastructure Subsector

Within the Department of Justice, the FBI supports the Election Infrastructure Subsector by countering foreign influence operations and collecting and processing threat information on election infrastructure. This effort is headed by the FBI's Foreign Influence Task Force, which integrates the agency's cyber, counterintelligence, counterterrorism, and criminal law enforcement resources to better understand threats posed by foreign influence operations. Among other things, the task force investigates cyber operations targeting election infrastructure or public officials, and covert influence operations designed to influence public opinion and sow division through disinformation and misinformation on social media.[24] The FBI exchanges threat information with CISA and other federal partners to help states and local jurisdictions detect and prevent operations targeting the election infrastructure.

[23]Department of Homeland Security, *Election Infrastructure Subsector Specific Plan: An Annex to the National Infrastructure Protection Plan 2013* (2018).

[24]According to officials from the FBI's Foreign Influence Task Force, when the agency identifies such threats through social media, it partners with DHS to brief affected companies on key indicators, impacts to the election infrastructure, and actionable intelligence in an effort to highlight terms of service violations and encourage companies to take action and implement future protective measures. The FBI may be limited in investigating and deterring misinformation and disinformation campaigns in cases where there are no indicators of a foreign actor or foreign influence, due to sensitivities regarding constitutional guarantees of freedom of speech.

Further, the EAC supports the Election Infrastructure Subsector by carrying out its responsibilities under the Help America Vote Act.[25] Specifically, the EAC develops voluntary voting system guidelines and oversees the testing and certification of voting systems. Under the Help America Vote Act, the EAC works through the Technical Guidelines Development Committee to establish a set of principles, guidelines, and requirements specifying how voting systems are to meet standards of functionality, accessibility, and security.[26]

The EAC has also provided states with operational grants to replace voting systems.[27] According to the Acting Executive Director of EAC, states also used the grants to increase the security of election systems, such as voter registration systems, and apply other cybersecurity enhancements. Additionally, the EAC and CISA have collaborated to develop select initiatives—such as web-based training for election officials—to expand outreach to states and local jurisdictions.

NIST supports the Election Infrastructure Subsector by conducting research to develop and provide standards, tests, guidelines, best practices, and lab accreditation assistance that EAC and states and local jurisdictions may use at their discretion. The Director of NIST chairs the Technical Guidelines Development Committee. At the request of the Committee, the Director of NIST provides technical support for the Committee to carry out its duties, such as by participating in election and constituency working groups to provide technical leadership in support of the development of voluntary voting system guidelines.

[25]See Pub. L. No. 107-252, 116 Stat. 1666 (codified as amended at 52 U.S.C. §§ 20901-21145). The Help America Vote Act was enacted in 2002 and authorized about $3.86 billion in federal funding over several fiscal years to assist state and local governments in making improvements in election administration, such as replacing aging voting equipment. To help promote effective state and local administration of federal elections, the act established the EAC as an independent federal commission and, among other things, directed the Commission to develop voluntary voting system guidelines against which voting equipment can be tested and certified.

[26]The Technical Guidelines Development Committee is an advisory board to EAC that helps develop voluntary voting system guidelines. It is composed of the Director of NIST and a group of 14 other stakeholders including those with technical and scientific expertise relating to voting systems appointed jointly by the EAC and the Director of NIST.

[27]Operational grants include Title II Section 251 Requirements Payments Grants and Section 101 grants for the improvement of election administration, as well as Section 102 grants (now expired) for replacement of noncompliant voting systems.

NIST also helps election officials identify and prioritize opportunities to improve their cybersecurity posture. For example, it established a joint working group with the Election Infrastructure Subsector Government Coordinating Council and Subsector Coordinating Council to develop a framework of cybersecurity practices tailored to elections. In doing so, NIST works with the election community to identify the resources and outcomes needed to ensure the security of the election infrastructure. As part of this effort, it receives feedback from states and local jurisdictions, as well as from CISA, through the Election Infrastructure Subsector Government Coordinating Council.

DHS Provides Services to States and Local Election Jurisdictions, and Selected Election Officials Reported Being Satisfied with DHS's Assistance

DHS, through CISA, has taken steps to assist election officials in securing election infrastructure by providing services in three areas: regional support and assistance, education and awareness, and information sharing and analysis among federal, state, and local organizations. Appendix II provides a list of the services that CISA makes available to states and local election jurisdictions.

Regional support and assistance. CISA employs personnel with cyber and physical security expertise in its 10 regional offices throughout the country. According to CISA, as of November 2019, these experts included 24 cybersecurity advisors and 100 protective security advisors who perform and coordinate security assessments for the 16 critical infrastructure sectors, including the Election Infrastructure Subsector. A single advisor may be responsible for performing and coordinating assessments for an entire state or region and across multiple critical infrastructure sectors.

The cybersecurity advisors and protective security advisors consult with state and local election officials and identify services that CISA can provide on a voluntary, no cost basis. For example, according to CISA Election Security Initiative officials, cybersecurity advisors and protective security advisors have promoted CISA services and assessments, such as an assessment of network security vulnerabilities and an assessment of risks associated with information and communication technology

suppliers and service providers.[28] In addition, protective security advisors have conducted physical inspections of the protections over facilities that store election-related equipment such as voting machines or poll books. Protective security advisors told us that they also provide a web-based tool that states or local jurisdictions can use to identify security gaps and preparedness across facilities.

CISA officials stated that, although regional personnel promote cybersecurity and physical security services to election officials, personnel based at CISA headquarters conduct the more advanced cybersecurity assessments. For example, the Vulnerability Management Branch provides vulnerability scanning and risk and vulnerability assessments, while the Threat Hunting Branch responds to cyber incidents.[29]

In September 2019, officials from the Election Security Initiative told us that, based on the CISA Director's guidance, the agency gives requests from election infrastructure stakeholders a higher level of priority than requests from the other sectors. The precise length of the wait for service depends on the type of service. For some services, such as vulnerability scanning, there is no wait time, according to CISA officials, because CISA can activate the service within 24 hours.

Education and awareness. CISA disseminates educational materials to raise awareness of election security-related issues and services available to state and local election officials. For example, CISA provides a web-based training course to help election officials understand the principles of information technology management and has developed guidance to help states and localities adopt recommended information technology practices to improve their security posture. According to CISA, as of November 2019, 1,201 individuals had completed the online course.

[28]Such risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain.

[29]A risk and vulnerability assessment identifies vulnerabilities that adversaries could leverage to compromise network security controls, and may include the following methodologies: scenario-based network penetration testing, web application testing, wireless testing, configuration reviews of servers and databases, and detection and response capability evaluation. Vulnerability scanning is a service that scans internet-accessible systems for known vulnerabilities on a continual basis. As CISA identifies potential vulnerabilities, it is to notify the affected organization so that pre-emptive risk mitigation efforts can be implemented to avert vulnerability exploitation.

Further, CISA conducted two election infrastructure tabletop exercises known as “Tabletop the Vote” in August 2018 and June 2019 to help the Election Infrastructure Subsector community collaborate and identify best practices and areas for improvement in election-related cyber incident planning, identification, response, and recovery.[30] The 2018 tabletop exercise included 44 states, the District of Columbia, 16 federal entities, the National Association of Secretaries of State, and the National Association of State Election Directors. According to CISA officials, the June 2019 exercise included 47 states, the District of Columbia, 15 federal entities, the National Association of Secretaries of State, the National Association of State Election Directors, the National Governors Association, and the National Conference of State Legislatures. CISA officials also noted that CISA personnel, including regional personnel, have presented at numerous national and state meetings of election officials, such as the Election Center’s annual conference in August 2019.

In addition, as part of CISA’s Last Mile initiative, the agency collaborates with state and local election officials to create customized posters that highlight efforts to strengthen election security. The purpose of the posters is to describe the state’s or local jurisdiction’s election infrastructure assets and systems, characterize risks, and offer specific measures it should implement to mitigate those risks. Election officials can present the posters to voters, lawmakers, and their own personnel to bolster confidence in the security of their election systems. As of November 2019, CISA reported that it had delivered Last Mile posters to 19 states (including six states since the 2018 election) and 1,202 local election jurisdictions.

Information sharing and analysis. CISA collects and analyzes election security-related information—such as threat indicators, incident alerts, and vulnerability data—and shares this information with election officials to help them assess cybersecurity controls, detect threats, and mitigate risks. To further this goal, CISA partnered with the Center for Internet Security and the Election Infrastructure Subsector Government Coordinating Council to create the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) in February 2018. State and local election offices can join the EI-ISAC at no cost and receive

[30]An election infrastructure tabletop exercise is a simulation based on real world events and potential risks facing the election infrastructure designed to promote discussion of potential impacts to voter confidence, operations, and election integrity within a collaborative environment.

election-focused cyber defense tools and products.[31] According to the Director of the EI-ISAC, as of November 2019, its members included 50 states, the District of Columbia, and 2,267 local jurisdictions.

CISA officials stated that the EI-ISAC is the primary mechanism that CISA uses to exchange information throughout the election community. For example, the EI-ISAC produces a quarterly threat report to assist the election community in the analysis of active information security threats. From its inception through September 2019, the EI-ISAC had sent out 263 alerts to its members, including weekly, spotlight, and other emails, according to EI-ISAC officials.

EI-ISAC officials added that CISA funds the EI-ISAC to, among other things, deploy an intrusion detection sensor in each state specifically for voter registration systems and other supporting infrastructure to detect malicious activity and provide network security alerts.[32] CISA officials stated that the agency, in coordination with the EI-ISAC, analyzes data from these sensors to identify trends in threats and vulnerabilities across states and local jurisdictions.

CISA also manages the National Cybersecurity and Communications Integration Center (NCCIC), which receives reports of suspected malicious cyber activity from state and local officials, analyzes attempts to infiltrate election systems, and shares information about threats and vulnerabilities through the EI-ISAC. The NCCIC has also assisted election officials in responding to incidents, upon request. According to CISA officials, in fiscal years 2018 and 2019, NCCIC's Hunt and Incident Response Teams provided services to 10 states and 16 local election jurisdictions, such as incident response activities and proactive reviews for malicious activity at the time of service.

Table 2 identifies selected services that CISA provided to states and local jurisdictions in 2018 and 2019, as of November 6, 2019.

[31]The Center for Internet Security operates the EI-ISAC under a cooperative agreement with DHS. EI-ISAC membership is open to all state, local, tribal, and territorial government organizations, associations that represent election officials, and contractors that directly support the operations or maintenance of election office information technology systems.

[32]According to the EI-ISAC, its intrusion detection sensors, known as Albert sensors, recognize and alert on potentially malicious traffic occurring on a network using a unique signatures set based on commercial signatures, internal research, and indicators of advanced threats.

Table 2: Selected Cybersecurity and Infrastructure Security Agency (CISA) Services and Assessments Provided to States and Local Election Jurisdictions in 2018 and 2019, as of November 6, 2019

Service	Number provided to states	Number provided to local election jurisdictions
Vulnerability scanning[a]	40	161
Risk and vulnerability assessments[b]	26	20
Remote penetration tests[c]	4	44
Phishing campaign assessments[d]	10	5
Last Mile posters[e]	19	1,202

Source: Data reported by CISA. | GAO-20-267

Note: This table presents the number of services and assessments that CISA provided, not the number of states and local jurisdictions that received the services and assessments, as some jurisdictions may have received a service or assessment more than once. States and local jurisdictions that did not choose to receive services and assessments through CISA may be receiving them through their state's information technology department, a contractor, or other arrangements.

[a]Vulnerability scanning is a service that scans internet-accessible systems for known vulnerabilities on a continual basis, so that the election agency can take preemptive risk mitigation steps.

[b]Risk and vulnerability assessments identify vulnerabilities that adversaries could leverage to compromise network security controls. A risk and vulnerability assessment may include the following methodologies: scenario-based network penetration testing, web application testing, wireless testing, configuration reviews of servers and databases, and detection and response capability evaluation.

[c]Remote penetration tests use remote teams to assess, identify, and mitigate vulnerabilities to pathways into networks or election systems. Remote penetration testing focuses entirely on externally accessible systems. Remote penetration testing may include scenario-based external network penetration testing, external web application testing, and phishing campaign assessments.

[d]Phishing campaign assessments evaluate organizations' susceptibility and reaction to malicious emails of varying complexity.

[e]Last Mile posters are developed collaboratively by CISA and state or local election officials, and highlight efforts to strengthen election security. CISA is to work closely with election officials to tailor posters to the states' or localities' needs.

Selected Election Officials Are Generally Satisfied with DHS's Election Security Assistance and Identified Various Benefits and Challenges

State election officials with whom we spoke were generally satisfied with CISA's support to secure their election infrastructure. Specifically, officials from seven of the eight states we contacted said that they were very

satisfied with CISA's election-related work, while officials from the eighth state said that they were somewhat satisfied.[33]

Officials from five states told us that their relationship with CISA had improved markedly since early 2017, when the elections subsector was established.[34] For example, state officials said that CISA has made progress in this area. The Secretary of Homeland Security's designation of elections as critical infrastructure was initially controversial among state and local officials. For example, in February 2017, the National Association of Secretaries of State voted to oppose the designation of elections as critical infrastructure, citing the states' constitutional authority to regulate elections. In addition, CISA officials told us that a lack of trust and communication between DHS and state and local election officials hindered initial efforts to establish the Election Infrastructure Subsector. However, officials from one state told us that, despite initial reservations about DHS's role in election security, CISA has become a good partner over time. An official from another state expressed appreciation that CISA appears to be honestly and earnestly working to gain states' trust.

Officials representing the National Association of Secretaries of State and the National Association of State Election Directors also stated that CISA had worked to improve its relationships with state election officials. According to these officials, CISA has expanded outreach efforts by attending state association meetings and conferences to present information on CISA's resources and the threat environment and has impressed election officials with the level of detail provided by CISA's threat reporting. An official from the Election Center, which represents local election officials, stated that CISA officials attend every cybersecurity and critical infrastructure event hosted by the center. CISA officials stated that, while it is not possible to meet individually with all of the local election jurisdictions nationwide, it can engage with multiple local election jurisdictions at one time at these association conferences.

[33]We asked officials in each state to identify whether they were very satisfied, somewhat satisfied, or not satisfied with CISA's support to election security.

[34]Because we did not pose identical questions to each state's election officials, the absence of consensus around a given response should not be interpreted as disagreement. For example, while officials from five states said that their relationship with CISA had improved since 2017, no officials said that their state's relationship with CISA had degraded since 2017.

Selected State and Local Election Officials Reported Benefits from CISA's Efforts

Election officials from selected states and local jurisdictions cited various benefits from CISA's support to election security. According to officials from six states, CISA's involvement in election security has increased the officials' understanding of the threat environment that the election community faces. They also said that CISA's involvement has helped them to plan for cybersecurity threats and to prioritize their election security efforts. For example, officials from one state said that CISA recommended that the state set priorities and focus on risk assessments and network segmentation.

In addition, election officials from five states spoke highly of CISA's expertise and availability. The officials said, for example, that CISA regional and headquarters personnel were easy to get in touch with and knowledgeable about the election community. As a result, the officials said that they had better access to training opportunities and informal advice.

Further, officials from each of the eight states spoke positively about the information that the officials received from the EI-ISAC. For example, state officials said that the EI-ISAC updated them regularly on election security incidents and vulnerabilities nationwide, allowing them to prepare for potential incidents.

Officials also stated that the EI-ISAC presented the information in a way that was understandable to election administrators who may not have backgrounds in information technology. For example, in a monthly "spotlight" email, the EI-ISAC defines a key cybersecurity term and explains to the election officials why it should matter to them. One official told us that through membership in the EI-ISAC, the state has learned about election security best practices from other states, and other officials said that EI-ISAC allows them to maintain visibility of nationwide threats and other election security issues. Officials from one state said that their contacts through the EI-ISAC helped them to identify a point of contact at social media companies so that they could inform the companies about election-related misinformation being spread online.

In addition, election officials from two states said that they have encouraged or required local election jurisdictions to enroll in the EI-ISAC. According to EI-ISAC officials, the number of local election jurisdictions enrolled in the EI-ISAC increased from 1,384 at the end of 2018 to 2,267

in November 2019, and included all three election jurisdictions that we contacted. Officials from two of the three local jurisdictions said that the EI-ISAC emails were valuable. For example, election officials from one local jurisdiction said that communication from the EI-ISAC is meaningful and targeted to bolster their election security efforts. Election officials from the other jurisdiction said that they use the EI-ISAC information to improve their continuity of operations plans. On the other hand, officials from the third local jurisdiction said that the information provided in EI-ISAC emails was too general and not specific enough to their circumstances.

Election officials from five states also spoke positively of the EI-ISAC situational awareness chat rooms, which DHS hosted on its Homeland Security Information Network.[35] These officials stated that they participated in and monitored the chat rooms on Election Day to maintain awareness of any emergent election security issues nationwide. For example, officials from one state said that the chat rooms helped them receive real time notification of issues in other states and possible solutions to those issues.

In addition, as previously mentioned, one of CISA's major efforts was the 3-day tabletop exercises held in August 2018 and June 2019, which state and local officials were able to attend remotely by video teleconference from sites around the country. Elections officials from five states said that the exercises conveyed important information and prompted thoughtful discussions among state and local officials. Election officials from four states said that the exercises helped them build relationships within their states, and election officials from three states also said the exercises helped to build relationships with federal agencies as well. In addition, officials from four states said that they conducted or were planning to conduct tabletop exercises modeled on CISA's exercises.

Election officials from three states said that CISA's cybersecurity assistance has helped them to assure voters that elections in their states are secure or to promote election security efforts. For example, officials from one state said that, when they get questions from the public about election security, they tell voters that CISA's assessments have shown that the state's election systems are free of malicious code. Election

[35]The Homeland Security Information Network is DHS's official system for sharing sensitive but unclassified information between federal, state, local, territorial, tribal, international, and private sector partners.

officials from another state said that CISA officials' outspokenness has created opportunities for state officials to discuss the importance of election security issues with local officials. Additionally, officials from five states told us they encourage local election officials to request election security services from CISA to increase the security posture of the local jurisdictions.

Officials Cited Challenges Linked to DHS's Election Security Efforts

Even though state and local election officials provided mostly positive feedback on DHS's election security assistance, officials also identified two challenges linked to DHS's assistance efforts. First, officials from three states stated that it is challenging to find time to schedule election security services. For example, officials from one state said that their biggest challenge is to find time in their state's election schedule for receiving CISA services because the state has seven to nine elections in off years (that is, years without congressional or presidential elections). Officials from another state said that they might have requested additional election services from CISA if the state had more time in its election calendar. However, none of the state officials with whom we spoke attributed this difficulty to CISA, as election calendars are outside of CISA's control.

In commenting on this challenge, CISA officials said that they have tried to accommodate states' and local election jurisdictions' needs, when possible. For example, CISA started offering remote penetration testing as an alternative to the risk and vulnerability assessment.[36] The officials said that the two services are similar, but the remote penetration testing can be completed in fewer days and does not require CISA personnel to be physically present in the election offices. CISA officials told us that smaller jurisdictions sometimes prefer this option.

Election officials also identified an additional challenge related to the intelligence briefings that were provided by DHS's Office of Intelligence and Analysis for state and local officials with security clearances leading

[36]A remote penetration test uses a dedicated remote team to assess, identify, and mitigate vulnerabilities to pathways into networks or election systems. Remote penetration testing focuses entirely on externally accessible systems and may include scenario-based external network penetration testing, external web application testing, and phishing campaign assessments.

up to the 2018 elections.[37] According to Office of Intelligence and Analysis officials, the briefings allowed state and local officials to become more informed about the national threat picture, which in turn, allowed them to adjust to the threat more effectively.

Election officials from two states said that the intelligence briefings had provided helpful contextual information about cyber threats. However, election officials in two other states said that the briefings were not as useful as the election officials had hoped because the briefings only provided information that was already available publicly, and election officials from another state said that they learned about a significant election security issue possibly related to their state through news reports. For example, an election official from a different state said that the state learned about threats from the Department of Justice's July 2018 indictment against foreign intelligence officers.

CISA officials stated that they are aware of this issue and have been trying to improve the communication of intelligence information to state and local election officials. For example, at a October 2019 hearing of the House of Representatives Committee on Homeland Security, a CISA senior cybersecurity advisor testified that DHS has begun working with the Intelligence Community to rapidly declassify relevant intelligence or provide as much intelligence as possible, at the lowest classification level possible, to state and local election officials.

CISA officials also told us that the agency has started working with cybersecurity intelligence firms to provide election security information to state and local officials without the need for national security clearances or travel to secure facilities. According to CISA officials, two cybersecurity intelligence firms provided webinars to election officials in September and October 2019. CISA officials said that these firms have sophisticated capabilities that they use to analyze information that is not classified. As a result, the cybersecurity intelligence firms can more easily share information with states and local election jurisdictions. CISA officials said that state and local officials will benefit from these briefings because they provide actionable threat information to election officials without requiring them to have security clearances or travel to secure facilities.

[37]These briefings were provided in person or via secure video teleconferences around the country. According to DHS officials, the Office of Intelligence and Analysis provided 97 briefings to state and territorial election officials and 193 briefings to local election officials leading up to the 2018 elections.

CISA Has Not Finalized Its Plans to Address Key Objectives and Challenges

According to DHS planning guidance, strategic-level planning provides a framework for guiding homeland security activities and generates the objectives and priorities, which influence the roles, responsibilities, and actions that are detailed in the operational-level plans. Further, subsequent operational-level plans are to identify the tasks and resources needed to execute strategic plans.[38]

Prior GAO work has shown that strategic and operations plans can help further define capabilities, including opportunities to leverage resources. Such plans can also provide a roadmap for addressing identified gaps and better position an agency and its components to work collaboratively and strategically with external partners, such as states and local jurisdictions.[39]

CISA has begun developing strategic and operations plans for assisting states and local jurisdictions in securing election infrastructure in preparation for the 2020 elections. Specifically, CISA has developed a draft strategic plan for securing election infrastructure, known as the #Protect2020 Strategic Plan. According to the draft, CISA intends for its strategic plan to be used to achieve the high-level goals and outcomes called for in the agency's August 2019 Strategic Intent.[40] The draft strategic plan focuses on four areas, also referred to as lines of effort: (1) protecting election infrastructure, (2) supporting political campaigns, (3) raising public awareness on foreign influence threats and building resilience, and (4) sharing intelligence and identifying threats.

In addition, the draft strategic plan identifies several objectives for each line of effort. For example, it includes three objectives for the protecting election infrastructure line of effort:

[38]Department of Homeland Security, *National Planning System* (February 2016).

[39]GAO-18-562; GAO-17-300; GAO-15-602; GAO-05-372; and GAO-04-408T.

[40]CISA, *Strategic Intent*, August 2019. CISA's August 2019 Strategic Intent identified election security as one of five operational priorities for the agency and established a common framework of goals and high-level outcomes for this priority.

- building stakeholder capacity to manage risks and handle adversaries, through activities such as creating incident response and communication plans and encouraging states to adopt and practice them;
- providing technology services to stakeholders to monitor and secure their networks, by promoting the use of CISA's voluntary services and assessments, among other things; and
- facilitating information sharing between the federal government, private sector, and state and local partners by, among other things, hosting situational awareness chat rooms prior to, during, and after state and federal elections.

As another example, the draft strategic plan identifies three objectives for the sharing intelligence and identifying threats line of effort:

- partnering with private sector firms and vendors to improve cyber threat intelligence, through activities such as developing threat indicators and warnings;
- cooperating across federal partners—including federal law enforcement and the Intelligence Community—by, among other things, advocating for the creation of a joint memorandum to consolidate and highlight current knowledge on election threat intelligence; and
- monitoring threat activity through actions such as using network monitoring capabilities to spot malicious activity and reveal key trends.

In addition, CISA officials stated that the agency has begun developing a draft operations plan, known as the 2020 Election Security Operations Plan. This plan is to—in conjunction with the strategic plan—describe key organizational functions, processes, and resources employed to carry out the agency's efforts in support of elections in 2020. CISA officials stated, as of November 2019, that the agency intended to finalize the strategic and operations plans by January 2020.

However, as of January 2020, CISA's plans were not yet complete. According to a CISA official, the plans were not finalized due to an

ongoing reorganization within CISA and limited staffing resources within the Election Security Initiative.[41]

While CISA has drafted the strategic plan, the agency has not yet completed a draft of its operations plan. CISA officials have noted the importance of the operations plan to help ensure the agency is adequately prepared to support election officials in securing election infrastructure in advance of elections, which begin with presidential primaries in February 2020, as well as subsequent primaries leading up to the November 2020 general election.

Further, CISA's operations plan may not fully address the four lines of effort 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 strategic plan's lines of effort—protecting election infrastructure and sharing intelligence and identifying threats. However, agency officials did not identify the extent to which the operations plan would address all of the objectives from these lines of effort in the strategic plan.

CISA officials also stated that the agency is 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. The officials stated that, given the limited amount of time remaining before election preparation activities commence, the agency decided to prioritize developing a plan for the first line of effort that addresses the primary customers of the agency's election services. In the absence of completed strategic and operations plans, a CISA official in one region stated in October 2019 that the region is moving forward with its own strategy for assisting states and local jurisdictions because the 2020 election cycle is scheduled to start with state primary elections in the region in March 2020.

The lack of finalized plans can affect CISA's achievement of higher-level objectives that take time to accomplish, such as building stakeholder capacity and public awareness. Until CISA finalizes its strategic and

[41]The agency intends to reorganize several of the functions within its headquarters and field operations, including those that support election security, to a new division. The details of the reorganization were not available for this review as they were still under deliberation within DHS, CISA, and the Congress. We have ongoing work examining the reorganization efforts of CISA.

operations plans for supporting elections in 2020 and ensures that the operations plan fully addresses all of the aspects of its strategic plan, CISA will not be well-positioned to execute a nationwide strategy for securing election infrastructure prior to the start of 2020 election activities.

CISA Identified Challenges Related to Its Efforts to Secure Election Infrastructure, but Has Not Documented How It Intends to Address Them

DHS's National Infrastructure Protection Plan, which provides strategic direction for national, critical infrastructure protection efforts, calls for sector-specific agencies to coordinate lessons learned and corrective actions and rapidly incorporate them to improve future efforts.[42] Further, GAO's *Standards for Internal Control* calls for management to document corrective action plans to remediate internal control deficiencies in a timely manner following the reporting and evaluation of issues.[43]

CISA has identified various challenges related to its election assistance efforts; however, the agency has not yet documented plans that address them. Following the 2018 midterm elections, CISA and the RAND Corporation conducted two reviews of CISA's efforts supporting the elections, in order to inform strategic planning and strengthen future operations. The first review, conducted by the RAND Corporation under a contract with DHS, assessed election security operations that CISA undertook from January 2017 through the November 2018 midterm elections.[44] The review relied upon input from DHS personnel, the EI-ISAC, associations representing state election officials, and election system vendors to identify lessons learned from CISA's activities to assist in securing election infrastructure. In the second review, CISA conducted an after action review covering its efforts to assist in securing election infrastructure from September 2018 to December 2018, based on input

[42]Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

[43]GAO-14-704G.

[44]Benjamin Boudreaux, Quentin E. Hodgson, Edward Chan, *Quick Look: Elections Security Lessons Learned from the 2017-2018 Election Cycle*, Homeland Security Operational Analysis Center operated by the RAND Corporation, April 2019.

from personnel within DHS and its federal partners who participated in the agency's election security operations.[45]

Both reviews identified various challenges that CISA needed to address in its planning for 2020. For example, the RAND review cited challenges related to the services and threat briefings CISA provided to states and local jurisdictions. The review noted, among other things, that CISA:

- lacked an approach for prioritizing its activities based on election security risks, which could limit the agency's ability to dedicate increased attention and resources to the jurisdictions with the highest risk;
- did not adequately tailor services, which could have made it more difficult to meet the resource and time constraints of customers such as local election jurisdictions; and
- did not always provide actionable recommendations in DHS classified threat briefings or make 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.

Additionally, the CISA after action report identified a number of internal operational challenges associated with its election-related efforts in 2018. For example, the report cited:

- a lack of understanding by CISA headquarters staff of the roles and functions of regional field staff, which led to redundant requests for information from headquarters staff to regional staff;
- the lack of a single agency-wide platform to maintain an awareness of election threats, which resulted in confusion among CISA personnel about which threat information was accurate and current; and
- 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.

Further, both reviews cited challenges regarding CISA's ability to manage incident information and provide Election Day incident response

[45]Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *2018 Midterm Elections Security Operations After Action Report*, DRAFT (Washington, D.C.: April 2019). As of November 2019, the after action report has not been finalized and remains in draft form.

capabilities in the event of a compromise. For example, with regards to the 2018 election, the reviews noted:

- few capabilities that CISA field staff could quickly provide on Election Day, which could limit the agency's timeliness in mitigating or responding to an incident;
- 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; and
- a lack of outreach and situational reporting on incidents, threats, and trends on Election Day from headquarters to regional staff following the closure of the polls on the East Coast, which hindered CISA's coordination of such information with state and local officials.

While CISA identified challenges related to its prior efforts, it has not developed plans to address them. According to a CISA official, the agency does not intend to develop a separate plan addressing how it will remediate the identified challenges in the RAND report. Rather, CISA officials noted that the agency plans to address the challenges from that report in the strategic plan and operations plan that it is developing. In addition, the officials noted that CISA may address challenges through other actions that the agency expects to take, such as hiring additional staff.

However, CISA's draft strategic plan, as of November 2019, had only addressed three challenges from the RAND report—countering the threat of disinformation, clarifying how CISA is to support political campaigns, and prioritizing outreach to local jurisdictions. The extent to which the strategic plan, when finalized, will address the other outstanding challenges remains unclear. In addition, the extent to which the operations plan will document how the agency is to address challenges in the RAND report remains uncertain as the operations plan has not yet been completed. Further, CISA has not documented how the agency is to address challenges in the RAND report through other actions that it expects to take before the 2020 elections.

Similarly, CISA officials stated that the agency intends to address a subset of the challenges from CISA's after action report in its anticipated operations plan. However, the extent to which the operations plan will document how the agency is to address challenges in the after action report remains unclear, given that the operations plan has not yet been completed.

Without documented plans that address prior challenges, CISA will not be well-positioned to effectively address the challenges identified in prior reviews. This includes addressing how CISA will coordinate among its personnel and provide accurate threat information and other capabilities that address the needs of the election infrastructure community in the remaining months ahead of the 2020 elections.

Conclusions

With primary elections beginning in February 2020 and culminating in the general election in November 2020, CISA has limited time remaining to help states and local election jurisdictions protect their election infrastructure in advance of these elections. State and local election officials that we contacted have been generally satisfied with CISA's election security efforts. However, CISA's unfinished planning means the agency may be limited in its ability to execute a nationwide strategy for securing election infrastructure. In particular, the #Protect2020 Strategic Plan's higher-level objectives—such as building stakeholder capacity and public awareness—necessarily take time to accomplish. In addition, CISA has not fully assessed and documented how it will address challenges identified in prior assessments, which limits the ability of CISA to address these challenges in its current efforts.

Recommendations for Executive Action

We are making three recommendations to the Director of the Cybersecurity and Infrastructure Security Agency:

- The CISA Director should urgently finalize the strategic plan and the supporting operations plan for securing election infrastructure for the upcoming elections. (Recommendation 1)
- The CISA Director should ensure that the operations plan fully addresses all lines of effort in the strategic plan for securing election infrastructure for the upcoming elections. (Recommendation 2)
- The CISA Director should 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. (Recommendation 3)

Agency Comments and Our Evaluation

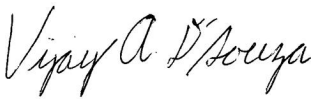
DHS provided written comments on a draft of this report, which are reprinted in appendix III. In its comments, the department concurred with all three of our recommendations and identified actions that it plans to take to implement each of the recommendations.

For example, the department stated that CISA intends to finalize its strategic and operations plans by February 14, 2020. The department noted that these plans are to provide a strategic overview and operational framework in support of the primaries and the general election in 2020. Further, the department stated that the operations plan, when finalized, is to address all lines of effort in the strategic plan. In addition, the department noted that both the strategic and operations plans are to further document DHS's plans to address challenges identified during the 2017-2018 election cycle. If implemented effectively, the actions that DHS plans to take in response to the recommendations should address the weaknesses that we identified during our review.

DHS and CISA officials also provided technical comments, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Acting Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Vijay A. D'Souza, Director, Information Technology and Cybersecurity, at (202) 512-6240 or dsouzav@gao.gov or Rebecca Gambler, Director, Homeland Security and Justice, at (202) 512-8777 or gamblerr@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



Vijay A. D'Souza
Director, Information Technology and Cybersecurity

Rebecca Gambler
Director, Homeland Security and Justice

Appendix I: Sources of Cybersecurity Threats to the Election Infrastructure

The election process relies on various assets—such as information technology systems, networks, equipment, and facilities—that can be broadly categorized as physical, cyber, and human components of the Election Infrastructure Subsector. The assets and components of the election infrastructure are susceptible to a variety of unintentional, or nonadversarial, and intentional, or adversarial, threats. The table below identifies sources of cybersecurity threats to election infrastructure.

Table 3: Sources of Cybersecurity Threats to the Election Infrastructure

Source	Description
Nonadversarial/nonmalicious	
Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications.
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies.
Failure in software	Failures in operating systems, networking, and general-purpose and mission-specific applications.
Natural or manmade disasters	Events beyond an entity's control such as fires, floods, tsunamis, tornados, hurricanes, and earthquakes.
Unusual natural events	Natural events beyond the entity's control that are not considered disasters (e.g., sunspots).
Infrastructure failures or outages	Failures or outages of telecommunications or electrical power.
Unintentional user errors	Failures resulting from accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities.

Source	Description
Adversarial/malicious	
Hackers/hacktivists	Hackers who break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists, or ideologically motivated actors who take advantage of cyber vulnerabilities to further political goals.
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) whose position within the organization allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. These individuals engage in purely malicious activities and should not be confused with nonmalicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs that use cyber tools as part of their information-gathering and espionage activities.
Criminal groups and organized crime	Criminal groups who seek to attack systems for monetary gain. Specifically, organized criminal groups that leverage cyber vulnerabilities to commit identity theft, online fraud, and computer extortion.
Terrorists	Terrorists who seek to destroy, incapacitate, or purposefully misuse critical infrastructures in order to threaten national security, weaken the economy, and damage public morale and confidence.
Unknown malicious outsiders	Threat sources/agents who, due to their success in remaining anonymous, are unable to be classified as one of the five types of threat sources/agents listed above.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center. | GAO-20-267

Appendix II: Voluntary Services for the Election Infrastructure Subsector Provided by CISA

The Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA), has taken steps to assist state and local election officials in securing election infrastructure by providing a variety of services on a voluntary, no cost basis. These services include cybersecurity assessments, detection and prevention activities, and information sharing. The table below identifies voluntary services that CISA offers to states and local election jurisdictions.

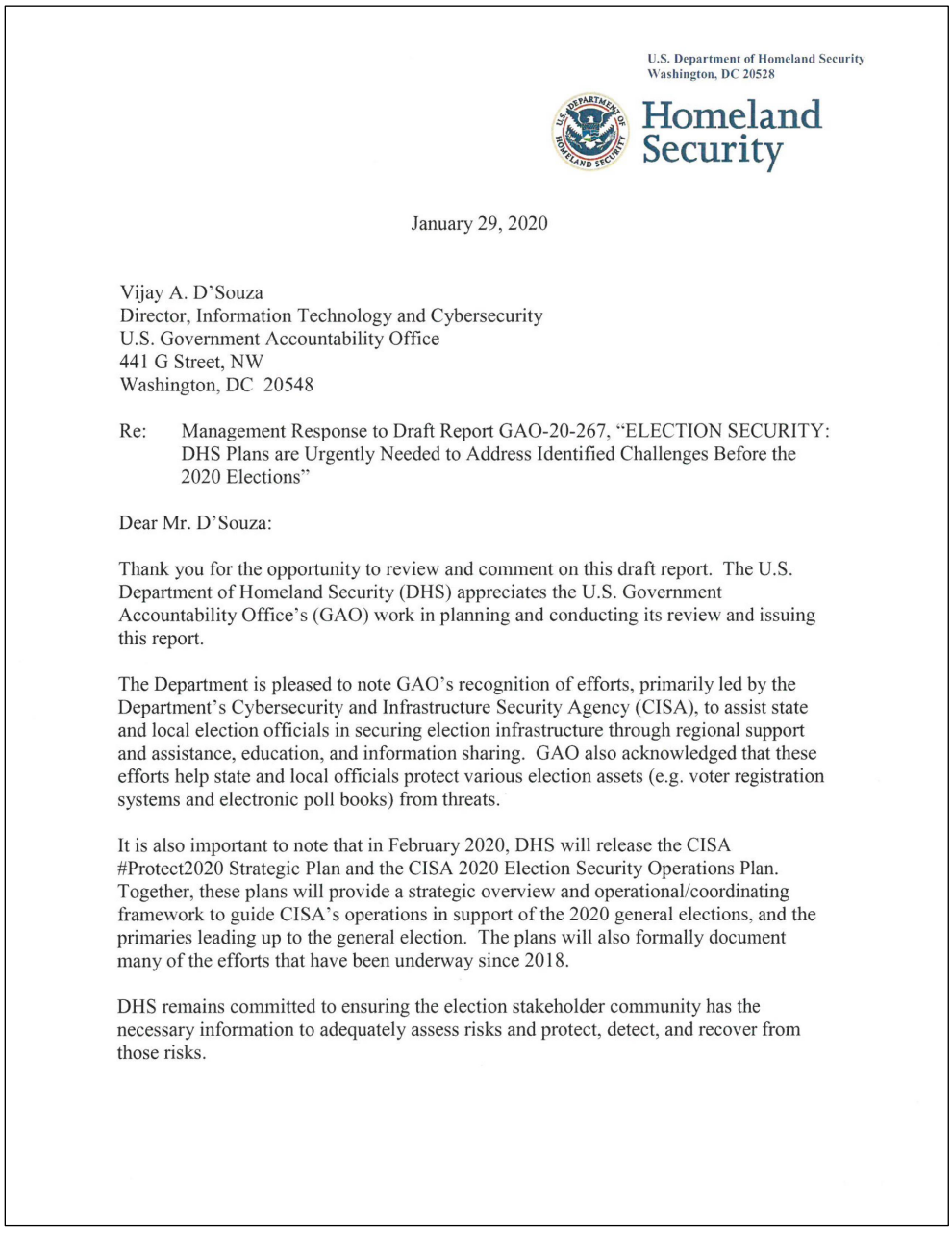
Table 4: List of Voluntary Services for the Election Infrastructure Subsector Provided by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)

Service	Description
Cybersecurity assessments	
Cyber resilience review	An assessment that evaluates the maturity of state or local jurisdiction capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities.
External dependencies management assessment	An assessment to evaluate a state's or local jurisdiction's management of its external dependencies, such as services and facilities provided by a vendor or third party. Through the external dependencies management assessments, election officials can learn how to manage risks arising from dependencies within the information and communication technology supply chain.
Cyber infrastructure survey	A survey evaluating the effectiveness of the state's or local jurisdiction's security controls, cybersecurity preparedness, and overall cyber resilience. The organization's critical cybersecurity services are assessed against more than 80 cybersecurity standards grouped in five areas: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.
Phishing campaign assessment	An assessment evaluating a state's or local jurisdiction's susceptibility and reaction to malicious emails of varying complexity.
Risk and vulnerability assessment	An assessment identifying vulnerabilities that adversaries could leverage to compromise network security controls. A risk and vulnerability assessment may include the following methodologies: scenario-based network penetration testing, web application testing, wireless testing, configuration reviews of servers and databases, and detection and response capability evaluation.

Service	Description
Remote penetration testing	A remote penetration test uses a dedicated remote team to assess, identify, and mitigate vulnerabilities to pathways into networks or election systems. Remote penetration testing focuses entirely on externally accessible systems. Remote penetration testing may include scenario-based external network penetration testing, external web application testing, and phishing campaign assessments.
Vulnerability scanning	A service that scans internet-accessible systems for known vulnerabilities on a continual basis. As CISA identifies potential vulnerabilities, it is to notify the affected organization so that pre-emptive risk mitigation efforts can be implemented to avert vulnerability exploitation.
Validated architecture design review	A review of system architecture and design, system configuration, and log files as well as analysis of the organization's network traffic to develop a detailed picture of the communications, flows, and relationships between devices and, thus, identify anomalous communication flows.
Cyber security evaluation tool	A desktop application that guides asset owners and operators through a systematic process of evaluating operational technology and information technology.
Detection and prevention	
Continuous diagnostics and mitigation program	The continuous diagnostics and mitigation program identifies a state's or local jurisdiction's cybersecurity risks and alerts personnel to mitigate significant problems first based on potential impact. Continuous diagnostics and mitigation capabilities assist states' or localities' network administrators in understanding their respective networks' security posture.
Enhanced cybersecurity services	The enhanced cybersecurity services facilitate protection of a state's or local jurisdiction's networks by offering intrusion detection and prevention services through approved service providers. The program shares sensitive and classified cyber threat information with accredited service providers who use the information to block malicious traffic from entering customer networks.
Hunt and incident response team	The hunt and incident response team provides incident response, management, and coordination activities for cyber incidents occurring in the critical infrastructure sector. The team works with states or local jurisdictions to identify and contain adversary activity and develop mitigation plans for removal and remediation of the root cause of the incident.
Advanced malware analysis center	A facility offering continuous analysis of malicious code. States or local jurisdictions submit samples through a website and receive a technical document outlining analysis results and detailed recommendations for malware removal and recovery activities.
Information sharing	
Automated indicator sharing	A platform that enables states or local jurisdictions to exchange cyber threat indicators between the federal government, state, local, tribal, and territorial governments, and the private sector.
Homeland Security Information Network	A trusted network for states or local jurisdictions to share sensitive but unclassified information. The Homeland Security Information Network shares information products over the network using the traffic light protocol, which is a set of designations used to facilitate greater sharing of sensitive information with the appropriate audience.
National Cyber Awareness System	CISA designed a system for making information available to organizations to improve situational awareness among technical and non-technical audiences by providing timely information about cybersecurity threats and general security topics. The information includes technical alerts, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices.
Last Mile posters	CISA collaborates with state or local election officials to create 20 inch by 30 inch posters highlighting efforts to strengthen election security, called Last Mile posters. CISA is to work closely with election officials to tailor posters to the states' or localities' needs.

Source: GAO analysis of CISA information. | GAO-20-267

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

January 29, 2020

Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-267, "ELECTION SECURITY: DHS Plans are Urgently Needed to Address Identified Challenges Before the 2020 Elections"

Dear Mr. D'Souza:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of efforts, primarily led by the Department's Cybersecurity and Infrastructure Security Agency (CISA), to assist state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing. GAO also acknowledged that these efforts help state and local officials protect various election assets (e.g. voter registration systems and electronic poll books) from threats.

It is also important to note that in February 2020, DHS will release the CISA #Protect2020 Strategic Plan and the CISA 2020 Election Security Operations Plan. Together, these plans will provide a strategic overview and operational/coordinating framework to guide CISA's operations in support of the 2020 general elections, and the primaries leading up to the general election. The plans will also formally document many of the efforts that have been underway since 2018.

DHS remains committed to ensuring the election stakeholder community has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

The draft report contained three recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-20-267

GAO recommended that the CISA Director:

Recommendation 1: Urgently finalize the strategic plan and the supporting operations plan for securing election infrastructure for the upcoming elections.

Response: Concur. By February 14, 2020, CISA's National Risk Management Center (NRMC) expects to finalize the #Protect2020 Strategic Plan and CISA's integrated operations function will release the 2020 Election Security Operations Plan, both of which address the need for documentation of the Department's strategic and operational plans to address challenges identified through the 2017-2018 election cycle. Together, these plans will provide a strategic overview and operational/coordinating framework to guide CISA's operations in support of the primaries and the 2020 general election. Estimated Completion Date (ECD): February 14, 2020.

Recommendation 2: Ensure that the operations plan fully addresses all lines of effort in the strategic plan for securing election infrastructure for the upcoming elections.

Response: Concur. When finalized in February 2020, the 2020 Election Security Operations Plan will address all lines of effort in the #Protect2020 Strategic Plan. ECD: February 14, 2020.

Recommendation 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.

Response: Concur. CISA addressed a number of remedial actions identified in a report entitled, "The Homeland Security Operational Analysis Center (HSOAC) Quick Look: Security Lessons Learned from the 2017-2018 Election Cycle, dated April 2019." In particular, this report addresses a series of "Needs Going Forward," which will be further documented in the finalized #Protect2020 Strategic Plan and 2020 Election Security Operations Plan.

The Election Infrastructure Subsector Government Coordinating Council and Election Infrastructure Subsector Coordinating Council also expect to publish an updated Election Infrastructure Subsector-Specific Plan (SSP) by January 31, 2020. This document will guide the voluntary, collaborative election security efforts of election officials and the private sector organizations that provide services, systems, or technology that supports the election administration process through 2020 and beyond. As the Sector-Specific

Agency for the Election Infrastructure Subsector, CISA will play a key role in supporting efforts to accomplish the SSP goals and objectives. ECD: February 14, 2020.

4

Agency Comment Letter

Text of Appendix III: Comments from the Department of Homeland Security

Page 1

January 29, 2020

Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-267, "ELECTIONSECURITY: DHS Plans are Urgently Needed to Address Identified Challenges Before the 2020 Elections"

Dear Mr. D' Souza:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Goverm11ent Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of efforts, primarily led by the Department's Cybersecurity and Infrastructure Security Agency (CISA), to assist state and local election officials in securing election infrastructure through regional support and assistance, education, and information sharing. GAO also acknowledged that these efforts help state and local officials protect various election assets (e.g. voter registration systems and electronic poll books) from threats.

It is also important to note that in February 2020, DHS will release the CISA #Protect2020 Strategic Plan and the CISA 2020 Election Security Operations Plan. Together, these plans will provide a strategic overview and operational/coordinating framework to guide CISA's operations in support of the 2020 general elections, and the primaries leading up to the general election. The plans will also formally document many of the efforts that have been underway since 2018.

DHS remains committed to ensuring the election stakeholder community has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

Page 2

The draft report contained three recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE

Director
Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GAO-20-267

GAO recommended that the CISA Director:

Recommendation 1:

Urgently finalize the strategic plan and the suppo1iing operations plan for securing election infrastructure for the upcoming elections.

Response: Concur. By February 14, 2020, CISA' s National Risk Management Center (NRMC) expects to finalize the #Protect2020 Strategic Plan and CISA's integrated operations function will release the 2020 Election Security Operations Plan, both of which address the need for documentation of the Department's strategic and operational plans to address challenges identified through the 2017-2018 election cycle. Together, these plans will provide a strategic overview and operational/coordinating framework to guide CISA's operations in support of the primaries and the 2020 general election.

Estimated Completion Date (ECO): February 14, 2020.

Recommendation 2:

Ensure that the operations plan fully addresses all lines of effort in the strategic plan for securing election infrastructure for the upcoming elections.

Response: Concur. When finalized in February 2020, the 2020 Election Security Operations Plan will address all lines of effort in the #Protect2020 Strategic Plan. ECO: February 14, 2020.

Recommendation 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.

Response: Concur. CISA addressed a number of remedial actions identified in a report entitled, "The Homeland Security Operational Analysis Center (HSOAC) Quick Look: Security Lessons Learned from the 2017-2018 Election Cycle, dated April 2019." In particular, this report addresses a series of "Needs Going Forward," which will be further documented in the finalized #Protect2020 Strategic Plan and 2020 Election Security Operations Plan.

The Election Infrastructure Subsector Government Coordinating Council and Election Infrastructure Subsector Coordinating Council also expect to publish an updated Election Infrastructure Subsector-Specific Plan (SSP) by January 31, 2020. This document will guide the voluntary, collaborative election security efforts of election officials and the private sector organizations that provide services, systems, or technology that supports the election administration process through 2020 and beyond. As the Sector-Specific Agency for the Election Infrastructure Subsector, CISA will play a key role in supporting efforts to accomplish the SSP goals and objectives. ECD: February 14, 2020.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contacts

Vijay A. D'Souza, (202) 512-6240, dsouzav@gao.gov

Rebecca Gambler, (202) 512-8777, gamblerr@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Josh Leiling (Assistant Director), Tom Jessor (Assistant Director), Torrey Hardee (Analyst-in-Charge), Roger Bracy, Rebecca Eyler, Richard Hung, Amanda Miller, Heidi Nielson, Monica Perez-Nelson, Jeff Tessin, Eric Warren, and Haley Weller made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548