OFFICE OF INSPECTOR GENERAL

DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure

Homeland Security

October 22, 2020

OIG-21-01

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

October 22, 2020

MEMORANDUM FOR: The Honorable Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2020.10.21 18:59:03 -04'00'

SUBJECT: *DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure*

Attached for your action is our final report, *DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at enhancing the coordination efforts to secure the election infrastructure. The Department concurred with all three recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may review the recommendations for closure. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to the congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sondra McCauley Assistant Inspector General, Office of Audits, at (202) 981-6000.

DHS OIG HIGHLIGHTS

DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure

October 22, 2020

Why We Did This Audit

The election process is a cornerstone of American democracy. Prompted by suspicious cyber activities on election systems in 2016, the DHS Secretary designated the election infrastructure as a subsector to one of the Nation's 16 existing critical sectors. We conducted this audit to determine the effectiveness of DHS' coordination efforts to secure the election infrastructure since our last report in 2019.

What We Recommend

We are recommending that CISA revise planning documents to address risks, improve information sharing, and conduct timely assessments to better secure the election infrastructure.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

DHS has improved coordination efforts to secure the Nation's systems used for voting, but should take additional steps to protect the broader election infrastructure, which includes polling and voting locations and related storage facilities, among other things. The Cybersecurity and Infrastructure Security Agency (CISA) has developed a set of plans and guidance aimed at securing election systems for the 2020 election cycle. But, the plans do not sufficiently mitigate other potential risks to physical security, terrorism threats, or targeted violence to the election infrastructure, nor do they identify dependencies on external stakeholders that impede mission performance. DHS senior leadership turnover and ongoing CISA reorganization have hindered CISA's ability to enhance planning and effectively monitor its progress in securing the Nation's election infrastructure.

Since our 2019 report, CISA has increased its outreach and coordination with election stakeholders. CISA can further improve the quality of information shared, as well as the timeliness of its assistance to election stakeholders. Inadequate classification authority, duplicative data sharing, and limited staffing have restricted CISA's ability to provide additional services and assessments. With the 2020 elections at hand and increased potential for revised election processes due to the COVID-19 pandemic, it is critical that CISA institute a well-coordinated approach and provide the guidance and assistance necessary to secure the Nation's election infrastructure.

Management Response

CISA concurred with all three of our recommendations. We included a copy of CISA's response in its entirety in Appendix B.

Table of Contents

Background 1

Results of Audit 7

DHS Has Not Adequately Addressed Physical Security Risks to the Election Infrastructure 7

CISA Has Increased Assistance to Election Stakeholders, but Improvements Are Needed 14

Recommendations 28

Appendixes

Appendix A: Objective, Scope, and Methodology 31
Appendix B: Management Comments to the Draft Report 33
Appendix C: Technology Audits and Analytics Support Major Contributors to This Report 37
Appendix D: Report Distribution 38

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DRE	Direct Recording Electronic
I&A	Office of Intelligence and Analysis
IT	Information Technology
OIG	Office of Inspector General
NCCIC	National Cybersecurity and Communications Integration Center

Background

A secure election process is vital to our national interest and U.S. democracy. The American people's confidence in the security and resilience of the election infrastructure is also central to the voting process. On October 1, 2016, former Department of Homeland Security Secretary Jeh Johnson stated that malicious cyber actors had been scanning a large number of state election systems, which could be a preamble to attempted intrusions. In a few cases, DHS determined that malicious actors gained access to state voting-related systems, although the Department was not aware of any manipulation of data at that time.[1]

The suspicious activities and potential attacks during the 2016 Presidential election were later attributed to Russian hackers targeting voter registration files and public election sites — mostly through scanning for vulnerabilities — in 21 states. In July 2018, the Department of Justice indicted 12 Russian nationals for allegedly hacking the election infrastructure and stealing personal information for about 500,000 voters.[2]

On October 7, 2016, DHS and the Office of the Director of National Intelligence released a joint statement on election security urging state and local governments to be vigilant and seek cybersecurity assistance from the Department. The joint statement illustrated the importance of, and need for, coordinated effort among state election officials and the Federal government to safeguard the Nation's election infrastructure.

While it has been almost 4 years since the Russian operatives allegedly targeted our election systems in 2016, foreign adversaries continue to aim to influence our election process. On June 4, 2020, a major search engine confirmed that foreign adversaries were still targeting campaign staff of both political parties before the 2020 Presidential election.

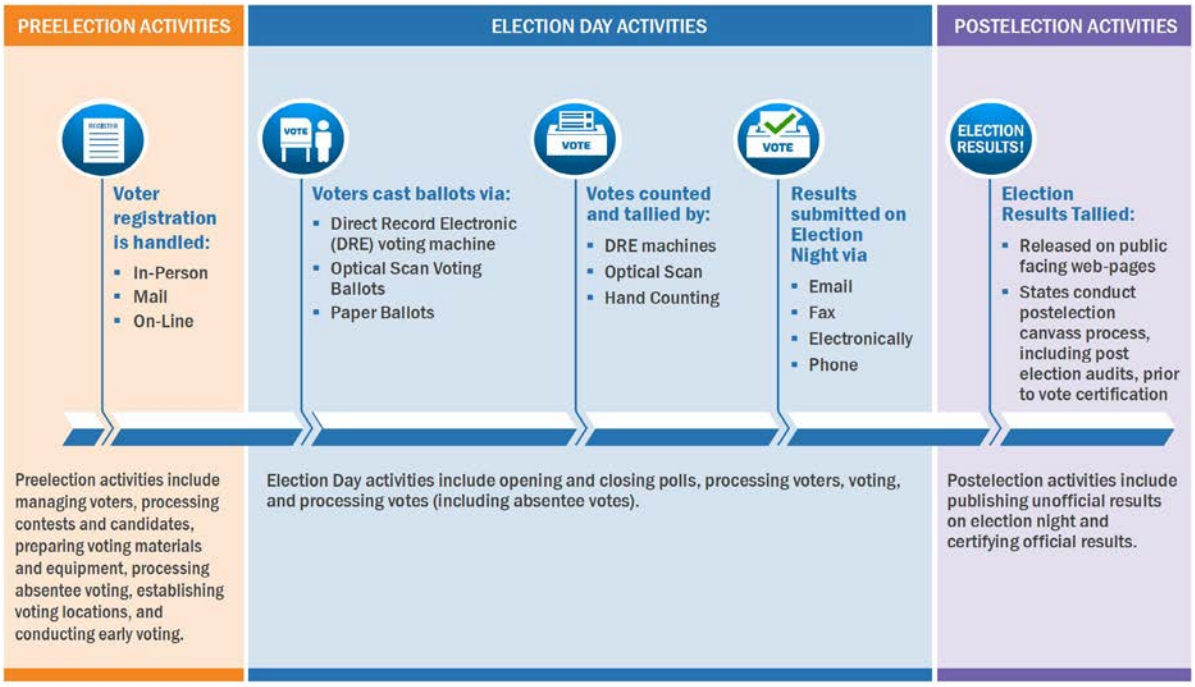
U.S. Electoral Process

Our Nation's election process includes pre-election, Election Day, and post-election activities. Figure 1 shows the phases of this process.

---

[1] Statement from Jeh Johnson before the House Permanent Select Committee on Intelligence, June 21, 2017.
[2] NPR, *Justice Department Charges Russian Cyberspies With Attack On 2016 Election*, July 13, 2018, https://www.npr.org/2018/07/13/628773789/deputy-attorney-general-rod-rosenstein-unveils-new-hacking-charges-in-dnc-case.

Figure 1. U.S. Electoral Process



Source: U.S. Electoral Process Infographic[3]

As illustrated in Figure 1, during the pre-election phase, qualified voters are registered to vote either in-person, by mail, or online. Election officials may perform the following tasks: (1) process candidates' materials for elections, (2) prepare ballots, (3) perform logic checks and accuracy validation on voting equipment, and (4) establish voting locations and timetables for early and absentee voting.

Election Day activities involve opening and closing polls, ballot casting, vote counting and tallying, and submission of results. Ballots are cast by voters and scanned using various election equipment. Election officials submit results via email, fax, phone, or electronically to the states' chief election officials.[4]

Post-election activities begin with tallying votes then submission and publication of unofficial election results. Once the votes are counted, election officials release unofficial results to the public via public web pages and other

[3] *U.S. Electoral Process Infographic,* obtained from: https://www.dhs.gov/topic/election-security.
[4] States may include all 50 states, the District of Columbia, and U.S. territories.

media. Additionally, election officials may perform audits to confirm the proper functionality of voting machines and/or verify the accuracy of reported results. Ultimately, election officials certify the results. In most states, election officials are obligated by statute to post the certified results on websites, in polling places, by newspaper, or at courthouses.

U.S. Election Infrastructure

State and local governments manage the complex mix of people, processes, and technology that make up our Nation's election infrastructure. The Constitution and Federal voting rights laws[5] grant states broad latitude in how they administer Federal general elections, which occur every 2 years in November. Few states administer elections in exactly the same manner. While elections are usually administered at the county level, in some states, cities or townships manage elections. As of September 2020, according to the Cybersecurity and Infrastructure Security Agency (CISA), there were 7,997 election administration jurisdictions in the country. The sizes of these jurisdictions vary dramatically, with the smallest towns having only a few hundred registered voters, while the largest jurisdiction in the country has more than 4.7 million.[6]

The diversity in voting systems and software across the Nation presents considerable cybersecurity challenges. For example, there are 67 different types of voting machines manufactured by 7 different companies currently certified for use in any of the election administration jurisdictions across the United States.[7] The election infrastructure's reliance on technology for efficiency and convenience introduces even greater cybersecurity risks. Moreover, state and local jurisdictions may have different requirements for securing their systems, such as configuration settings, audit logging, intrusion detection capability, and patch management.

Computer-enabled election systems may be subject to cyber intrusion. The risks to computer-enabled election systems vary by county and jurisdiction, depending upon the types of devices, network architectures, information technology (IT) governance measures, and other protective measures implemented. For example, election infrastructure elements that are potentially vulnerable to cyber and physical intrusion include:

---

[5] The White House, *Our Government, Elections and Voting,* https://www.whitehouse.gov/about-the-white-house/elections-voting/.
[6] *Election Administration at State and Local Levels*, National Conference of State Legislatures, February 3, 2020.
[7] According to information found on the U.S. Election Assistance Commission's website https://www.eac.gov/voting-equipment/certified-voting-systems.

- Electronic Voting Systems – In laboratory testing environments, security researchers have repeatedly demonstrated that some voting machines are vulnerable to compromise, usually due to physical access to the machines, which could result in the manipulation of vote totals.
- Voter Registration Databases – Online voter registration systems may be vulnerable to cyber attackers seeking to gain unlawful access to voter registration databases.
- Public Dissemination of Voting Results – State governments' information technology solutions generally include public internet connections to disseminate election results to the public and media on Election Day. Public internet use could result in inaccurate reporting on numbers of votes.

DHS' Responsibility for Securing the Nation's Election Infrastructure

DHS is the lead Federal agency for supporting critical infrastructure security and resilience. Within DHS, CISA leads coordination efforts to manage risks to the Nation's 16 critical infrastructure sectors.[8] The election infrastructure is a subsector of the Government Facilities Sector,[9] which includes a wide variety of buildings located in the United States and overseas, owned or leased by Federal, state, local, or tribal governments. Examples of these facilities include general use office buildings, special-use military installations, embassies, courthouses, and national laboratories.

On January 6, 2017, former Secretary Jeh Johnson designated the election infrastructure, which is organized as a subsector of the Government Facilities sector under DHS' purview.[10] In his designation, Secretary Johnson recognized that the election infrastructure is vital to our national interest, cyberattacks on this country are becoming more sophisticated and bad cyber actors — ranging from nation states to cyber criminals and hacktivists — are

[8] The Nation's 16 critical infrastructure sectors include systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
[9] The remaining 15 critical infrastructure sectors include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.
[10] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, designates DHS and the General Services Administration as co-Sector Specific Agencies responsible for the Government Facilities Sector.

becoming more dangerous. Former Secretary John Kelly subsequently affirmed the designation during a congressional hearing in June 2017. The election infrastructure includes the following:

- voter registration databases and associated IT systems;
- IT networks, systems, and equipment used to manage elections (such as counting, auditing, and displaying election results, as well as post-election reporting to certify and validate results);
- voting systems and associated infrastructure;
- related storage facilities; and
- polling places, including early voting locations.

CISA's Election Services

CISA aims to work collaboratively with those on the front lines of elections — state and local governments, election officials, Federal partners, and vendors — to manage risks to the Nation's election infrastructure. In December 2018, CISA dissolved the Election Task Force and formally established the Election Security Initiative within the National Risk Management Center.[11] According to CISA, the Election Security Initiative assists state and local partners in identifying and addressing risks to election infrastructure through a variety of means, such as sharing information, offering training, conducting risk assessments, and facilitating the delivery of CISA capabilities like vulnerability assessments, exercises, and incident response.

While the ultimate responsibility for administering the Nation's elections rests with state and local governments, CISA offers a variety of services and resources to assist them upon request. Some of CISA's general offerings include:

- Cybersecurity Assessments – CISA provides a range of cybersecurity assessments[12] to evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA's cybersecurity

[11] The Election Task Force was created in 2017 to centralize the coordination of the Department's assistance to state and local governments with their election infrastructure.
[12] CISA's Cybersecurity Advisors, Protective Security Advisors, and the National Cybersecurity and Communications Integration Center conduct assessments using the same cyber and physical security assessment templates for all 16 critical sectors.

assessment services are offered solely on a voluntary basis and are available upon request.

- Detection and Prevention – CISA rapidly notifies relevant critical infrastructure stakeholders of elevated risk exposure, conducts incident management operations, provides vulnerability assessments, and directly deploys risk management information, tools, and technical services to mitigate risk.
- Information Sharing and Awareness – In coordination with DHS' Office of Intelligence and Analysis (I&A), and several Federal partners, CISA provides information about emerging threats so that stakeholders can take appropriate actions to mitigate potential risks.[13]
- Tools and Training – DHS offers tools and training to help election stakeholders to reduce risk. This includes "Last Mile" posters, which are scalable, customizable tools to help inform election stakeholders of their risks and how to reduce them. CISA's tabletop exercises include scenarios and discussion questions to address potential threats to the election stakeholder's infrastructure.

Prior Office of Inspector General Reporting

In February 2019, we reported that DHS had taken some steps to mitigate risks to the Nation's election infrastructure, but still needed to improve planning, increase staffing, and provide clearer guidance to facilitate its coordination with states.[14] Specifically, despite Federal requirements, DHS had not completed the plans and strategies critical to identifying emerging threats and mitigation activities, and establishing metrics to measure progress in securing the election infrastructure. While DHS provided assistance to state and local election officials upon request, we found that staff shortages, a lengthy security clearance process, and state and local officials' historic mistrust of Federal government assistance restricted DHS efforts to provide the services and assessments needed to secure the election infrastructure. As of April 2020, all five recommendations cited in the report had been closed because DHS provided evidence of: (1) progress made to increase the Election Security Initiative staff from 8 to 22, (2) increased Election Infrastructure Information Sharing and Analysis Center enrollment, and (3) recording lessons learned reports and exercise after action plans.

[13] Federal partners include, but are not limited to, the Department of Justice's Federal Bureau of Investigation, the U.S. Election Assistance Commission, the National Security Agency, and the Office of the Director of National Intelligence.
[14] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, OIG-19-24, February 28, 2019.

We conducted this audit to evaluate the effectiveness of CISA's efforts to coordinate with the states to secure the Nation's election infrastructure and implement corrective actions to address our prior recommendations.

Results of Audit

DHS has improved coordination efforts to secure the Nation's systems used for voting, but should take additional steps to protect the broader election infrastructure, which includes polling and voting locations and related storage facilities, among other things. CISA has developed a set of plans and guidance aimed at securing election systems for the 2020 election cycle. But, the plans do not sufficiently mitigate other potential risks to physical security, terrorism threats, or targeted violence to the election infrastructure, nor do they identify dependencies on external stakeholders that impede mission performance. DHS senior leadership turnover and ongoing CISA reorganization have hindered CISA's ability to enhance planning and effectively monitor its progress in securing the Nation's election infrastructure.

Since our 2019 report, CISA has increased its outreach and coordination with election stakeholders. CISA can further improve the quality of information shared, as well as the timeliness of its assistance to election stakeholders. Inadequate classification authority, duplicative data sharing, and limited staffing have restricted CISA's ability to provide additional services and assessments. With the 2020 elections at hand and increased potential for revised election processes due to the COVID-19 pandemic, it is critical that CISA institute a well-coordinated approach and provide the guidance and assistance necessary to secure the Nation's election infrastructure.

DHS Has Not Adequately Addressed Physical Security Risks to the Election Infrastructure

DHS has taken steps during the past 2 years to develop election security plans and guidance aimed at mitigating risks to the Nation's election infrastructure. These materials have helped to outline key election security-related risks to election systems. But, the materials do not adequately address other potential threat areas that were included in DHS' *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019, such as physical security risks, terrorism threats, and targeted violence. CISA also has not updated other critical plans or strategic documents concerning the election infrastructure. Department leadership changes and protracted CISA

reorganization have continued to delay CISA's efforts to complete its election infrastructure planning.

Inadequate DHS Plans and Strategies to Support the 2020 Election

During 2019 and 2020, CISA developed or updated at least five planning documents and guides to help secure the election infrastructure ahead of the 2020 election cycle. CISA created these documents to facilitate collaboration by defining roles and responsibilities among stakeholders in the private sector; Federal, state, local, tribal, and territorial governments; and nongovernmental organizations. These documents outline objectives and key actions for coordination and incident response. Table 1 shows the five election infrastructure documents CISA has developed since 2019.

Table 1. DHS Plans and Strategies since Our Last Review

Document Name	Description
1. *#Protect2020 Strategic Plan*, February 2020	Defines lines of effort and objectives for achieving the mission to secure election infrastructure ahead of the 2020 election cycle.
2. *CISA 2020 Election Security Operations Plan*, February 2020	Defines CISA's responsibilities in support of state and local officials, private sector partners, and partisan organizations for the 2020 elections.
3. *Election Infrastructure Subsector-Specific Plan*, 2020	Outlines collaboration efforts and actions between public and private sector partners to protect election infrastructure and mitigate risk of hazards and threats, including natural disasters, terrorist attacks, cyberattacks, and other large-scale disruptions. The plan also identifies and prioritizes assets, assesses risks to election infrastructure, implements protective programs, and measures the effectiveness of these activities.[15]
4. *Homeland Security Operational Analysis Centers Election System Risk Prioritization*, July 2019	Focuses on the impact of potential individual cyber-attacks against election system components, including: theft of information, changing information within or the functionality of a system, and disruption or denial of the use of the system.
5. *Election Infrastructure Security Resource Guide*, May 2019	Discusses CISA's available resources to assist state and local election officials.

Source: Office of Inspector General (OIG) analysis of DHS documents

[15] We previously reported that DHS developed the *Election Infrastructure Subsector Specific Plan*, an annex to the 2013 *National Infrastructure Protection Plan*, in our report, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, OIG-19-24, February 28, 2019.

These plans and strategies provide general information to help protect the IT systems and electronic assets that support the election. According to CISA officials, the component has focused its election security efforts around cybersecurity risks, particularly those associated with internet-connected systems, which CISA assesses to be the most significant risk area to election infrastructure. The officials added that there are existing intelligence requirements and mechanisms to share both cyber and physical threat information, though they stated intelligence on physical threats is not common.

The plans cover potential cybersecurity disruptions to state and local election systems. However, they do not adequately address other elements such as physical security risk, threats of terrorism, and targeted violence at related storage facilities, polling places, and centralized vote tabulation locations that support the election process. More specifically, CISA did not sufficiently address physical security, terrorism, and targeted violence in three of its recent election security related documents:

1. *#Protect2020 Strategic Plan*, February 2020, focused on election system security in terms of "cyber" throughout the document. CISA uses the terms "election system" and "election infrastructure" interchangeably and only identifies physical security risk at the polling station in the "Last Mile" poster. Further, when CISA discusses the threat to state and local officials, poll workers, and election systems, it only cites threats from "foreign states and criminal organizations," not from targeted violence, mass shootings, gun violence, or domestic extremist groups.

2. *CISA 2020 Election Security Operations Plan*, February 2020, describes how state and local officials, volunteer poll workers, and election system vendors are responsible for administering safe and secure elections. CISA provides the resources and support necessary to ensure a comprehensive response to incidents affecting the integrity of elections. The plan details CISA's nine critical information requirements for the 2020 general elections. However, more than half of CISA's critical information requirements focus on cybersecurity incidents.

3. *Election Infrastructure Subsector-Specific Plan*, 2020, was revised to assess and mitigate risk. While this guide describes what physical locations outlined in the 2017 designation encompasses, it does not sufficiently address physical security risks and counterterrorism threats. The guide only briefly discusses the need to prepare for

disaster recovery and foreign influence threats. In contrast, CISA's primary focus is to promote its cybersecurity services, risk management efforts, and audits as the key activities for the subsector.

Despite CISA not adequately addressing terrorism and targeted violence in its recent election security documents, DHS has emphasized the need to address threats of terrorism and targeted violence in its 2019 department-level framework.[16] The framework reiterates that the threat posed by foreign terrorist organizations remains a priority for the Department and the Nation as a whole. Specifically, according to the framework, "our Nation's infrastructure and public spaces are high-value targets for terrorism and targeted violence." DHS also emphasizes the importance of understanding both positive and potentially malicious uses of technology as it can be used to incite violence and misinformation campaigns. Recognizing the potential threat of terrorism and risks to the Nation's critical infrastructures, DHS acknowledged the need for additional resources and submitted a funding request in its FY 2021 budget to address terrorism as part of its Homeland Security mission, including election security efforts.

However, CISA did not include in its plans the priority actions cited in the framework,[17] such as informing state and local officials about all potential threats to the election infrastructure. As part of its mission to improve cybersecurity, CISA is already sharing cyber threat information with law enforcement agencies. To enhance the protection of the Nation's election infrastructures, CISA must also communicate the potential physical security risk, terrorism threats, and targeted violence, as well as cybersecurity, to state and local officials, as they are responsible for administering and managing the elections.

DHS Has Not Updated Other Key Security Planning Documentation

Although DHS has made progress in establishing a core set of election security plans and guidance, it has not yet updated two overarching critical infrastructure plans to accurately reflect evolving risks and priorities in the election infrastructure security. Specifically, DHS has not updated the following plans to include the specific goals, objectives, milestones, and priorities needed to monitor and secure the election infrastructure, and address other emerging threats.

[16] *DHS Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019. In the framework, Goal #4 focuses on *Enhance U.S. Infrastructure Protections and Community Preparedness,* which covers election infrastructure as part of the Government Facilities Sector.
[17] *DHS Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019.

- *National Infrastructure Protection Plan* – This plan guides the national effort to manage risk to the Nation's critical infrastructure. The plan establishes a vision, mission, and goals, supported by a set of core principles focused on risk management and partnership, to influence future critical infrastructure security and resilience planning. In February 2013, the President issued a policy directive, which explicitly called for an update to the existing 2009 plan because of significant changes in the critical infrastructure risk, policy, and operating environment. In January 2017, former Secretary Johnson announced that the Nation's election infrastructure would be recognized as a priority in any future version of this plan. However, as of July 2020, DHS had not updated the plan — approximately 3.5 years later.
- *Government Facilities Sector-Specific Plan* – This plan provides a strategy for improving sector resilience by addressing emerging threats and establishing priorities and goals for mitigating risks.

We identified the same issue in our 2019 report, stating that these updates are necessary to align and prioritize CISA's efforts and establish metrics for measuring progress for the election infrastructure.[18] Updating these plans will also promote stronger unity of effort in departmental cybersecurity activities to protect the subsector. During our prior audit, CISA stated the Department planned to coordinate with the General Services Administration to update the *Government Facilities Sector-Specific Plan*, but that effort was not yet completed at the time of this audit. CISA also planned to revise the *National Infrastructure Protection Plan* and the *Joint National Priorities* in collaboration with representatives from all 16 critical sectors. Once both documents are revised, the sector-specific plans can be updated. According to CISA, in collaboration with public and private sector partners from all critical infrastructure sectors, it initiated actions to update the *National Infrastructure Protection Plan* in 2019. CISA anticipates the update to the *National Infrastructure Protection Plan* will be completed in 2021.

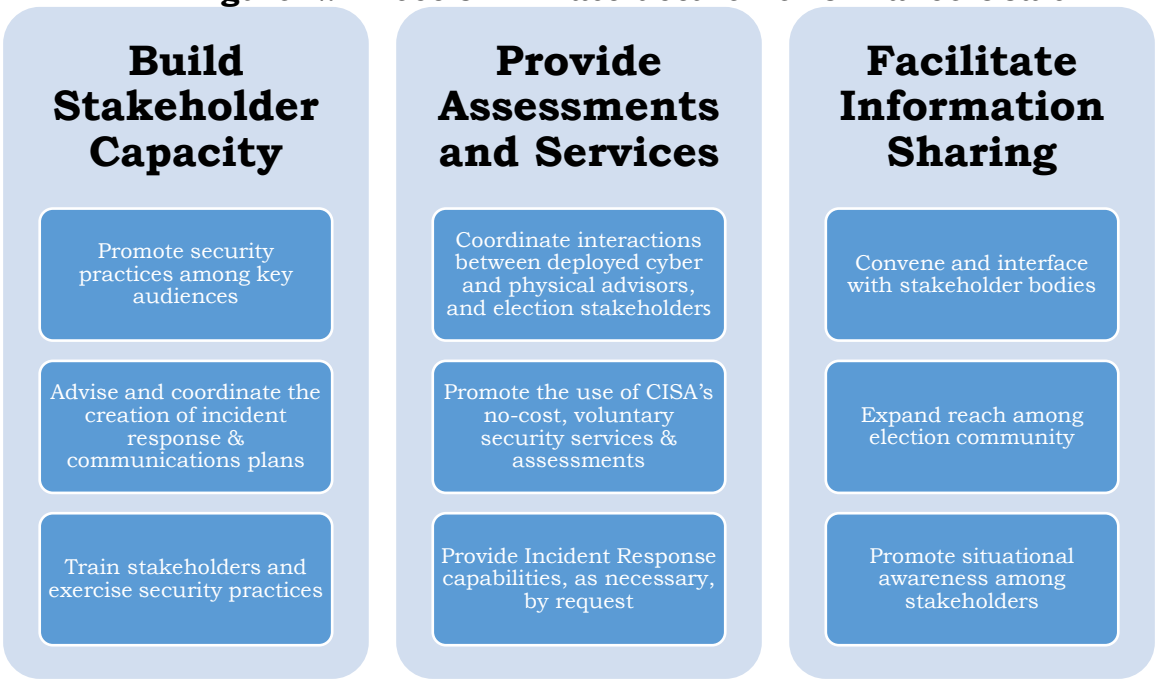
Performance Goals Lacked the Required External Factors

The *GPRA Modernization Act of 2010* requires Federal agencies to have performance goals in their strategic plans that are results-oriented, describe how they will achieve them, and identify key external factors that may limit the

[18] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, OIG-19-24, February 28, 2019.

Federal agency's ability to complete their goals.[19] In accordance with this requirement, CISA established election infrastructure performance goals in its #*Protect2020 Strategic Plan*. These goals are shown in Figure 2.

Figure 2. Election Infrastructure Performance Goals



Source: CISA's #*Protect2020 Strategic Plan*

Additional CISA performance goals include reaching out to election stakeholders and performing cyber hygiene vulnerability scanning. Specifically, their goals are to determine how much stakeholder outreach is conducted through conferences, meetings, and summits. Further CISA measures the number of products delivered within less than 60 days of state and local election officials' requests. Further, the National Cybersecurity and Communications Integration Center (NCCIC)'s goal is to have all 50 states subscribed to its voluntary cyber hygiene vulnerability scanning service.[20]

However, CISA did not identify the required external factors beyond its control that could significantly affect its ability to achieve their election infrastructure performance goals. Identifying external factors that could impact the election

[19] Some external factors that could impact election infrastructure are natural disasters, terrorism, and targeted violence.
[20] The mission of NCCIC, which is part of CISA, is to reduce the risk of systemic cybersecurity and communications challenges in its role as the Nation's flagship cyber defense, incident response, and operational integration center.

infrastructure will allow CISA to better prepare to deal with all situational risk and achieve its goals.

CISA Faced Challenges in Completing Plans to Secure the Election Infrastructure

Continual changes in DHS leadership and within the CISA organization have hindered CISA's progress in election infrastructure planning activities. As we reported in February 2019, (1) there were two DHS Secretaries within the first 12 months of the current Administration, and (2) CISA has been undergoing a protracted reorganization since its November 2018 re-designation. Such flux has continued since that time. In fact, since April 2019, there have been two additional Acting DHS Secretaries and the CISA reorganization is ongoing. As of May 2020, approximately 1.5 years after its re-designation, CISA remained unable to provide us with a detailed organization chart approved by its management.

Consequently, CISA has not yet defined its organizational structure or delineated roles and responsibilities across its personnel. The absence of an approved organization structure has also led to confusion within the Department. For example, I&A officials told us in March 2020, NCCIC was recently re-organized. However, when we reached out to CISA officials for confirmation in April 2020, they dismissed this notion. According to CISA officials, the confusion may arise when some people refer to NCCIC according to its statutory authority while others refer to the organizational body (i.e., the Cybersecurity Division) that carries out the functions described in the statute.

Amid the leadership vacancies and repeated turnover, within DHS, CISA has not sufficiently prioritized key activities or established effective performance measures to monitor its progress in accomplishing its mission and goals of securing the Nation's election infrastructure. Without DHS senior leadership guidance as a foundation, CISA cannot work successfully with sector representatives to develop the plans and strategies needed to secure the election infrastructure.

Further, when assisting state and local election officials, CISA has primarily focused on the cybersecurity of election systems instead of broader election infrastructure aspects including related storage facilities, polling places, and centralized vote tabulation locations used to support the election process. CISA's focus on cybersecurity may be attributed to reported cybersecurity threats and misinformation campaigns from foreign nations during the 2016 and 2018 elections. While beneficial, CISA's primary focus on cybersecurity

has limited DHS' ability to provide the strategic direction needed to secure the election infrastructure from broader types of potential risks.

Potential Consequences of Limited Election Security Planning

Given increased targeted violence in recent years and the impact of the ongoing COVID-19 pandemic, the risk to our Nation's critical infrastructure sectors has changed dramatically since 2013. While attacks on physical election infrastructure locations and assets are rare, CISA should consider both physical and cyber threats as part of a comprehensive understanding of the threat and incorporate them in its election security and resilience planning. For example, an individual drove a van into a voter registration tent manned by campaign volunteers in February 2020. CISA cannot effectively secure the election infrastructure or manage risk to the Nation's critical infrastructure based on the 2013 *National Infrastructure Protection Plan* by focusing on cybersecurity alone. A clear roadmap, sufficiently addressing broader risks, is needed to better guide DHS efforts and help achieve its goals of securing the election infrastructure.

Comprehensive planning that addresses election systems, storage facilities, polling places, vote tabulation locations, and IT communication facilities, is essential to secure the election infrastructure to support our election process. Without a well-defined and organized strategy with specific priorities, key milestones, and goals and objectives, CISA cannot ensure the actions taken to secure the election infrastructure are effective. Specifically, without updating the *National Infrastructure Protection Plan*, DHS may not have adequately identified the various threats and vulnerabilities associated with the election infrastructure subsector and opportunities for mitigating potential risks. Until this plan is updated to include the election infrastructure, DHS cannot achieve its 2013 goals of (1) assessing and analyzing the impact to the critical infrastructure that may result from potential threats or vulnerabilities, (2) enhancing critical infrastructure resilience through advance planning and mitigation, and (3) sharing actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.

CISA Has Increased Assistance to Election Stakeholders, but Improvements Are Needed

CISA has generally increased its outreach and coordination with election stakeholders since our 2019 report. However, improvements are needed in the quality of CISA information sharing as well as the timeliness of its technical

assistance to nationwide stakeholders in the election process. A number of factors have restricted CISA's ability to provide additional services and election systems assessments. By addressing these deficiencies, CISA can improve its efforts to assist stakeholders in safeguarding our Nation's election systems.

CISA's Outreach, Coordination, and Technical Assistance in Critical Sectors

In February 2013, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, directed the Federal Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities might better protect and defend themselves against cyber threats. Also in February 2013, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, required the DHS Secretary, in coordination with sector-specific agencies and other Federal agencies, to:

> (1) provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators, and
>
> (2) facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure.

Additionally, the White House *National Cyber Strategy of the United States*, dated September 2018, requires the Federal government to accomplish the following:

- Provide technical and risk management services, support training and exercises, maintain situational awareness of threats to this sector upon request, and improve the sharing of threat intelligence with state and local officials to better prepare and protect election infrastructure.
- Continue to coordinate the development of cybersecurity standards, guidance, and tools to safeguard the electoral process.
- Provide threat and asset response to recover election infrastructure in the event of a significant cyber incident.

<u>CISA Outreach and Coordination with Stakeholders</u>

In accordance with this guidance, CISA has participated in a series of coordination meetings with state and local election officials, and Federal partners, to raise awareness of cybersecurity issues related to the Nation's

election systems. Additionally, DHS coordinates on an ongoing basis with other Federal agencies and state and local election officials, such as the Election Assistance Commission, Department of Justice's Federal Bureau of Investigation, National Association of Secretaries of States, National Security Agency, National Association of State Election Directors, and the Office of the Director of National Intelligence.

Since our last report, CISA continues to coordinate with and provide assistance to state and local election officials.[21] To help improve the security of the Nation's election systems and facilitate information sharing, DHS works with the following:

- Election Infrastructure Subsector Government Coordinating Council. This is a government partnership council with the primary goal of sharing election security information among governments at the Federal, state, and local levels and collaborating on best practices to mitigate and counter threats to election infrastructure. Members include the Federal, state, and local government agencies that own, operate, or administer physical or digital/cyber assets, systems, and processes related to the conduct of elections or that have responsibility for supporting the security and resilience of those assets, systems, and processes.

- Election Infrastructure Subsector Coordinating Council. Established in February 2018 for private sector election infrastructure providers, this Council provides election industry stakeholders (whose services, systems, products, or technology are used by or on behalf of state or local governments to administer the U.S. election process) a self-governing forum for voluntary interaction among themselves and with their counterparts, as outlined in Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 2013.

- Election Infrastructure Information Sharing and Analysis Center. According to CISA officials, the component provides direct funding to this center through a cooperative agreement that requires the center to offer specific services to its members. Through this center, election agencies gained access to an elections-focused cyber defense suite of resources, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices. All 50 states, and local, tribal and territorial

[21] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, OIG-19-24, February 28, 2019.

governments, and more than 2,300 local jurisdictions signed up for the cyber threat information-sharing service from the Election Infrastructure Information Sharing and Analysis Center. The 2,300 local jurisdictions represented an increase from the 849 referenced in a prior report.[22] The key services the center offers are:

• 24/7 Security Operation Center	• Weekly News Alert
• Secure Portal Access for Communication and Document Sharing	• Incident Response Services
• Malicious Code Analysis Platform	• Cybersecurity Tabletop Exercises
• Monthly Members-only Webcasts	• Vulnerability Management Program
• Election-specific Threat Alerts	• Nationwide Cyber Security Review
• Quarterly Threat Report	• Awareness and Education Materials

CISA has also increased its outreach and information sharing, and raised cyber threat and incident awareness with state and local election officials since our last report. For example, CISA produced an outreach document, *Key Steps for Election Officials to Take to Improve Their Cybersecurity Posture*, to encourage election officials to (1) join the Elections Infrastructure Information Sharing and Analysis Center, (2) familiarize themselves with state election systems, (3) test the election infrastructure security, and (4) educate themselves about phishing scams. The following are some of the actions CISA took from March 2019 to February 2020:

[22] *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*, OIG-19-24, February 28, 2019.

• Participated in a 3-day National Association of State Election Directors winter conference to discuss the *Election Infrastructure Security Resource Guide*.	• Conducted a public awareness campaign to educate the electorate about the possibility of foreign actors spreading divisiveness to interfere with our democratic processes.
• Developed guidance on protecting the election systems from ransomware, and CISA services and support to recover from ransomware.	• Produced an outreach document that encourages state and locals to obtain a .gov domain, typically only available to U.S. government agencies. Using the .gov domain signifies trust and credibility. Two-step verification is required for all users.
• Issued Cybersecurity Best Practices for Election Officials to raise the importance of addressing new and emerging cyber threats and vulnerabilities, mitigating vulnerabilities timely, restricting access to election infrastructure, and developing a plan and performing periodic backups of sensitive information.	• Issued guidance, Domain-Based Message Authentication, Reporting and Conformance, which is an email authentication policy to raise the awareness of bad actors using fake email addresses disguised as legitimate emails from trusted sources.
• Produced numerous one-page outreach handouts, such as Disinformation Stops with You, Recognize the Risk, Question the Source, Think before You Link, and Talk to Your Circle, which provide ways to combat misinformation campaigns.	• Encouraged state and local election stakeholders to use multi-factor authentication, where a system requires a user to present a combination of two or more credentials for user identity verification at login.

State Election Stakeholders Found CISA's Outreach and Coordination Helpful

Election stakeholders have been generally satisfied with CISA's coordination efforts and activities. Based on feedback from our interviews with 11 state election officials, we attributed the improvement to CISA's increased outreach and coordination with election stakeholders since our 2019 report. We have summarized state election officials' feedback in Table 2.

Table 2. Selected State Election Stakeholders' Satisfaction with CISA's Coordination and Outreach Activities

Attribute Questioned	Yes	No	NA
DHS Performed More Outreach to States	10 (91 percent)	0 (0 percent)	1 (9 percent)
DHS Made Election Infrastructure a Priority	10 (91 percent)	0 (0 percent)	1 (9 percent)
DHS Had Positive Working Relationship with States	9 (82 percent)	0 (0 percent)	2 (18 percent)
DHS Made Progress	9 (82 percent)	0 (0 percent)	2 (18 percent)

Source: OIG summary from 11 state election stakeholder interviews

CISA Provided Additional Services for State and Local Election Organizations

Upon request, CISA offers the following no-cost cyber and physical security assessments and services, and incident coordination to help state and local stakeholders secure their election infrastructure. According to CISA officials, CISA headquarters' dedicated assessment teams provide the majority of the cybersecurity services. CISA officials added that the most commonly requested cybersecurity assessments by election stakeholders are Remote Penetration Testing and Risk and Vulnerability Assessments.

- Remote Penetration Testing. Focuses entirely on externally accessible systems, and may incorporate scenario-based external network penetration testing, external web application testing, and phishing campaign assessments.
- Vulnerability Scanning. (formerly Cyber Hygiene Scanning) Assesses internet-accessible systems on a continual, remote basis to identify vulnerabilities and configuration errors.
- Cybersecurity Exercises. Assist election infrastructure partners in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities.
- Phishing Campaign Assessments. Evaluate an organization's susceptibility and reaction to phishing emails of varying complexity.
- Risk and Vulnerability Assessments. Combine national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide actionable remediation recommendations prioritized by risk.
- Validated Architecture Design Reviews. Assist with architecture and design review, system configuration, log file review, and analysis of network traffic to identify anomalous communication flows.

- Hunt and Incident Response Team. Provides incident response, management, and coordination activities for cyber incidents. The Hunt and Incident Response Team also works with its constituents to identify and contain adversary activity and develop mitigation plans for removal and remediation of root cause.

Regional Cybersecurity Advisors perform the following cybersecurity assessments:

- Cyber Infrastructure Surveys. Evaluate the effectiveness of more than 80 cybersecurity controls, including incident response capabilities.
- Cyber Resilience Reviews. Assess the cybersecurity management capabilities implemented to protect critical IT services.
- External Dependencies Management Assessments. Assess activities and practices used to identify, analyze, and reduce supply chain risks.

In addition, Protective Security Advisors may offer the following:

- Assist Visits. Enhance DHS' relationship with state and local election stakeholders by informing them of the importance of their election infrastructure facilities, reinforcing the need for continued vigilance, and providing an overview of CISA's available resources to enhance election infrastructure security and resilience.
- Infrastructure Survey Tool. Identify facilities' physical security, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery.
- Security Assessment at First Entry. A rapid physical security assessment that provides owners and operators with a review of their existing security measures and feedback on making their facilities more secure.
- Regional Resiliency Assessment Program. Generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure by resolving infrastructure security and resilience knowledge gaps, informing risk management decisions, identifying opportunities and strategies to enhance infrastructure resilience, and improving critical partnerships

among the public and private sectors. According to CISA, the program is an additional capability that it offers, however, there has been no application of the program to the election infrastructure.

CISA Increased Its Assistance to State and Local Election Stakeholders

CISA increased its assistance to state and local election stakeholders since our prior audit. Between FY 2019 and FY 2020, CISA conducted 225 cybersecurity assessments at selected localities, as compared to 134 from FY 2017 to FY 2018. CISA's range of cybersecurity assessments evaluated operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. These services are available upon request without cost to state and local election jurisdictions.

In addition, CISA performed 13 tabletop exercises between FY 2019 and FY 2020, as compared to just 6 conducted from May to August 2018.[23] For example, in June 2019, CISA and numerous election infrastructure partners conducted *The Tabletop the Vote 2019: National Election Cyber Exercise.* This tabletop was a large comprehensive exercise, which included CISA, representatives from 47 states, and many other election infrastructure partners. The exercise helped evaluate cyber incident management for all state, local, tribal, and territorial entities and Federal participants, and increased participants' awareness of a range of incident response issues. The tabletop exercise identified best practices and areas for improvement in cyber incident planning, identification, response, and recovery through simulation of a realistic scenario that may affect voters' confidence, voting operations, and the integrity of elections. The scenario was based on a combination of real world events as well as potential risks facing election infrastructure, including:

- news and social media manipulation related to political candidates and the conduct of elections;
- spear phishing campaigns targeting elections officials and personnel;
- disruption of voter registration information systems and processes;
- denial of service attacks and web defacements impacting board of election websites and web applications; and

[23] As of August 2020, CISA officials stated they were on schedule to complete 18 tabletop exercises by the end of FY 2020.

- malware infections affecting election personnel computers and election management system software, and disruption to the vote by mail process.

CISA's Response to the COVID-19 Pandemic

COVID-19, also known as coronavirus, is an infectious disease unknown before an outbreak in Wuhan China, in December 2019. On March 11, 2020, COVID-19 was declared a pandemic affecting many countries globally. CISA created a *COVID-19 & Elections* website to post voluntary guidance from the Joint Working Group, which included suggestions for election stakeholders on how to prepare for the upcoming elections while dealing with the pandemic.[24] Given the ongoing COVID-19 pandemic, voters could be required to maintain social distance and wear masks at polling stations, as shown in Figure 3.

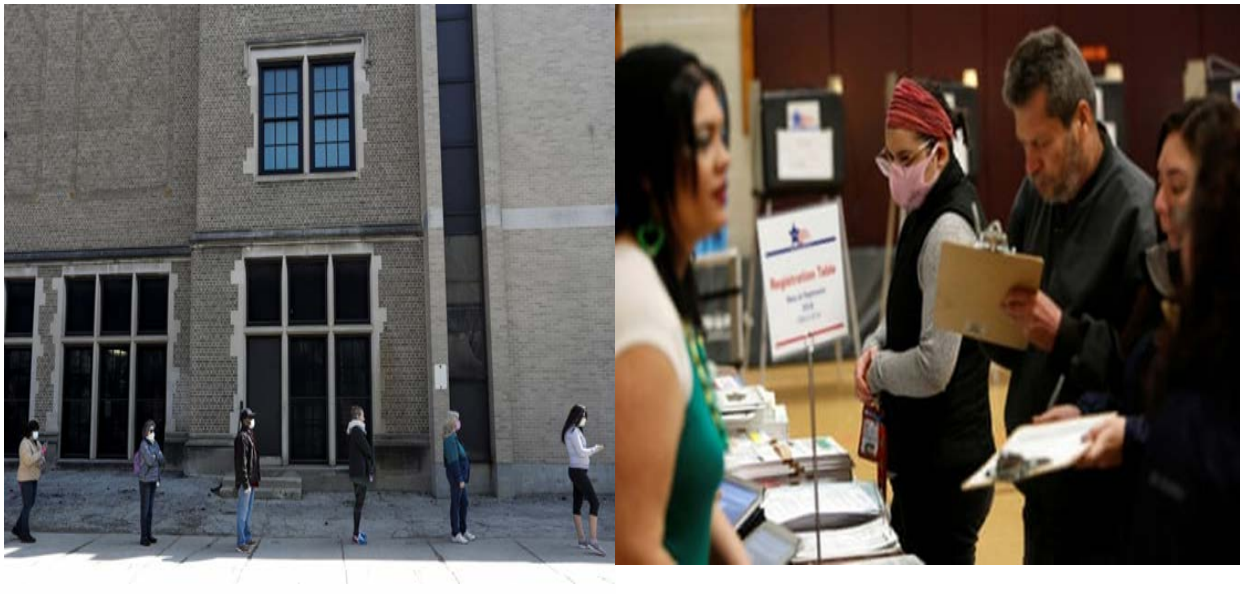


Figure 3. In-person voting during COVID-19
Source: Wisconsin Public Radio, April 14, 2020; the Guardian, April 23, 2020

In spring 2020, CISA provided guidance to state, local, tribal, and territorial election officials on how to administer elections amid the COVID-19 pandemic. CISA guidance included:

- ballot drop box,

[24] In response to the current pandemic, the Election Infrastructure Subsector Coordinating Council and Election Infrastructure Government Coordinating Council created a COVID-19 Joint Working Group.

- election education and outreach for increased absentee or mail voting,
- electronic ballot delivery and marking,
- inbound ballot process,
- managing an increase in outbound ballots,
- signature verification and cure process,
- helping voters to request a mail-in ballot,
- vote by mail project timeline of activities, and
- printing/mailing organizations.

Additionally, in June 2020, CISA created a *COVID-19 Disinformation Toolkit* designed to help officials bring awareness to misinformation appearing online related to the COVID-19 pandemic. The White House, the Centers for Disease Control and Prevention, and DHS' Federal Emergency Management Agency also created a joint resource that addressed frequently asked COVID-19 pandemic questions. The list was posted to faq.coronavirus.gov to provide answers to questions such as:

- "What are the symptoms?"
- "Should I get tested?"
- "How does it spread?"
- "How do I reduce my risk?"

CISA Improvements Needed in the Quality of Information Shared and the Timeliness of Services

While CISA has continued providing steady outreach and coordination to assist election officials, the cyber threat information it shared was not always useful. Improving coordination between CISA and I&A is essential to effectively aid election stakeholders with mitigating risks associated with the subsector.

CISA Needs to Improve the Quality of Information Shared

Based on our interviews with selected CISA regional staff, the cyber threat information CISA and I&A shared with election stakeholders was not always considered useful.[25] DHS is required to maintain situational awareness of

[25] We interviewed 12 Cybersecurity Advisors, 15 Protective Security Advisors, and 10 Regional Directors who interface with state and local election stakeholders, I&A, and officials from other Federal agencies.

threats, and improve the sharing of threat intelligence with stakeholders to better prepare and protect election infrastructure.[26] However, according to selected CISA regional staff, the information was over-classified, not tailored to election stakeholders needs, and could be obtained elsewhere. According to our interviews with CISA's regional staff 12 Cybersecurity Advisors, 15 Protective Security Advisors, and 10 Regional Directors, the following are opportunities to improve the quality of information shared with stakeholders:

- 8 (22 percent) of 37 CISA regional staff stated the information was overly classified.
- 8 (22 percent) of 37 CISA regional staff stated briefings were not tailored to stakeholders needs.
- 7 (19 percent) of 37 CISA regional staff stated the information could be obtained from public sources. In one example, by the time the cyber threat information was declassified for sharing with election stakeholders, they had already learned about it through the news media.
- 5 (14 percent) of 37 CISA regional staff stated that after attending briefings, election officials could not share the information with their information technology staff and county clerks to remediate vulnerabilities as they did not possess the proper clearances.
- 1 (3 percent) of 37 CISA regional staff stated some briefings were repetitive.
- 7 (19 percent) of 37 CISA regional staff stated Fusion Centers were too far away and not convenient.[27]

Representatives of other Federal agencies also told us about their work with CISA to secure the election infrastructure. One Federal agency representative discussed receiving duplicative election infrastructure threat information from CISA and DHS' I&A. Another Federal agency official stated, "I cannot think of a single thing in a classified briefing that I have not read from the media," indicating he had received complaints from others about DHS' intelligence briefings not being helpful.

[26] The White House, *National Cyber Strategy of the United States*, September 2018; and Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.
[27] Fusion Centers are state-owned and operated centers that serve as focal points in states to share threat-related information among state, local, tribal and territorial, Federal, and private sector partners.

CISA Did Not Perform Timely Assessments

Based on our independent review of CISA's cybersecurity assessment records, along with interviews with selected CISA regional staff, CISA did not always perform assessments timely. NCCIC records contained information about cybersecurity assessments they performed, including:

- Phishing Campaign Assessment,
- Remote Penetration Testing,
- Risk and Vulnerability Assessment, and
- Validated Architecture Design Review.

However, after reviewing the records we determined that 42 (53 percent) of 79 NCCIC cybersecurity assessments were not completed quickly enough to meet stakeholder needs.[28] For example:

- A Secretary of State initially requested a Phishing Campaign Assessment in October 2017. However, CISA did not begin the assessment until June 2018. CISA's records show NCCIC did not complete the assessment until January 2019, more than a year after the request was made.
- Another State Board of Elections requested CISA perform a Risk and Vulnerability Assessment in July 2018. The assessment did not begin until July 2019. NCCIC ultimately completed the testing in September 2019, more than a year after the initial request.

In addition, 4 of 37 (11 percent) CISA regional staff we interviewed stated that CISA's cybersecurity assessments were not timely. According to 27 (73 percent) of the 37 CISA regional staff we interviewed, CISA needed more Cybersecurity Advisors to help private sector entities and state, local, territorial, and tribal governments prepare for and protect themselves against cybersecurity threats.

According to CISA officials, cyber assessments are being requested by state and local election officials more often than physical assessments. However, based on records we obtained, we could not determine whether CISA had performed

[28] NCCIC provided records for 121 cybersecurity assessments. However, NCCIC formalized its assessment tracking records in May 2019. Some gaps still exist and some "Initial Request Date" information was missing. Therefore, we excluded assessments that did not have an "Initial Request Date" from our analysis.

physical assessments related to election systems for state and local officials. Since CISA only performed election physical assessments upon request, we could not determine whether stakeholders made any requests for physical assessments, or if requests were made but CISA did not record them.

Obstacles to Information Sharing and Timely Election Assistance

CISA faced a number of challenges that affected the type of information it shared and the election services it provided. Specifically, a lack of Original Classification Authority to declassify classified information, inadequate communication with I&A, and insufficient resources restricted CISA's ability to provide the level of assistance stakeholders needed to better secure election systems.

Lack of Authority to Declassify Information

CISA does not have the authority to declassify information classified by other sources. DHS has to maintain the same classification for information it receives unless the Original Classification Authority declassifies the information. To illustrate, DHS does not have the authority to declassify any information the Department did not generate. Specifically, DHS cannot generate reports or release any information that may hinder another agency's ongoing investigation, work in progress, or violate applicable classification policies.

Inadequate Communication with I&A

According to I&A officials, at times both CISA and I&A reach out to the same election stakeholders. Although CISA and I&A have different priorities, they share similar information with the same election stakeholders. For example, I&A officials said their goal is to provide Intelligence Information Reports, which are vehicles used to communicate threat information, as a snapshot in time, to the Intelligence Community at the lowest classification and as quickly as possible. However, before it shares cyber information, CISA conducts forensics analysis and develops a complete picture of the event, which takes time. As such, some election stakeholders may perceive the subsequent information they receive to be duplicative with information already received by I&A.

Subsequent to our fieldwork, CISA officials stated that since late 2019, the Election Security Initiative has worked with I&A on reports, analysis, and red teaming activity. CISA officials believe this work results in better products, more accurate information flows, and better communication with I&A on joint

briefings and Intelligence Community products. I&A officials also stated they would work with CISA to address and improve communication between the two components.

Staffing Shortages in CISA

Insufficient resources have hindered CISA's ability to provide timely assistance to state and local election officials. As of May 2020, CISA had 132 Cyber and Protective Security Advisors providing technical assistance and performing security assessments for all 16 critical infrastructure sectors. Both types of advisors also serve as critical infrastructure security and vulnerability mitigation subject matter experts to promote CISA's outreach and partnership effort by providing technical assistance to improve cyber and physical security awareness coordination with other DHS components, such as I&A. As part of their duties, these advisors offer cyber and physical security training for all of the critical infrastructure sectors. For example, these advisors may be required to assist with state, local, and Federal officials' response to current events, such as the current COVID-19 pandemic, or assist faith-based and community organizations' preparation to guard against violent extremist threats.

Our interviews with 12 Cybersecurity Advisors, 15 Protective Security Advisors, and 10 Regional Directors disclosed that CISA's current staffing level is not adequate to provide support to state and local election officials for securing the election infrastructure. According to these selected officials, they may not be able to devote their full attention to this effort, as they are also responsible for a range of services and activities to assist all 16 critical sectors. Each advisor's election security workload depends on the number of assigned election jurisdictions, which may vary across states. Elections are usually administered at the county level; however, in some New England and Midwestern states the cities and townships oversee elections. As we stated in a prior section, according to CISA there were 7,997 election administration jurisdictions in the country, as of September 2020. The size of these jurisdictions varies dramatically, with the smallest towns having only a few hundred registered voters, and the largest jurisdiction in the country, Los Angeles County, having more than 4.7 million, which is a lot for 132 advisors to cover nationwide.

Cybersecurity and Protective Security Advisors expressed concerns that their outreach efforts must satisfy not only the needs at the state level, but the needs at the county and local levels as well. Increasing CISA's resources commensurate with the need for services across all 16 critical infrastructure

sectors would allow the advisors to perform assessments more timely, including those for the election infrastructure sub-sector.

CISA officials acknowledged that staffing shortages have hindered the efforts to secure the Nation's critical infrastructures, including elections. According to officials, CISA is taking actions to alleviate some of these concerns. For example, as of August 2020 the component is actively recruiting to fill its vacant positions (54 Cybersecurity and 15 Protective Security Advisors), authorized under the Fiscal Year 2020 budget.

Opportunities for CISA to Improve Its Assistance to Election Stakeholders

Clearly, CISA can improve its efforts to assist stakeholders with addressing threats to the Nation's election infrastructure. With the November 2020 elections fast approaching, protecting the Nation's election infrastructure becomes more critical with each passing day. Given the recent history of foreign state interference, suspicious activities, and targeted attacks on the U.S. democratic process, all types of security — systems, cyber, and physical — are necessary to safeguard the various technologies, processes, and facilities comprising the election infrastructure. The COVID-19 pandemic may call for adjustments or additional planning for ensuring a successful election.

DHS also needs to improve its approach for addressing stakeholder needs in the current threat environment. Better coordination with I&A can help CISA improve the information shared with states and localities to prepare and protect election infrastructure more effectively. Improved outreach and services can help CISA persuade state and local officials to request more technical assistance and exchange relevant information to secure the subsector. Further, increased staffing can help CISA perform better and more timely assessments, when requested. By addressing these deficiencies, CISA and the Nation can be better prepared to counter the emerging threats and various types of attacks that may be aimed at our election infrastructure as we progress toward Election Day.

Recommendations

We recommend the Director of CISA:

Recommendation 1: Coordinate with the Office of the Secretary to revise the *National Infrastructure Protection Plan* and other planning documents to incorporate current and evolving risks as well as mitigation strategies needed to secure the Nation's election infrastructure.

Recommendation 2: Improve the collaboration between I&A and CISA, which can help to enhance the quality and reduce the redundancy of information DHS shares with Federal agencies and state and local election officials.

Recommendation 3: Assign the staff resources needed to conduct timely cybersecurity and physical assessments to assist states and localities with securing the election infrastructure.

Management Comments and OIG Analysis

CISA concurred with all three of our recommendations. A copy of CISA's response in its entirety is included in Appendix B. CISA also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate.

We obtained written comments on a draft of this report from the CISA Director. In the comments, the Director noted that CISA is pleased with OIG's recognition that it developed plans and guidance aimed at securing election systems for the 2020 election cycle, as well as increasing outreach and coordination to election stakeholders. Following is a summary of CISA's response to each recommendation and the OIG's analysis.

CISA Comments to Recommendation #1: Concur. According to CISA, it initiated actions, in coordination with public and private sector critical infrastructure partners, to update the NIPP in 2020. CISA currently expects to complete the update to the 2013 NIPP by March 2021. CISA also stated that its National Risk Management Center routinely conducts and updates its risk assessments and planning documents to account for the evolving risk environment and continues to develop an Operational Posture document. This document will set the cadence of events for November 3, including the timing of interagency meetings and reporting, as well as establish interagency communication mechanisms. Estimated Completion Date: March 31, 2021.

OIG Analysis of DHS Comments: CISA's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CISA provides documentation to support that all planned corrective actions are completed.

CISA Comments to Recommendation #2: Concur. CISA strives to improve the quality of information shared with election infrastructure stakeholders. For

example, the Election Security Initiative detailed a risk analyst to collaborate with the Intelligence and Analysis Directorate on reports, analysis, and red teaming activity for election security. CISA's Integrated Operations Division is also working with the directorate on a short-term concept of operations for 2020 election security to enhance the flow and quality of information. Based on lessons learned from the short-term concept of operations, a longer-term concept of operations will be developed and delivered by the end of February 2021 to support future elections. Estimated Completion Date: February 26, 2021.

OIG Analysis of DHS Comments: CISA's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CISA provides documentation to support that all planned corrective actions are completed.

CISA Comments to Recommendation #3: Concur. CISA stated it prioritized assessments of election infrastructure entities and the Cybersecurity Division, Vulnerability Management Assessment Branch, plans to conduct 20 election-specific onsite assessments in FY 2021. Further, CISA's Integrated Operations Division received an increase of 50 Cybersecurity Advisors in the enacted budget for FY 2020. CISA has hired 7 Cybersecurity Advisors and issued job offers to another 23 candidates. Estimated Completion Date: March 31, 2021.

OIG Analysis of DHS Comments: CISA's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CISA provides documentation to support that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. We conducted this audit to evaluate the effectiveness of the Department's efforts to coordinate with the states to secure the Nation's election infrastructure since our last audit.

Our audit focused on the requirements, recommendations, and goals outlined in the following key documents:

- *GPRA Modernization Act of 2010*;
- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience,* February 2013;
- Executive Order 13636, *Improving Critical Infrastructure* Cybersecurity, February 2013;
- Secretarial Memorandum, *Designation of Election Infrastructure as a Critical Infrastructure Subsector*, January 2017;
- The White House, *National Cyber Strategy of the United States of America*, September 2018; and
- *DHS Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019.

To conduct our audit, we interviewed 12 Cybersecurity Advisors, 15 Protective Security Advisors, 10 Regional Directors, 26 CISA/Election Security Initiative/NCCIC staff, and an I&A intelligence officer and branch chief. We also met with representatives from the following Federal agencies that work with CISA on election security:

- The Department of Justice's Federal Bureau of Investigation;
- The Federal Election Commission, United States of America; and
- The U.S. Election Assistance Commission.

In addition, we interviewed four officials from the National Association of Secretaries of States and seven officials from the National Association of State Election Directors.

As part of our review, we evaluated the actions CISA has taken to protect the election infrastructure subsector of the Government Facilities Sector. We assessed the effectiveness of the assistance CISA has provided to state and local election officials to identify and mitigate election infrastructure risks. Further, we obtained and analyzed computer-processed data related to the number of assessments performed as part of CISA's effort to secure the election infrastructure. To assess the reliability of these data, we interviewed agency officials knowledgeable about the information, and reviewed the data for completeness and obvious inconsistency errors. We found no discrepancies or errors in the data.

Due to the current COVID-19 pandemic, the audit team was unable to (1) receive classified briefing or materials related to the current threats to the election infrastructure, (2) meet with selected members of the Intelligence Community (i.e., the Director of National Intelligence, and the National Security Agency), and (3) receive the information requested from CISA and I&A timely. Finally, this audit was not designed to evaluate CISA's pre-pandemic preparedness or the effectiveness of CISA's response to the COVID-19 pandemic.

We conducted this performance audit between January and August 2020 in the Washington, D.C. area, pursuant to the *Inspector General Act of 1978*, as amended, and consistent 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 upon our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

October 12, 2020

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Christopher C. Krebs
Director

SUBJECT: Management Response to Draft Report: "DHS Has Secured The Nation's Election Systems, But Work Remains To Protect the Infrastructure" (Project No. 20-015-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA is pleased to note OIG's recognition that CISA developed a set of plans and guidance aimed at securing election systems for the 2020 election cycle, as well as CISA's increase in outreach and coordination with state and local governments, election officials, Federal partners, vendors, and other election stakeholders.

However, we are concerned that the release of the report less than one month before Election Day is problematic. We recommend adjusting the timeline of future audits to account for the entirety of an election cycle, to include election day and the certification time period, and allow sufficient time for CISA to implement its recommendations ahead of the next election cycle. CISA remains committed to defending our election infrastructure from foreign influence and physical threats and continues to make election security a top priority for the Department.

The draft report contained three recommendations, with which CISA concurs. Attached find our detailed response to each recommendation. CISA previously submitted technical comments under a separate cover for OIG's consideration.

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.

Attachment

Attachment: Management Response to Recommendations Contained in 20-015-AUD-CISA

OIG recommended that the Director of CISA:

Recommendation 1: Coordinate with the Office of Secretary to revise the National Infrastructure Protection Plan [NIPP] and other planning documents to incorporate current and evolving risks as well as mitigation strategies needed to secure the Nation's election infrastructure.

Response: Concur. CISA Infrastructure Security Division, in coordination with public and private sector partners across all critical infrastructure sectors, initiated an update to the NIPP in 2020. It is important to note, however, that updating the NIPP will not significantly impact CISA's election security operations, since the NIPP is a strategic document and CISA already worked with the Government Coordinating Council and Sector Coordinating Council to develop the sector specific plan. In addition, updates to sector specific plans are conducted in coordination with the Sector Specific Agency, in this case, the General Services Administration—but are not a requirement of statute or the NIPP. Further, the Joint National Priorities are a secondary NIPP support product, and may not be continued in the future, after completing the update to the NIPP. CISA currently expects to complete the update to the 2013 NIPP by March 2021.

CISA National Risk Management Center (NRMC) also routinely conducts and updates its risk assessments and planning documents to account for the evolving risk environment. For example, in July 2020, CISA issued the "Election Infrastructure Cyber Risk Assessment," which provided additional information on risks to key points of preparation, enabling the administration of elections. Also, in July 2020, CISA released a "Mail-in Voting in 2020 Infrastructure Risk Assessment" in acknowledgement of states expanding the use of mail-in voting in response to the COVID-19 pandemic. This assessment focuses specifically on the systems and infrastructure necessary to administer mail-in voting. Additionally, NRMC and CISA Integrated Operations Division (IOD) continue to develop an Operational Posture document that will be shared with the National Security Council (NSC) and interagency stakeholders. This operational plan will establish the cadence of events for November 3, including the timing of interagency meetings and reporting, as well as establish interagency communication mechanisms. Estimated Completion Date (ECD): March 31, 2021.

Recommendation 2: Improve the collaboration between the Office of Intelligence and Analysis [I&A] and CISA, which can help to enhance the quality and reduce the redundancy of information DHS shares with Federal agencies and state and local election officials.

2

Response: Concur. CISA continually strives to improve the quality of information shared within the election infrastructure subsector. Specifically, since 2019, the Election Security Initiative (ESI) detailed a risk analyst one day per week to co-locate with I&A to collaborate on reports, analysis, and red teaming activity for election security. This joint work resulted in improved products and information flows, as well as more agile communication on joint briefings and intelligence products between CISA, I&A, and the rest of the Intelligence Community. On multiple occasions, CISA also briefed National Security Agency staff worldwide on election infrastructure risk to inform collection efforts.

Additionally, CISA IOD is working with I&A on a short-term concept of operations for 2020 election security to enhance the flow and quality of information between CISA Intelligence and I&A to be signed in early October. A longer-term concept of operations, based on lessons learned from the short-term concept of operations, will be developed and delivered by the end of February 2021 to support future elections. ECD: February 26, 2021.

Recommendation 3: Assign the staff resources needed to conduct timely cybersecurity and physical assessments to assist states and localities with securing the election infrastructure.

Response: Concur. Assessing election infrastructure remains CISA's top priority. As a result, CISA prioritized assessments of election infrastructure entities above all others, and met the demand of our stakeholders in providing assessments in advance of the 2020 Election. In fiscal year (FY) 2020, for example, CISA conducted 118 assessments on election infrastructure entities, out of 270 total assessments. For comparison, the sector with the next highest number of assessments was the healthcare sector, with 29 assessments. In addition, the CISA Cybersecurity Division, specifically the Vulnerability Management Assessment Branch, is targeting 20 election-specific onsite assessments in fiscal year 2021. The 20 onsite assessments will be split evenly between the Risk and Vulnerability Assessment and the Validated Architecture Design Review services. CISA does not need to conduct assessments for all election infrastructure entities, because we conducted enough assessments to understand the sector and develop products which benefit the entire sector. Further, CISA emphasizes developing and making available automated assessments such as Cyber Hygiene and self-assessments which are infinitely scalable.

In addition, CISA IOD received an increase of 50 federal Cybersecurity Advisors (CSAs) in the FY 2020 Enacted Budget, who will directly support state government officials in their attempt to secure and build resilient information technology systems. This is especially true of those that will support local, state, and national elections. CISA is in the process of hiring those personnel, and placed seven CSA state coordinators thus far, with 23 further candidates selected and in the process of being issued job offers. While

3

CISA offices review the remaining resumes and conduct interviews for the remaining CSA state coordinator positions. Protective Security Advisors are also augmenting, where possible, CISA's current CSA cadre to support states and localities with cyber and physical assessments. Finally, in addition to assessments, CISA provides further support to election infrastructure partners in the form of vulnerability alerts, exercise support, and by participating in various state working groups, as appropriate. ECD: March 31, 2021.

4

Appendix C
Technology Audits and Analytics Support Major Contributors to This Report

Chiu-Tong Tsang, Director
Marcie McIsaac, Audit Manager
Stuart Josephs, Auditor-in-Charge
Barry Bruner, Auditor
Brendan Burke, Auditor
Mark Phillips, Auditor
Omar Russell, Auditor
Kelly Herberger, Supervisory Communications Analyst
Pamela Brown, Independent Referencer
Gary Alvino, Independent Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Assistant Director for Cybersecurity, CISA
Assistant Director for Infrastructure Security, CISA
Audit Liaison, CISA

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305