OFFICE OF INSPECTOR GENERAL

Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure

Homeland Security

February 28, 2019
OIG-19-24

DHS OIG Highlights

Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure

February 28, 2019

Why We Did This Audit

The election process is a cornerstone of American democracy. Prompted by the suspicious cyber activities on election systems in 2016, Secretary Jeh Johnson designated the election infrastructure as a subsector to one of the Nation's existing critical sectors. Our audit objective was to evaluate the effectiveness of the Department's efforts to coordinate with states on securing the Nation's election infrastructure.

What We Recommend

We recommend that DHS provide resources to ensure an organized strategy, improve services, expand outreach, and enhance information sharing.

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

The Department of Homeland Security has taken some steps to mitigate risks to the Nation's election infrastructure; however, improved planning, more staff, and clearer guidance could facilitate its coordination with states. Specifically, despite Federal requirements, DHS has 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. Senior leadership turnover and a lack of guidance and administrative staff have hindered DHS' ability to accomplish such planning. Until such issues are addressed and resolved, DHS cannot ensure effective guidance, unity of effort, and a well-coordinated approach to securing the Nation's election infrastructure.

Further, DHS provides assistance to state and local election officials upon request. Over time, the assistance provided has increased and the quality of information shared has improved. However, staff shortages, a lengthy security clearance process, and state and local officials' historic mistrust of Federal government assistance restrict DHS' efforts to provide the services and assessments needed to secure the election infrastructure. Addressing these issues is essential for continued improvement in the services, outreach, and quality of information DHS shares with election stakeholders.

Management Response

DHS concurred with all five recommendations and had corrective actions underway to address the findings.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

February 28, 2019

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

FROM: John V. Kelly
Acting Inspector General

SUBJECT: *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*

Attached for your action is our final report, *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at enhancing the program's effectiveness. The Department concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendation 5 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1 through 4 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 close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. 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 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 F. McCauley, Assistant Inspector General, Office of Audits, at
(202) 981-6000.

Attachment

Table of Contents

Appendixes

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DRE	Direct Recording Electronic
I&A	Office of Intelligence and Analysis
OIG	Office of Inspector General

Background

A secure and resilient election process is vital to our national interest. On October 1, 2016, 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 had determined that malicious actors gained access to state voting-related systems, but the Department was not aware of any manipulation of data at that time.

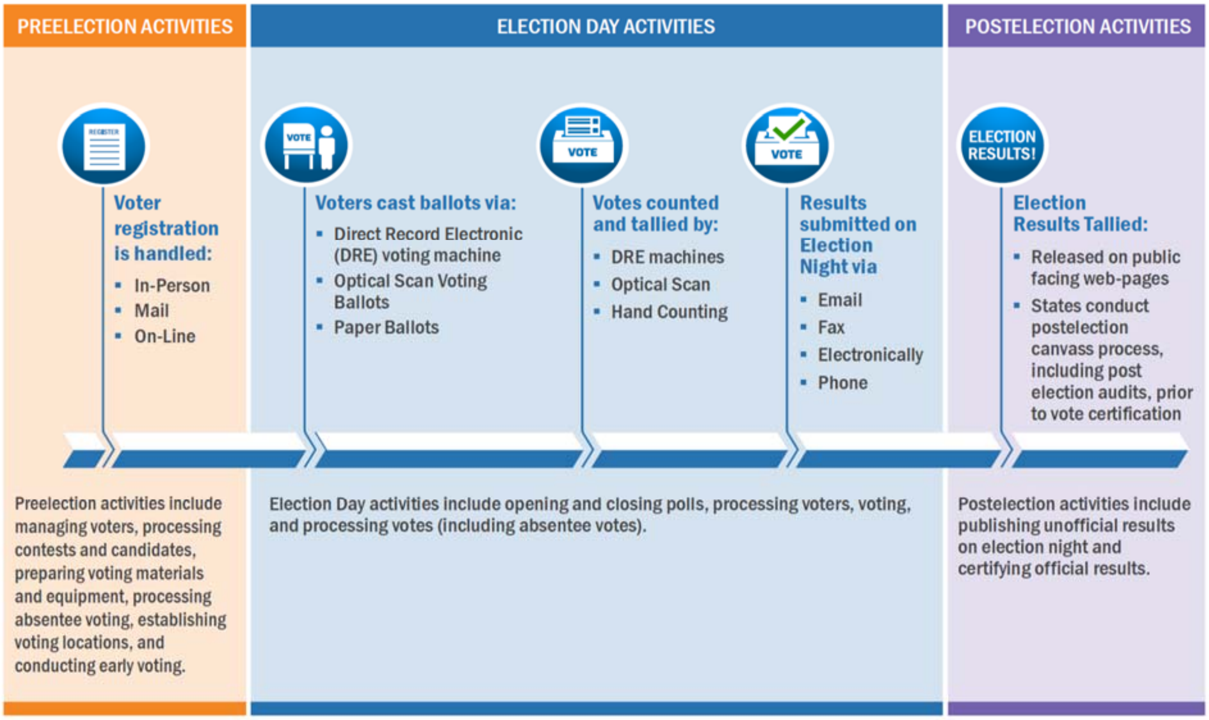
On October 7, 2016, DHS and the Office of the Director of National Intelligence released a joint statement on election security urging state and local governments to be vigilant and seek cybersecurity assistance from the Department. The joint statement illustrated the importance of and need for coordinated effort among states election officials and the Federal government to safeguard the Nation’s election infrastructure. Any potential compromise of the infrastructure that supports our election process would undermine voters’ confidence in the democratic election process.

The suspicious activities or potential attacks during the 2016 Presidential election were 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 on about 500,000 voters.

The Election Process

Our Nation’s election process includes pre-election, election day, and post-election activities. Figure 1 depicts the phases of this process, from voter registration, to ballot casting, to vote tallying, to submission and publication of the election results.

Figure 1: U.S. Electoral Process



PREELECTION ACTIVITIES

Voter registration is handled:

- In-Person
- Mail
- On-Line

Preelection activities include managing voters, processing contests and candidates, preparing voting materials and equipment, processing absentee voting, establishing voting locations, and conducting early voting.

ELECTION DAY ACTIVITIES

Voters cast ballots via:

- Direct Record Electronic (DRE) voting machine
- Optical Scan Voting Ballots
- Paper Ballots

Votes counted and tallied by:

- DRE machines
- Optical Scan
- Hand Counting

Results submitted on Election Night via

- Email
- Fax
- Electronically
- Phone

Election Day activities include opening and closing polls, processing voters, voting, and processing votes (including absentee votes).

POSTELECTION ACTIVITIES

Election Results Tallied:

- Released on public facing web-pages
- States conduct postelection canvass process, including post election audits, prior to vote certification

Postelection activities include publishing unofficial results on election night and certifying official results.

Source: DHS Election Security website

As illustrated in Figure 1, during the pre-election phase, qualified voters are registered to vote either in-person, by mail, or online. Voting officials perform the following tasks: (1) process candidates' election material, (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. Voting officials submit results via email, fax, phone, or electronically to the states' chief election officials.[1]

Post-election activities begin with tallying votes and submitting and publishing election results. After the votes are counted, voting officials release unofficial results to the public via public web pages and other media. Additionally, the voting officials perform audits to ensure that the reported election results are accurate. Ultimately, voting officials certify the final results. In most states, election officials are obligated by statute to post the certified results on a website, in a polling place, by newspaper, or at the courthouse.

[1] States may include all 50 states, the District of Columbia, and United States territories.

The U.S. Election Infrastructure

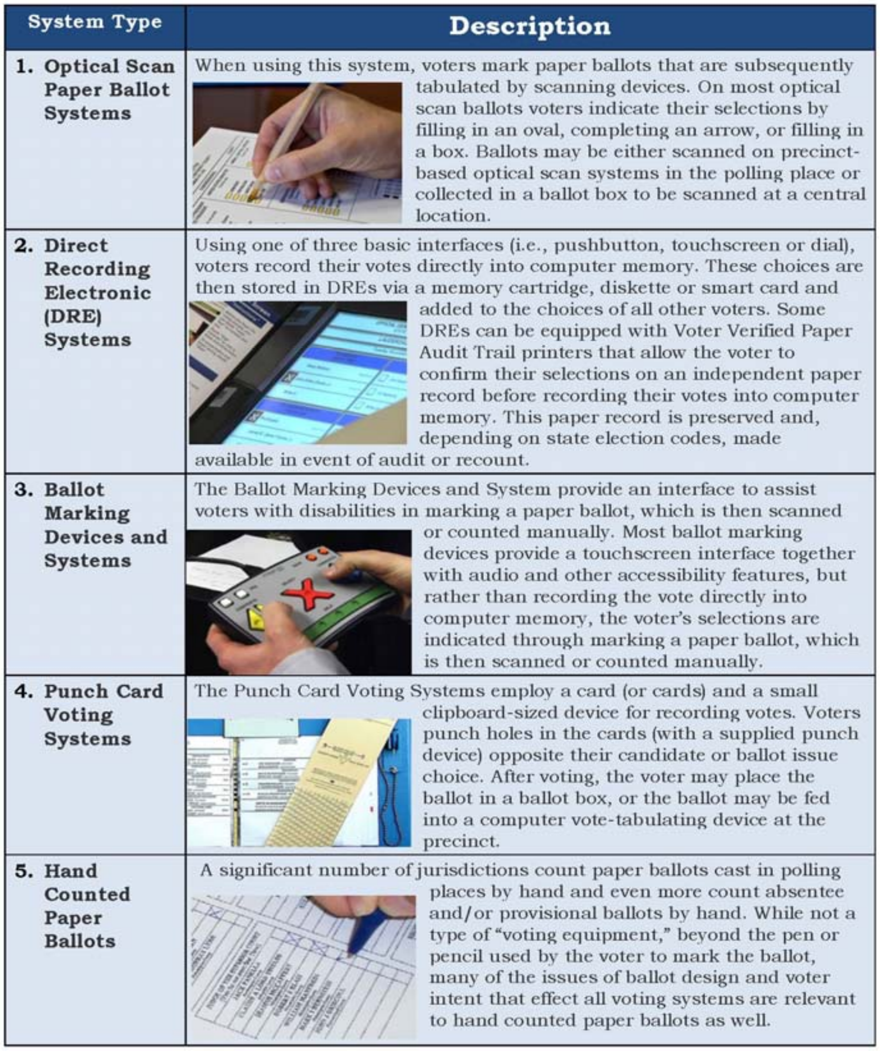
State and local governments manage the complex mix of people, processes, and technology that make up our Nation's elections infrastructure. The Constitution and Federal voting rights laws grant states broad latitude in how they administer Federal elections, which occur every 2 years in November. Few 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. There are more than 10,000 election administration jurisdictions in the country. The size of these jurisdictions varies 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.[2]

Across the Nation, the election infrastructure increasingly relies on Internet-based technology for efficiency and convenience. However, reliance on digital technologies introduces various cybersecurity risks. According to a 2016 DHS intelligence assessment, voting precincts in more than 3,100 counties across the United States use nearly 50 different types of voting machines produced by 14 different manufacturers. In addition, state and local jurisdictions may have different requirements for securing their election systems, such as configuration settings, audit logging, intrusion detection capability, and patch management. The diversity in voting systems and voting software provides significant challenges to cybersecurity.

Figure 2 depicts the various types of voting procedures and equipment commonly used in U.S. elections.

[2] "Election Administration at State and Local Levels," National Conference of State Legislatures, June 15, 2016

Figure 2: Examples of Voting and Ballot Marking Systems



System Type	Description
1. Optical Scan Paper Ballot Systems	When using this system, voters mark paper ballots that are subsequently tabulated by scanning devices. On most optical scan ballots voters indicate their selections by filling in an oval, completing an arrow, or filling in a box. Ballots may be either scanned on precinct-based optical scan systems in the polling place or collected in a ballot box to be scanned at a central location.
2. Direct Recording Electronic (DRE) Systems	Using one of three basic interfaces (i.e., pushbutton, touchscreen or dial), voters record their votes directly into computer memory. These choices are then stored in DREs via a memory cartridge, diskette or smart card and added to the choices of all other voters. Some DREs can be equipped with Voter Verified Paper Audit Trail printers that allow the voter to confirm their selections on an independent paper record before recording their votes into computer memory. This paper record is preserved and, depending on state election codes, made available in event of audit or recount.
3. Ballot Marking Devices and Systems	The Ballot Marking Devices and System provide an interface to assist voters with disabilities in marking a paper ballot, which is then scanned or counted manually. Most ballot marking devices provide a touchscreen interface together with audio and other accessibility features, but rather than recording the vote directly into computer memory, the voter's selections are indicated through marking a paper ballot, which is then scanned or counted manually.
4. Punch Card Voting Systems	The Punch Card Voting Systems employ a card (or cards) and a small clipboard-sized device for recording votes. Voters punch holes in the cards (with a supplied punch device) opposite their candidate or ballot issue choice. After voting, the voter may place the ballot in a ballot box, or the ballot may be fed into a computer vote-tabulating device at the precinct.
5. Hand Counted Paper Ballots	A significant number of jurisdictions count paper ballots cast in polling places by hand and even more count absentee and/or provisional ballots by hand. While not a type of "voting equipment," beyond the pen or pencil used by the voter to mark the ballot, many of the issues of ballot design and voter intent that effect all voting systems are relevant to hand counted paper ballots as well.

Source: Office of Inspector General (OIG)-generated based on background research

The risk to computer-enabled election systems varies by county, depending on the types of devices and processes used by polling stations. For example, elements of the Nation's election infrastructure that are potentially vulnerable to cyber intrusions include:

- <u>Electronic Voting Systems</u>: 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 government information technology solutions generally include a public Internet-connected portion that is used to report election results to the general public and media on election day, which some states have begun migrating to the cloud. The public Internet could be used to report inaccurate vote results to the public and media.

Responsibility for Securing the Election Infrastructure

DHS plays a central role in protecting the Nation's critical infrastructure. DHS' Cybersecurity and Infrastructure Security Agency leads coordination efforts to manage risks to the Nation's 16 critical infrastructure sectors. These sectors include systems and assets, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[3] Election infrastructure is a subsector of the government facilities sector, which includes a wide variety of buildings located in the United States and overseas and owned or leased by Federal, state, local, or tribal governments. These facilities include general use office buildings and special-use military installations, embassies, courthouses, national laboratories, national monuments and icons.[4]

On January 6, 2017, Secretary Johnson designated the election infrastructure as a subsector of the government facilities critical infrastructure sector under DHS' purview.[5] In his designation, Secretary Johnson stated that election infrastructure was vital to our national interest, cyber attacks on this country are becoming more sophisticated, and bad cyber actors — ranging from nation states, cyber criminals, and hacktivists — are becoming more dangerous.

[3] On November 16, 2018, the President signed the *Cybersecurity and Infrastructure Security Act of 2018* (Public Law 115-278), re-designating the previous National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA).

[4] 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.

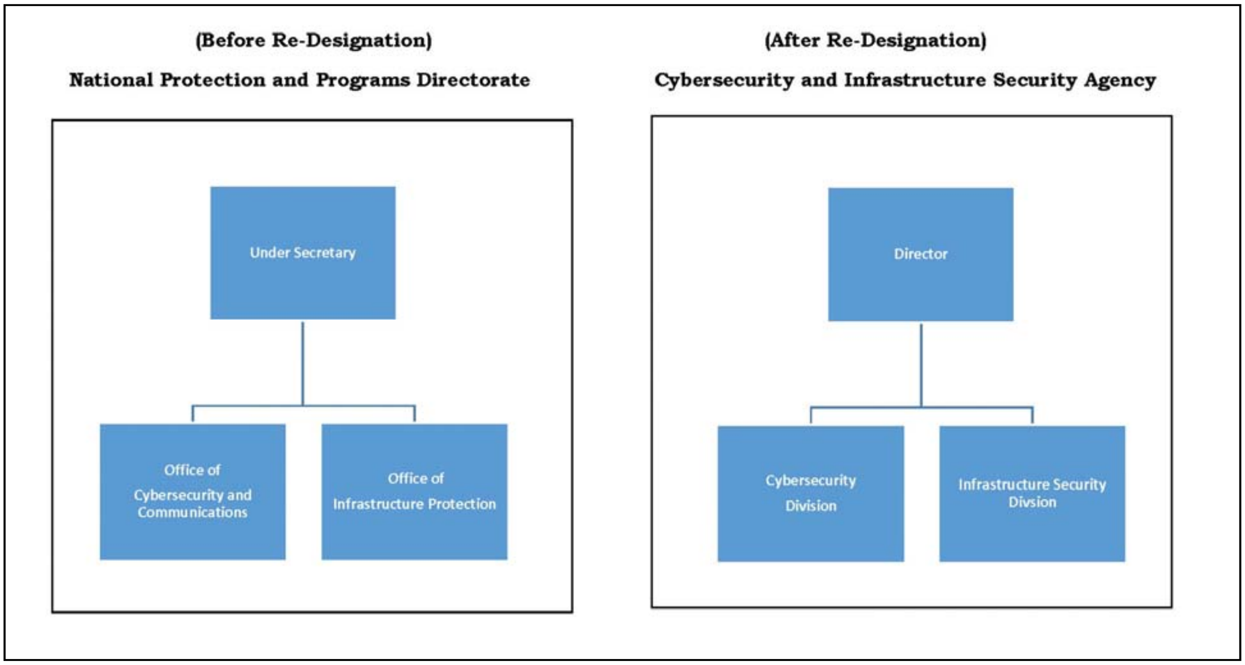
[5] *Statement by Secretary Jeh Johnson on the Designation on Election Infrastructure as a Critical Infrastructure*, January 6, 2017. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, designates DHS and the General Services Administration as co-Sector Specific Agencies for the government facilities sector.

Subsequently, Secretary John Kelly affirmed the designation during a Congressional hearing on June 6, 2017. The election infrastructure subsector includes storage facilities, polling places, and centralized vote tabulation locations used to support the election process, as well as information and communications technology. The subsector also includes voter registration databases, voting machines, and other systems used to manage the election process and report election results on behalf of state and local governments. Under the new designation, states that voluntarily request DHS' assistance (e.g., cyber and physical security) would have priority access to threat intelligence and the ability to participate in joint cybersecurity defense exercises to help safeguard their election infrastructures.

As part of critical infrastructure sectors, information about security and vulnerabilities, shared with the Federal government under the *Critical Infrastructure Information Act,* is considered Protected Critical Infrastructure Information. Under this designation, Protected Critical Infrastructure Information is not subject to disclosure under the *Freedom of Information Act* and state, local, tribal, and territorial disclosure laws. This protection allows the critical infrastructure community to discuss vulnerabilities and problems without the fear of publicly exposing sensitive information.

Prior to CISA's re-designation, the Office of Cybersecurity and Communications and its Office of Infrastructure Protection jointly assisted state and local partners by conducting and facilitating vulnerability assessments to help identify and address risks to election infrastructure. Together, the offices provided information on emerging threats so that state and local officials could take appropriate actions to mitigate potential risks. In addition, DHS offered tools and training to its state and local partners to manage the risks associated with their assets, systems, networks and facilities. DHS' Cybersecurity and Infrastructure Security Divisions, within CISA, still provide the same kind of assistance, information, tools and training. Figure 3 depicts a simplified organizational chart for the offices primarily responsible for securing election infrastructure before and after CISA's re-designation.

Figure 3: Simplified Organizational Chart of Offices Before and After Re-Designation


(Before Re-Designation)
National Protection and Programs Directorate
Under Secretary
Office of Cybersecurity and Communications
Office of Infrastructure Protection
(After Re-Designation)
Cybersecurity and Infrastructure Security Agency
Director
Cybersecurity Division
Infrastructure Security Divsion

Source: OIG-generated based on background research

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. Subsequent to the issuance of our draft report, the previously known National Protection and Programs Directorate was re-designated as CISA. For the purpose of this report, we will continue to refer to the prior National Protection and Programs Directorate as CISA.

Results of Audit

DHS has taken some steps to mitigate risks to the Nation's election infrastructure; however, improved planning, more staff, and clearer guidance could better facilitate the Department's coordination with state and local officials. Specifically, despite Federal requirements, DHS has not completed the plans and strategies critical to identifying emerging threats and mitigation activities, or established metrics to measure progress in securing the election infrastructure. Senior leadership turnover and insufficient guidance and administrative staff have hindered DHS' ability to accomplish such planning. Until such issues are addressed and resolved, DHS cannot ensure effective guidance and a well-coordinated approach to securing the Nation's election infrastructure.

Further, DHS provides assistance to state and local election officials upon request. Over time, the assistance provided has increased and the quality of information shared has improved. However, insufficient staff, a lengthy security clearance process for state and local election officials, and state and local officials' historic mistrust of Federal government assistance hamper DHS' ability to provide the services and assessments needed to secure the election infrastructure. Addressing these issues is essential for continued improvement in the services, outreach, and quality of information DHS shares with election stakeholders.

Planning Activities to Secure the Election Infrastructure Can Be Improved

DHS developed and implemented the *Election Infrastructure Subsector-Specific Plan*. This plan facilitates collaboration among stakeholders in the private sector; Federal, state, local, tribal, and territorial governments; and nongovernmental organizations to reduce risks to the Nation's election infrastructure. However, DHS has not updated critical plans or strategic documents concerning the election infrastructure. These updates are necessary to align and prioritize DHS' efforts and establish metrics for measuring progress for the election infrastructure. Completing such plans and strategies would guide DHS' efforts with an organized strategy and establish the foundation for success.

A shortage of administrative staff has hindered DHS' ability to secure the election infrastructure. Without adequate planning, DHS cannot guarantee that the Department is providing effective strategic guidance, promoting a national unity of effort, and coordinating the overall Federal effort to secure the Nation's election infrastructure.

Planning Requirements for Protecting Critical Infrastructures and Measuring Progress

As previously stated, based on responsibilities identified within the *National Infrastructure Protection Plan*, in January 2017, Secretary Johnson designated election infrastructure as part of DHS' responsibility to secure the government facilities sector.[6] Consequently, CISA became responsible for updating associated plans to address potential election infrastructure risks. Consistent with the Secretary's designation and Federal law, CISA's planning includes

[6] *Statement by Secretary Jeh Johnson on the Designation on Election Infrastructure as a Critical Infrastructure*, January 6, 2017

establishing program goals and measuring program performance against those goals. The goals must be quantifiable and measurable with clearly defined milestones.

DHS Needs to Update Its Security Planning Documents to Include Election Infrastructure and Associated Risks

DHS developed only one security planning document to address the election infrastructure, the *Election Infrastructure Subsector-Specific Plan*.[7] The mission, vision, and goals described in the subsector-specific plan set the strategic direction and provide important information on the election infrastructure sector and risk management approaches to enhance the sector's security. The plan describes significant risks and risk management activities for the sector. Although the plan outlines short-, medium-, and long-term goals and priorities, it does not include milestones to evaluate the progress and effectiveness of its activities to secure the election infrastructure.

DHS has not included the election infrastructure in other key security planning documentation to ensure a unity of effort in coordinating departmental cybersecurity activities to secure the subsector. Therefore, the following plans do not identify the specific goals, objectives, milestones, and priorities needed to monitor and secure the election infrastructure.

- *DHS Cybersecurity Strategy*: This document establishes a 5-year framework to fulfill the Department's cybersecurity responsibilities by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making cyber infrastructure more secure and resilient.

- *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 a 2009 version of the plan because of significant changes in the critical infrastructure risk, policy, and operating environment. In January 2017, Secretary Johnson announced that the Nation's election infrastructure should be recognized as a priority in any future version of this plan; however, as of September 2018, DHS has not

[7] *Election Infrastructure Subsector-Specific Plan* is an annex to the 2013 *National Infrastructure Protection Plan*

updated the plan as expected—more than 18 months later. DHS officials provided no estimated date for revising the plan.

- *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. DHS officials said that, using the *Election Infrastructure Subsector-Specific Plan* as a foundation, the Department plans to coordinate with the General Services Administration to update the *Government Facilities Sector-Specific Plan.*

- *Assistant Secretary's Strategic Intent for FY 2018*: This document establishes goals and priorities for CISA's fiscal year 2018 efforts to enhance its cybersecurity workforce, increase risk management, improve cybersecurity to critical systems, and foster information sharing with priority partners in all sectors.

- *Office of Cybersecurity and Communications Annual Operating Plan for 2018*: This document outlines the Assistant Secretary's priorities for FY 2018 and the approaches to implementing these priorities.

CISA officials told us they anticipate completing and approving the cybersecurity strategy and implementation plans, including defined roles and responsibilities, key milestones, and performance measures, by late 2018.

Hindrances to Completing Planning to Secure the Election Infrastructure

Department leadership changes, a prolonged management vacancy at CISA, insufficient resources, and lack of staff support have delayed the Department's efforts to complete its election infrastructure planning.

Specifically, there were two DHS Secretaries within the first 12 months of the current Administration, the Deputy Secretary retired after 12 months, and the leadership position at CISA (i.e., former Under Secretary) was vacant until June 15, 2018. Amid the leadership vacancies and turnover at both levels, CISA did not prioritize key activities or establish effective performance measures to monitor its progress in accomplishing its mission and goals of securing the Nation's election infrastructure. With new leadership as of June 2018, CISA began efforts to develop the needed plans and strategies to secure the election infrastructure.

CISA did not have adequate staff to develop the required strategies, plans, and documents to ensure that election infrastructure needs and issues are addressed and progress is properly monitored. As of May 2018, CISA had 11 staff working full-time on election infrastructure security. However, the majority of these staff either were on detail from other CISA divisions (including the Director and four task force staff) or were contract personnel, lacking vested interest and providing no assurance of sustained administrative support for the long term.

Further, CISA has not defined the organizational structure, delineated the roles and responsibilities, or developed procedures for the assigned staff. In the absence of sustained administrative support to lay a foundation for securing the subsector, CISA focused on operational activities, such as participating in a series of coordination meetings with state and local officials and providing assistance to them. Stakeholders we interviewed, including state and local election officials, expressed concerns about inadequate DHS staffing, which they reported hindered their ability to develop relationships necessary for open dialogue on subsector vulnerabilities and problems.

Consequences of Insufficient Security Planning

Comprehensive planning to secure the election infrastructure is essential, especially given the myriad of election systems, storage facilities, polling places, vote tabulation locations, and information and communications technology facilities that support the election process. Without a well-defined and organized strategy with specific priorities, key milestones, and goals and objectives, the Department cannot ensure the actions taken to secure the election infrastructure are effective. Developing well-defined and organized plans and strategies with metrics, specific timeframes, and milestones will provide a clear roadmap for achieving the Department's goals to secure election infrastructure.

Specifically, without updating the *National Infrastructure Protection Plan*, DHS may not have identified all threats and vulnerabilities associated with the election infrastructure subsector and areas for mitigating potential risks. Until this plan is updated to include the election infrastructure, DHS cannot achieve its 2013 goals to (1) assess and analyze threats to vulnerabilities of, and consequences to critical infrastructure, (2) enhance critical infrastructure resilience through advance planning and mitigation efforts, and (3) share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.[8]

Updating other foundational documents, such as the DHS *Cybersecurity Strategy and Government Facilities Sector-Specific Plan* to include the election infrastructure subsector, can help guide DHS' coordination efforts with state and local government officials. Without appropriate plans in place, DHS cannot effectively communicate with appropriate stakeholders or respond to potential security incidents or adverse events.

DHS Can Enhance Its Coordination with and Assistance to State and Local Governments

DHS provides assistance to state and local election officials upon request. Over time, the assistance has increased and the quality of information shared has improved. However, some state and local officials lacked the proper clearances needed to receive classified information. Insufficient staffing, a lengthy security clearance process, and historic mistrust of the Federal government's assistance have restricted DHS' ability to provide the additional services, assessments and outreach needed to secure the election infrastructure. By addressing and resolving these issues, DHS can improve its efforts to assist stakeholders in safeguarding our Nation's election infrastructure.

Guidance on Providing Technical Assistance and Sharing Cyber Information in Critical Sectors

Both the President and the Department have provided guidance for DHS to assist state and local governments in securing the Nation's critical infrastructure. Specifically, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, requires the 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. Further, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* requires:

- Federal agencies to increase the volume, timeliness, and quality of cyber threat information shared with critical infrastructure owners, and

- DHS to expedite the processing of security clearances to appropriate

[8] *National Infrastructure Protection Plan 2013*

critical infrastructure personnel to facilitate information sharing.

In designating election infrastructure as a critical infrastructure subsector, Secretary Johnson also required DHS to:

- prioritize cybersecurity assistance to state and local election officials upon request, including the sharing of information to identify and mitigate system vulnerabilities, and

- grant security clearances to election officials to receive classified cyber threat information, as appropriate.

DHS Activities to Assist State and Local Governments

Since the designation of the election infrastructure as a subsector of the government facilities sector, DHS has taken various actions to coordinate with state and local election officials. The actions include participating in a series of coordination meetings with state and local election officials, private sector companies, and Federal partners to raise awareness of cybersecurity issues related to the Nation's election infrastructure. Some of the partners that DHS coordinates with include the Election Assistance Commission, the National Association of Secretaries of States, and the National Association of State Election Directors.

To help improve the security of the election infrastructure and facilitate information sharing, DHS also assisted in establishing the following entities:

- Election Infrastructure Subsector Government Coordinating Council to enable sharing of threat information between the Federal government and the council partners, and promote the Department's risk management efforts and available services to mitigate subsector threats.

- Elections Infrastructure Information Sharing and Analysis Center to provide election-focused cyber defense measures, sector-specific threat intelligence products, and threat and vulnerability monitoring services. All 50 States and 849 local jurisdictions have signed up for the cyber threat information sharing service from the Election Infrastructure Information Sharing and Analysis Center.

- Election Task Force to centralize the coordination of the Department's assistance to state and local governments with their election infrastructure.

- Government Facilities Sector Election Infrastructure Subsector Coordinating Council to enable information sharing and collaboration on best practices to mitigate and counter threats to election infrastructure.

From April to August 2018, DHS took the following actions to improve information sharing and raise cyber threat and incident awareness with state and local officials:

- published guidance on various threats and best practices (e.g., ransomware, and hypertext transfer protocol secure);[9]

- issued guidance on securing voter registration databases that identified potential threats and prevention measures;

- established the Communication Protocol and Notification Process for the election infrastructure subsector to improve the flow of information between Federal and state election officials by defining the requirements for information sharing, reporting incidents and threats, and responding to potential incidents;

- disseminated the *Incident Handling Overview for Election Officials* to provide incident handling steps to assist with incident readiness and response;

- published *Best Practices for Continuity of Operations* to provide recommended guidance and consideration for stakeholders to address as part of their network architecture, security baseline, continuous monitoring, and incident response practices;

- attended the National Association of State Election Directors and National Association of Secretaries of State Annual Conference to discuss cybersecurity and best practices;

- released the Department's "The Last Mile" cybersecurity awareness poster. The poster provides a thorough overview of the cybersecurity environment of a particular state to enhance cybersecurity planning at the local level. To date, DHS completed the "Last Mile" cybersecurity poster project for six states; and

[9] The Hyper Text Transfer Protocol Secure is an Internet communication protocol used to encrypt and securely transmit information between a user's web browser and the website to which they are connected.

- participated in joint meetings and briefings with Facebook, the Federal Bureau of Investigation, and state and local election officials to discuss recent actions taken to counter foreign threats and malicious interference operations.

In addition, DHS performs services to raise the situational awareness of individual state and local election organizations concerning election infrastructure issues, such as strategic cyber messaging, cyber and physical security assessments, and incident coordination.[10] DHS also performs no-cost cybersecurity assessments for state and local election organizations, including:

- Risk and Vulnerability Assessment: Combines national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide actionable remediation recommendations prioritized by risk.
- Cyber Infrastructure Survey: Evaluates the effectiveness of more than 80 cybersecurity controls, including incident response capabilities.
- Cyber Resilience Review: Assesses cybersecurity management capabilities and maturity as applied to protect critical information technology services.
- External Dependency Management: Assesses activities and practices used to identify, analyze, and reduce supply chain risks.
- Cyber Hygiene Scanning: Assesses systems on a continual basis and remotely to identify vulnerabilities and configuration errors.
- Cybersecurity Exercises: Assists election infrastructure partners in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities.

Further, DHS is providing funding for the Election Infrastructure Information Sharing and Analysis Center to install intrusion detection capabilities (i.e., sensors) on election networks. According to DHS in July 2018, these sensors covered election infrastructures in 35 states and 23 counties. DHS planned to deploy sensors to additional entities before the 2018 midterm elections.

[10] Cyber strategic messaging includes briefings, keynotes, and panel discussions to help improve cybersecurity awareness and organizations' cybersecurity postures.

From May to August 2018, DHS conducted a series of tabletop exercises in six counties in New York with a focus on protecting the integrity of the state's electoral systems against cyber attacks. Similarly, DHS hosted a 3-day exercise to assist its Federal partners, state and local election officials from 44 states and the District of Columbia and private vendors in identifying best practices and areas of improvement in Federal and state cyber incident planning, preparedness, identification, response, and recovery.

DHS Assistance to State and Local Governments Has Increased

To support state and local election officials in securing election infrastructure, DHS offers individual cyber and physical security assessments and services upon request. As of September 2018 DHS had performed the following:

- 64 assessments that include a mix of cyber infrastructure surveys, cyber resilience reviews, and external dependency management for 24 states (including 26 assessments since June 1, 2018),

- 23 risk vulnerability assessments for 18 states, and

- 219 outreach engagement activities for 43 states, including the District of Columbia (83 engagements since June 1, 2018).

As part of its protective and vulnerability mitigation services, DHS offers physical security assessments to state and local election officials. A program official told us that, as of July 2018, CISA had performed nine physical assessments, all of which were for one state. In addition, as of September 2018, the protective security advisors performed 68 security walkthroughs and 583 outreach engagements (training, security briefing).

Quality of Information Shared Has Improved

Initially, the Department did not provide stakeholders with a comprehensive summary (e.g., trend analysis, common vulnerabilities) of the threats associated with the election infrastructure, by consolidating the results from the assessments performed or compiling actionable information that stakeholders can use to mitigate potential risks. For example, CISA did not provide an overview or summary analysis of onsite election infrastructure assessments performed for the FY. In addition, CISA did not provide quantitative and qualitative summaries of assessment types, geographic locations, findings, and recommended mitigation strategies and best practices.

Subsequently, CISA officials provided us with lessons learned from technical assessments conducted by the Department's National Cybersecurity Assessments and Technical Team. Based on the current dataset, the team concluded that there is no clear difference in the cyber vulnerability posture of the election infrastructure as compared to the information technology environments in other critical infrastructure sectors. In addition, the lessons learned identified the top five election infrastructure vulnerabilities, based on the results of the team's assessments.

Hindrances to DHS' Election Infrastructure Security Efforts

Insufficient operational staff, a lengthy security clearance process, and historic mistrust between Federal and state and local officials have hindered DHS' ability to make significant progress in performing more assessments and providing technical assistance to secure the Nation's election infrastructure. Such hindrances were raised during a congressional hearing in October 2017. Specifically, a member of the House of Representatives raised concerns about the lengthy clearance process for election officials, reports of long wait times for DHS to perform a risk and vulnerability assessment, and the Department's struggle to build relationships with state and local officials.

Additional Staff Can Enhance DHS' Abilities to Provide Technical Assistance and Outreach

DHS' inability to provide more assistance to state and local election officials was due, in part, to staffing shortages. Currently, DHS does not have dedicated staff focused on election infrastructure. In total, DHS has 102 advisors who provide technical assistance and perform security assessments for all 16 critical infrastructure sectors. Twelve advisors focus on cybersecurity and 90 protective security advisors. The cybersecurity and protective security advisors serve as critical infrastructure security and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other DHS offices. As part of their duties, the advisors offer cyber and physical security training for all 16 critical infrastructure sectors. The advisors also serve as field agents, to promote CISA's outreach and partnership effort to provide technical assistance, improve cyber and physical security awareness, share information with state and local election officials as well as other services and products that DHS offers to the 16 critical infrastructure sectors. For example, these advisors may be required to work on transportation, maritime, and chemical facilities protection on any given day.

Our interviews with six cybersecurity advisors and eight regional directors for the protective advisors disclosed concerns that CISA is not adequately staffed to provide support to state and local election officials in their efforts to secure the election infrastructure. According to selected regional directors, because each advisor is responsible for all 16 critical sectors, the advisors may not be able to provide sufficient attention to secure the election infrastructure. Each advisor's workload depends on the number of assigned election jurisdictions (i.e., counties), which may vary across states. For example, as of March 2013, there were 3,242 counties and county equivalents in the 50 states, District of Columbia, and other U.S. territories. One CISA protective security advisor expressed concerns about being assigned to 6 states; however, there could be more than 80 counties or election jurisdictions in one state alone. Both cybersecurity and protective security advisors expressed concerns about the outreach efforts they must also perform to satisfy needs at the county and local levels.

Further, some advisors informed us that their priorities may change as they are required to focus on the next widespread or known event affecting the Nation. For example, some advisors told us that they had to provide ad-hoc active shooter training to combat and protect against school shootings at selected states. When their assistance is needed, advisors have to allocate their time to perform tasks in preparation for, during, and after annual special events that take place across the country, such as the National Football League's Super Bowl, Marine Corps Marathon, National Police Week, and Indianapolis 500 auto race.

To build a trusted relationship with state and local officials, some advisors expressed the need for performing periodic cyber and physical assessments on the election infrastructure. The advisors also expressed the need of having one national cyber team dedicated to perform comprehensive risk vulnerability assessments and cyber threat hunting activities for the election infrastructure. Some advisors also recommended that CISA establish dedicated cyber and incident response teams by region or state to serve better state and local election officials and other critical infrastructure sectors.

CISA officials acknowledged that staffing shortages have hindered DHS' efforts to secure the Nation's election infrastructure. At the same time, they advised that the Department is taking actions to alleviate some of these concerns. According to these officials, as part of their regular duties all 10 Regional Directors are responsible for outreach efforts for the election infrastructure. Also, CISA hired 12 additional cybersecurity advisors in FY 2017 and anticipates hiring 4 more cybersecurity and 10 protective security advisors in FY 2018. CISA plans to hire seven more protective security advisors in FY 2019. Further, CISA has requested 20 more advisor positions in the Department's FY 2020 budget request, which is pending the Department and congressional budget review process.

Lengthy Security Clearance Process

According to state and local officials, a second factor that hinders DHS' efforts to secure the election infrastructure is the lengthy security clearance process. One Federal election official told us that it took him more than a year to obtain a security clearance. Initially, DHS could not share actionable classified information with state and local election officials until the officials obtained proper security clearances. Some officials, such as secretaries of state and state election directors, experienced long delays in obtaining security clearances. As of July 2018, DHS had granted interim/secret clearances to 87 (87 percent) of the total 100 state election officials eligible to receive clearance. According to DHS documentation, for the 43 security clearances fully granted, the average time to complete the process was 4 months with the longest time of 9 months. Of the remaining 44 security clearances granted on an interim status (still pending), the average time was approximately 2 months.

State and local officials are subject to the same investigative and adjudicative requirements as their Federal counterparts. Eligibility determinations and subsequent access to classified information are dependent upon a favorable adjudication of the state and local officials' background investigation and their signing a non-disclosure agreement. Although the Department has no control over these security clearance investigations, which are performed by another agency, DHS' Office of Intelligence and Analysis (I&A) processes such requests to obtain clearance. I&A experiences delays in processing security requests because the office does not have enough staff. According to an I&A official, the office only has four staff to process security clearance requests for state and local election officials. These 4 staff process clearance requests for about 5,000 individuals assigned to state, local, and tribal territory entities.[11]

The lack of timely security clearances for state and local election officials affects DHS' ability to share classified information timely and effectively with them. According to CISA officials, to combat this common problem with security clearances for the Federal government, DHS offers 1-day read-ins to provide classified information to election officials with the need to know in every state. In addition, CISA officials stated that DHS has to maintain the same classification for information they received unless the Original

[11] The mission of the DHS I&A is to provide the Department with the intelligence and information it needs to keep the Nation safe, secure, and resilient. The office works closely with other components, intelligence organizations, and state, local, tribal, and private sector entities to ensure non-traditional streams of information are fused with traditional Intelligence Community sources to provide a complete assessment of threats to the Nation.

Classification Authority declassifies the information. DHS partners and state officials told us that the Department may take more than 2 weeks to declassify cyber-related indicators; as a result, the indicators are not considered timely or actionable. According to these state and local election officials, they attended a DHS-sponsored classified briefing in which they did not receive any new or value-added information from the meeting, as the information DHS shared was the same as that already reported in the news media.

Historic Mistrust of Federal Involvement

According to select state and local election officials, after Secretary Johnson designated the election infrastructure as a subsector of the government facilities sector, mistrust contributed to their reluctance to request DHS' assistance. Officials stated this mistrust stems from long-standing sensitivity over how states administer and conduct elections. State officials were concerned that the Federal Government might usurp their autonomy over the election process. Secretary Johnson emphasized designating the election infrastructure as a subsector to the existing government Facility sector. However, this did not supplant the role state and local governments have in administering and conducting elections. During our interviews with selected state and local officials from April to May 2018, they cited a lack of trust as the main obstacle to requesting the Department's assistance in securing their election infrastructures.

In January 2018, CISA acknowledged that DHS did not have effective relationships with state and local election officials, and it would take time and effort to improve the partnerships. To alleviate some concerns, DHS prioritized providing services and support to state and local election officials, including assisting these officials in obtaining security clearances and expediting physical and cybersecurity assessments for election stakeholders. According to DHS, virtually no backlog existed for automated assessments such as cyber-hygiene scans. However, narrative risk and vulnerability assessments are more labor-intensive, entail interviews and analysis, and may take more than 2 weeks. To help build trust, DHS hired a subject matter expert to improve its strategic outreach to state and local election officials in May 2018.

Through such guidance and engagement, DHS has made strides in increasing trust. In addition, I&A and CISA officials have discussed transferring security clearance processing for state and local election officials to CISA's Private Sector Clearance Program Division by November 2018, as a means of streamlining the process.

Results of Limited DHS Assistance to Election Stakeholders

More improvements are needed for the Department to assist stakeholders in addressing evolving threats to the Nation's election infrastructure. With the November 2018 mid-term elections fast approaching, securing the Nation's election infrastructure is more critical with each passing day. Specifically, in an August 2, 2018 press conference, the heads of the Intelligence Community and Federal law enforcement agencies confirmed that the threat to our Nation's election infrastructure is real and is continuing.[12] Further, after the press conference, Facebook, Microsoft, and Twitter announced they continue to discover and remove suspicious accounts and propaganda webpages connected to foreign governments that are aiming to influence the mid-term elections.

With additional staff, DHS can expand its services and provide more technical assistance and actionable information to state and local election officials to mitigate risks associated with the subsector. Increased staff can help CISA perform more outreach efforts to persuade state and local officials to request technical assistance and exchange relevant information and dispel suspicion about DHS' efforts to secure the subsector. More timely security clearances for state and local election officials will facilitate access to the classified data and threat assessments they need to secure their election systems.

Recommendations

We recommend the Director of CISA:

Recommendation 1: Prioritize hiring administrative and operational staffing to conduct the strategic planning, coordination, performance measurement, and physical and cybersecurity activities needed to mitigate election infrastructure risks effectively.

DHS Comments to Recommendation 1

CISA concurred with recommendation 1. CISA has already prioritized hiring for election infrastructure security. For example, in March 2018, CISA hired an official with significant elections expertise to advise the Department on all elections-related matters. Additionally, CISA recently converted the Election Task Force Director from a detail assignment to a permanent position to better manage and institutionalize the task force's work. CISA will apply lessons

[12] *Press Briefing by Press Secretary Sarah Sanders and National Security Officials*, White House, August 2, 2018

learned from the 2018 election cycle to enhance administrative management, particularly with regard to future staffing plans, and operational oversight.

In addition, CISA currently has three hiring actions in process — two positions that will augment the Sector Specific Agency work and one that will support planning, coordination, and performance management. The Election Task Force, which includes the Election Infrastructure Subsector Sector Specific Agency, has been staffed with full-time personnel and supplemented by a full range of DHS cybersecurity expertise, including personnel from the National Cybersecurity and Communications Integration Center, the National Risk Management Center, I&A, and the intelligence community. Field staff engage directly with election officials to increase information sharing and provide contacts for obtaining needed Federal cybersecurity and physical security resources. CISA will continue to prioritize hiring to mitigate election infrastructure risks effectively. Estimated Completion Date: December 31, 2019.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation 2: Enhance development of situational analysis and assessment summary reports that provide comprehensive information on threats, vulnerabilities, best practices, and security tips to election infrastructure sector stakeholders.

DHS Comments to Recommendation 2

CISA concurred with recommendation 2. As the report details, CISA does, and will continue, to provide services, develop analysis, and share information. More specifically, in 2018 CISA was able to share information with all 50 states and more than 1,400 local jurisdictions through the Election Infrastructure Information Sharing and Analysis Center. Additionally, through funding of the Election Infrastructure Information Sharing and Analysis Center, CISA was able to deploy more than 100 Albert Sensors on election infrastructure, including on over 40 states. CISA also performed weekly cyber-hygiene scans on 141 outward facing election networks, and conducted 35 risk and vulnerability assessments for election stakeholders. The data gained through these robust information sharing and services provided DHS greater, and previously unavailable, insight into the risks facing election systems. Based on this data, the Department developed analytical products on threats and vulnerabilities and shared those with the elections community. CISA views continuing this type of activity as critical to the ongoing success and security of the election subsector.

Moving forward, CISA will be able to build upon its previous work, which has created a foundation for producing a data rich environment and enabling more mature analysis for sharing with stakeholders. Both CISA and the Election Infrastructure Information Sharing and Analysis Center expect to perform these activities on an ongoing basis.

CISA's Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address the issues identified in our report, including the need to update its information sharing strategy, provide outreach and future engagements, and work with established governance structures. Estimated Completion Date: March 29, 2019.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation 3: Identify strategies to increase outreach to ensure state and local level buy-in and participation in activities for securing the election infrastructure.

DHS Comments to Recommendation 3

CISA concurred with recommendation 3. Since establishing elections as a critical infrastructure subsector in January 2017, CISA has focused on building partnerships with state, local, and private sector entities that run elections. This includes creating the Election Infrastructure Subsector Government Coordinating Council and the Election Infrastructure Subsector Coordinating Council. In partnership with both councils, CISA is working with all 50 states and more than 1,400 local jurisdictions to share information and manage risk. This entails establishing information sharing protocols (i.e., procedures) between Federal, state, and local officials regarding how threat information will be shared, how incidents will be responded to, and how all levels of government will communicate ongoing risks and threats to the election infrastructure. Additionally, the Government Coordinating Council has recommended long-term and short-term areas of focus for newly available Election Assistance Commission funding to the states.

CISA has used its field personnel deployed across all 50 states to build relationships and awareness within the election community regarding the support and services CISA offers. These field personnel have attended state and local conferences, provided training, and performed assessments across the country. Moving forward, CISA plans to continue using these personnel to engage with its state and local partners.

CISA has worked with secretaries of state and state election directors on a targeted campaign for local election officials. This effort, known as “the last mile,” has produced county-specific information. Through this last mile effort, CISA also has produced a checklist for each local office to use to build a more resilient election process.

CISA will continue to build upon existing partnerships to reach thousands of elections jurisdictions nationwide. This will involve another national-level tabletop exercise during the summer of 2019, followed by others in the months leading up to the 2020 elections. Such tailored and scalable services not only benefit local-level partners in the elections infrastructure subsector, but also serve as a foundation to expand outreach and services across all sectors.

Further, the Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address issues identified in OIG's report, including the need to update its information sharing strategy, provide outreach and future engagements, and work with established governance structures. Estimated Completion Date: March 29, 2019.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation 4: Enhance and expand the efforts of the Election Task Force, Election Infrastructure Information Sharing and Analysis Center, and other governance structures to share and tailor information that would assist stakeholders in securing the election infrastructure.

DHS Comments to Recommendation 4

CISA concurred with recommendation 4. Development and maturation of the Election Infrastructure Information Sharing and Analysis Center is foundational to continued work in the election subsector. During calendar year 2018, the Election Infrastructure Information Sharing and Analysis Center grew at an unprecedented rate. With more than 1,400 members, including all 50 states and private sector partners, the Election Infrastructure Information Sharing and Analysis Center represents the fastest growing information sharing and analysis center among all critical infrastructure sectors. Throughout 2018, the Center regularly shared tailored information with the election community to help manage risks to its systems. This included deploying more than 100 Albert sensors in more than 40 states, covering election systems that support approximately 90 percent of registered voters across the United States. CISA will continue to work with state and local officials to build the Election Infrastructure Information Sharing and Analysis Center membership, deploy additional Albert sensors, and mature information sharing across the subsector.

In support of the Election Task Force's mission, CISA has moved forward with hiring actions to institutionalize staff supporting election security in more permanent roles. Additionally, CISA continues to fund the information sharing and analysis function to support election officials. DHS has demonstrated commitment to enhancing and expanding support to stakeholders by applying dedicated resources to this mission, these work streams, and the organizations implementing them.

Finally, the Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address issues identified in our report, including the need to update its information sharing strategy, provide outreach and future engagements, and work with established governance structures. Estimated Completion Date: March 29, 2019.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation 5: Collaborate with I&A and the Intelligence Community to improve the sharing of classified information with election infrastructure stakeholders.

DHS Comments to Recommendation 5

CISA concurred with recommendation 5. CISA has worked with and will continue to work closely with I&A to support the Election Infrastructure Subsector. Since the Election Infrastructure Subsector was established, DHS has endeavored to improve information sharing mechanisms with election subsector partners, both at the classified and unclassified levels.

DHS continues to work with its partners in the Intelligence Community to declassify and make available any actionable election sector threat information in a timely manner. As necessary, DHS will relay classified information to appropriate state or local election officials with appropriate security clearances or through 1-day read-ins to stakeholders without clearances.

Further, CISA will continue to work with I&A, the Federal Bureau of Investigation, and other Intelligence Community members to provide classified information to our partners in a more timely and convenient manner. CISA will continue to refine the related processes with our partners to improve the quality of classified information provided, as well as the delivery mechanism used.

CISA requested that OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of DHS Comments

This recommendation will remain unresolved and open until CISA provides additional documentation and an estimated date for completing all corrective actions. Specifically, we request documentation to substantiate CISA's ongoing and future coordination efforts with I&A, the Federal Bureau of Investigation, and the Intelligence Communities to improve the quality and timeliness of classified information CISA provides to its partners.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security (DHS) 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.

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

- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (February 2013),
- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (February 2013),
- Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), and
- Secretarial Memorandum, *Designation of Election Infrastructure as a Subsector of the Government Facilities Critical Infrastructure* (January 2017).

To conduct our audit, we interviewed selected personnel from CISA and I&A concerning the services and assistance each entity provides to state and local election officials. In addition, we interviewed personnel from the following organizations to obtain their perspectives on DHS' efforts to coordinate with key election infrastructure stakeholders:

- The U.S. Election Assistance Commission,
- The National Association of Secretaries of States,
- The National Association of State Election Directors,
- The Election Infrastructure Subsector Government Coordinating Council,
- The Elections Infrastructure Information Sharing and Analysis Center, and

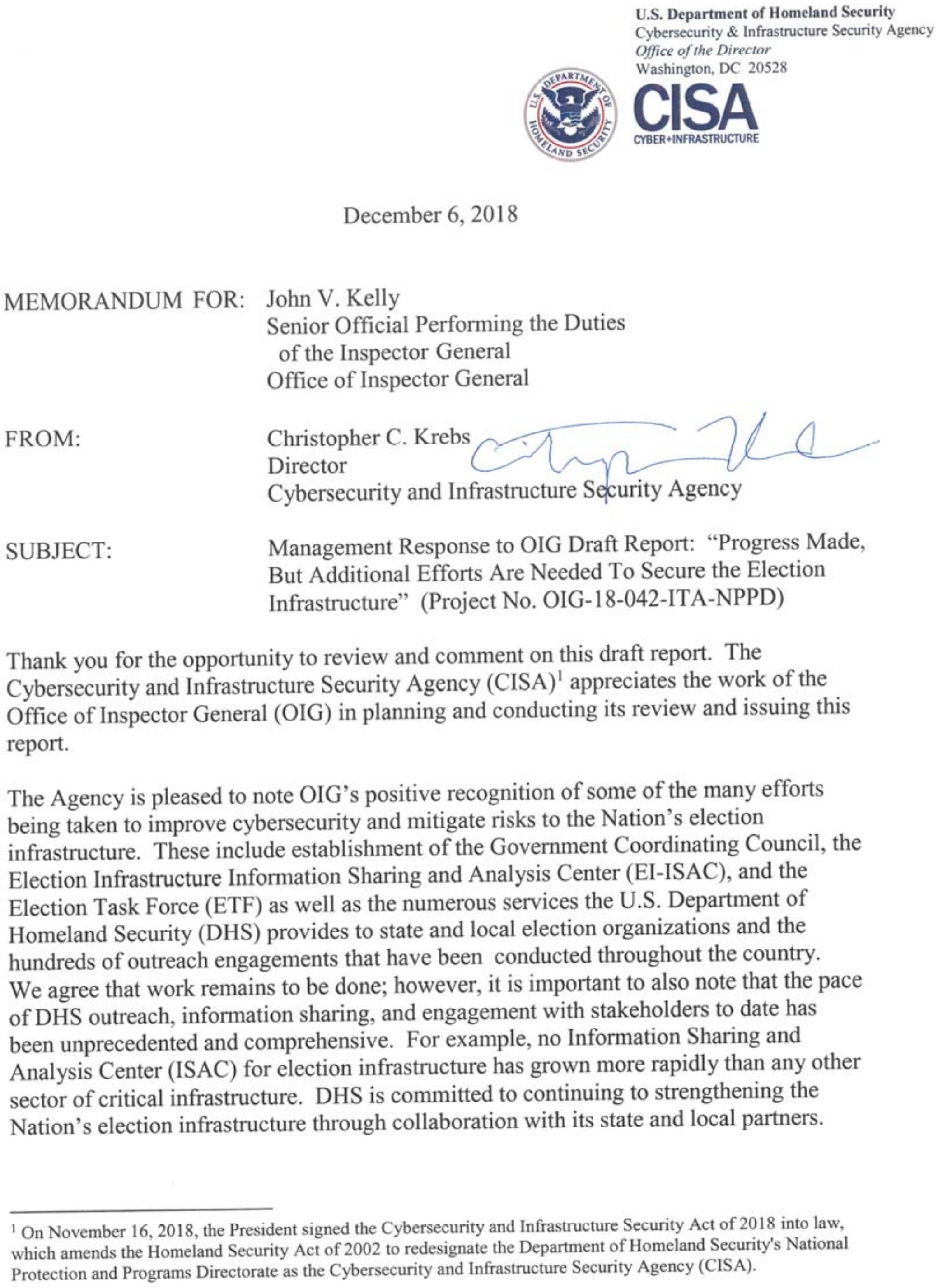
- The Election Center.

As part of our review, we evaluated the actions the Department has taken to protect the election infrastructure subsector of the government facilities sector. We also assessed the effectiveness of the assistance DHS 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 and security clearances granted to state and local officials as part of DHS' 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 with the data.

Although we reviewed classified information related to the election infrastructure, we did not include it in our report. We did not conduct work to determine whether foreign governments interfered in the 2016 election by using social media or other efforts to gain unauthorized access to political parties' information systems. These areas were not under our audit purview.

We conducted this performance audit between January and September 2018 in the Washington, DC 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 that 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

CISA
CYBER+INFRASTRUCTURE

December 6, 2018

MEMORANDUM FOR: John V. Kelly
Senior Official Performing the Duties
of the Inspector General
Office of Inspector General

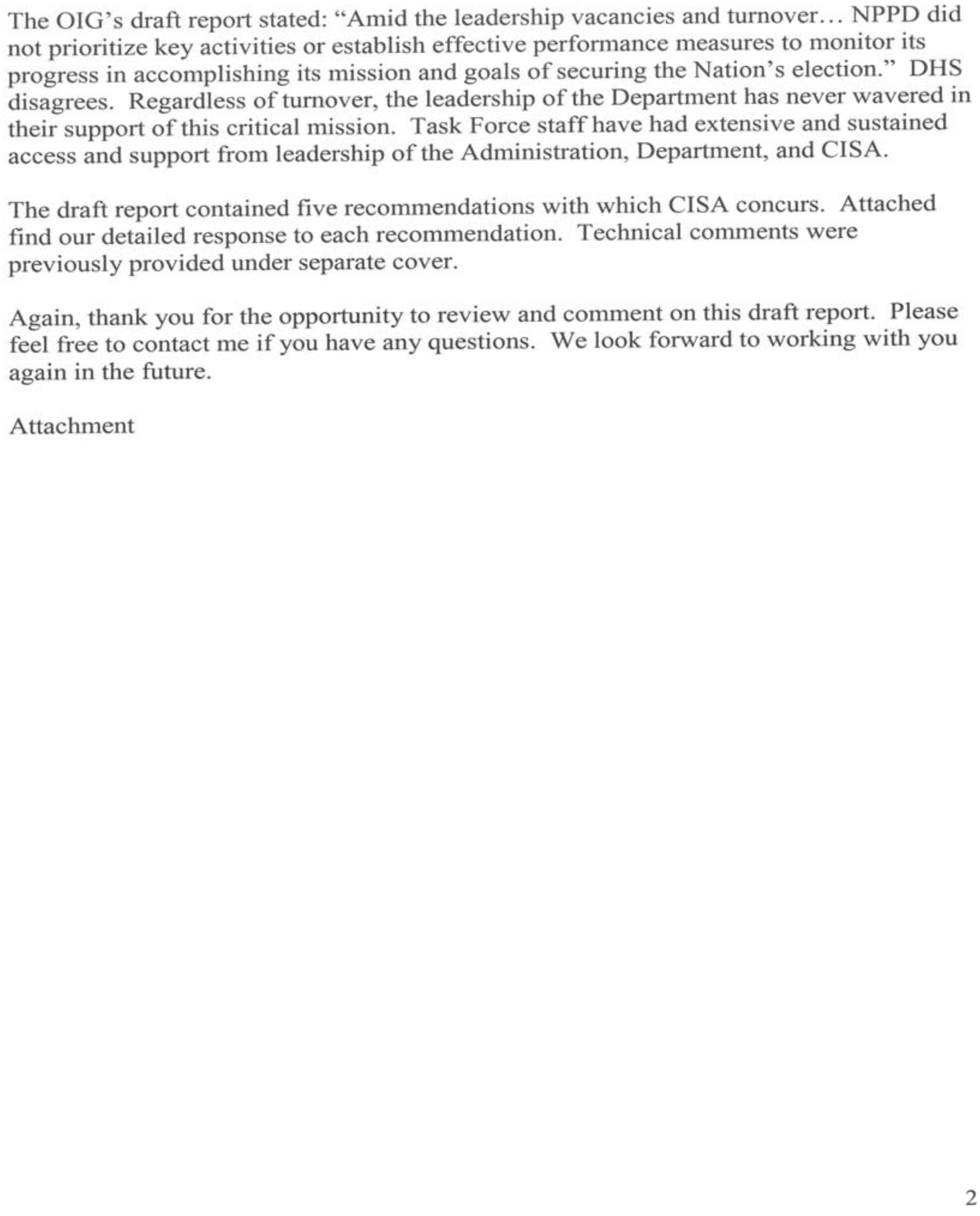
FROM: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to OIG Draft Report: "Progress Made, But Additional Efforts Are Needed To Secure the Election Infrastructure" (Project No. OIG-18-042-ITA-NPPD)

Thank you for the opportunity to review and comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA)[1] appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Agency is pleased to note OIG's positive recognition of some of the many efforts being taken to improve cybersecurity and mitigate risks to the Nation's election infrastructure. These include establishment of the Government Coordinating Council, the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the Election Task Force (ETF) as well as the numerous services the U.S. Department of Homeland Security (DHS) provides to state and local election organizations and the hundreds of outreach engagements that have been conducted throughout the country. We agree that work remains to be done; however, it is important to also note that the pace of DHS outreach, information sharing, and engagement with stakeholders to date has been unprecedented and comprehensive. For example, no Information Sharing and Analysis Center (ISAC) for election infrastructure has grown more rapidly than any other sector of critical infrastructure. DHS is committed to continuing to strengthening the Nation's election infrastructure through collaboration with its state and local partners.

[1] On November 16, 2018, the President signed the Cybersecurity and Infrastructure Security Act of 2018 into law, which amends the Homeland Security Act of 2002 to redesignate the Department of Homeland Security's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA).

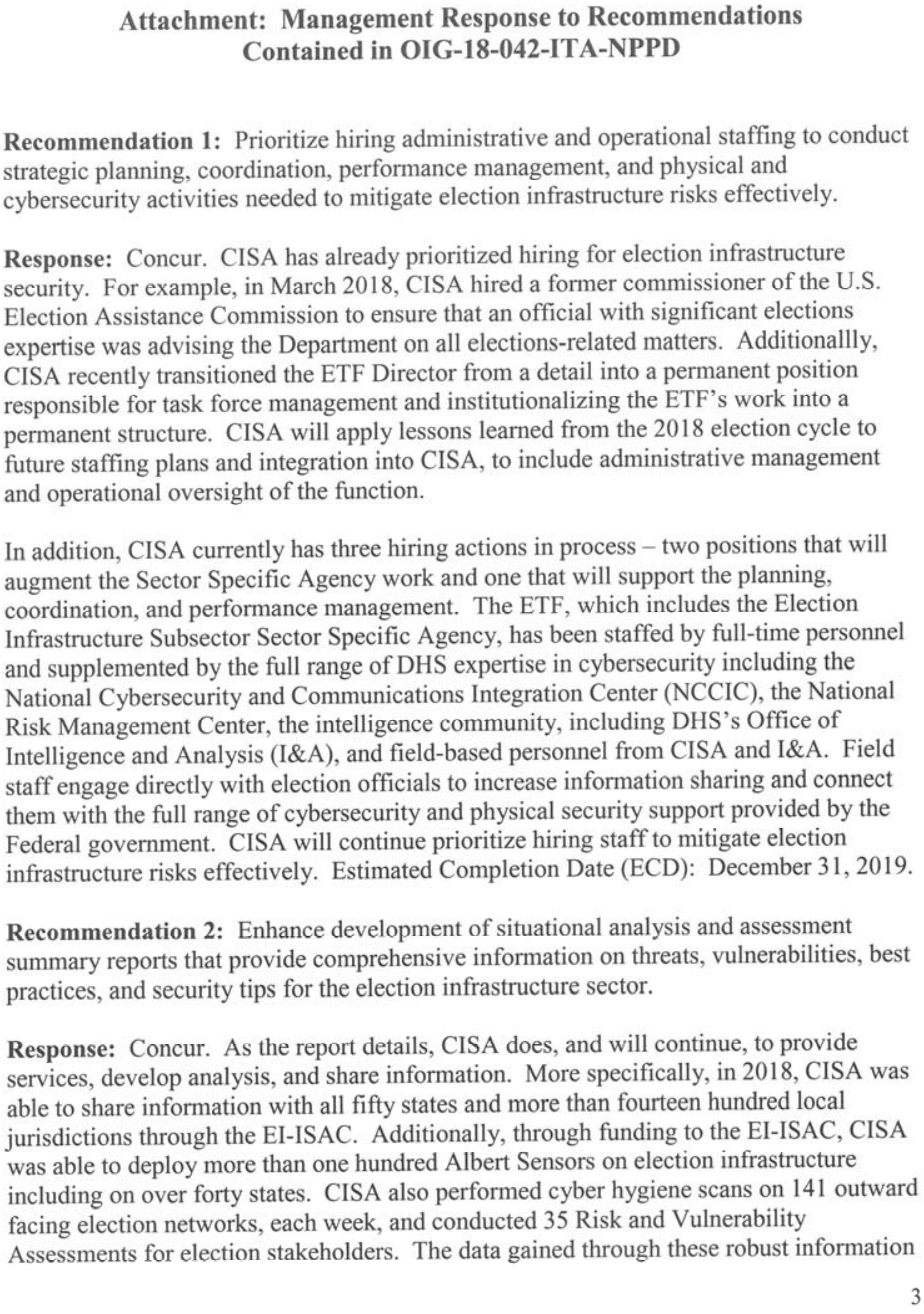


The OIG's draft report stated: "Amid the leadership vacancies and turnover… NPPD did not prioritize key activities or establish effective performance measures to monitor its progress in accomplishing its mission and goals of securing the Nation's election." DHS disagrees. Regardless of turnover, the leadership of the Department has never wavered in their support of this critical mission. Task Force staff have had extensive and sustained access and support from leadership of the Administration, Department, and CISA.

The draft report contained five recommendations with which CISA concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under 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.

Attachment



Attachment: Management Response to Recommendations Contained in OIG-18-042-ITA-NPPD

Recommendation 1: Prioritize hiring administrative and operational staffing to conduct strategic planning, coordination, performance management, and physical and cybersecurity activities needed to mitigate election infrastructure risks effectively.

Response: Concur. CISA has already prioritized hiring for election infrastructure security. For example, in March 2018, CISA hired a former commissioner of the U.S. Election Assistance Commission to ensure that an official with significant elections expertise was advising the Department on all elections-related matters. Additionallly, CISA recently transitioned the ETF Director from a detail into a permanent position responsible for task force management and institutionalizing the ETF's work into a permanent structure. CISA will apply lessons learned from the 2018 election cycle to future staffing plans and integration into CISA, to include administrative management and operational oversight of the function.

In addition, CISA currently has three hiring actions in process – two positions that will augment the Sector Specific Agency work and one that will support the planning, coordination, and performance management. The ETF, which includes the Election Infrastructure Subsector Sector Specific Agency, has been staffed by full-time personnel and supplemented by the full range of DHS expertise in cybersecurity including the National Cybersecurity and Communications Integration Center (NCCIC), the National Risk Management Center, the intelligence community, including DHS's Office of Intelligence and Analysis (I&A), and field-based personnel from CISA and I&A. Field staff engage directly with election officials to increase information sharing and connect them with the full range of cybersecurity and physical security support provided by the Federal government. CISA will continue prioritize hiring staff to mitigate election infrastructure risks effectively. Estimated Completion Date (ECD): December 31, 2019.

Recommendation 2: Enhance development of situational analysis and assessment summary reports that provide comprehensive information on threats, vulnerabilities, best practices, and security tips for the election infrastructure sector.

Response: Concur. As the report details, CISA does, and will continue, to provide services, develop analysis, and share information. More specifically, in 2018, CISA was able to share information with all fifty states and more than fourteen hundred local jurisdictions through the EI-ISAC. Additionally, through funding to the EI-ISAC, CISA was able to deploy more than one hundred Albert Sensors on election infrastructure including on over forty states. CISA also performed cyber hygiene scans on 141 outward facing election networks, each week, and conducted 35 Risk and Vulnerability Assessments for election stakeholders. The data gained through these robust information

3

sharing and services provided DHS greater and previously unavailable insight into the risks facing election systems. Based on this data, the Department developed analytical products on threats and vulnerabilities and shared those with the elections community. CISA views continuing this type of activity to be critical to the ongoing success and security of the subsector.

Moving forward, CISA will be able to build upon its previous work, which has created a foundation that will, over time, produce a data rich environment, and enable more mature analysis to be conducted and shared back with the stakeholders. This is expected to be ongoing and continuous activities performed by both CISA and the EI-ISAC.

CISA's Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address the issues identified in OIG's report, at appropriate, including our strategy for information sharing, outreach and future engagements, and work with established governance structures. ECD: January 31, 2019.

Recommendation 3: Identify strategies to increase outreach to ensure state and local level buy-in and participation in activities for securing the election infrastructure.

Response: Concur. Since establishing elections as a critical infrastructure subsector in January 2017, CISA has focused on building partnerships with state, local, and private sector entities that run elections. This work included the creation of the Election Infrastructure Subsector Government Coordinating Council and Election Infrastructure Subsector Coordinating Council. In partnership with both councils, CISA is now working with all fifty states and more than fourteen hundred local jurisdictions to share information and manage risk. This work has included the creation of information sharing protocols (i.e., procedures) between federal, state and local officials regarding how threat information will be shared, how incidents will be responded to, and how all levels of government will communicate regarding the ongoing risks and threats to election infrastructure. Additionally, the Government Coordinating Council recommended long-term and short term areas of focus for the newly available Election Assistance Commission funding to the states, including items such as auditability, training, and updating of outdated or unsupported software.

In addition, CISA utilized its field personnel deployed across all fifty states to build relationships and awareness within the election community regarding the support and services CISA offers. These field personnel have attended state and local conferences, provided training, and performed assessments across the country. Moving forward CISA plans to utilize these personnel to continue to engage locally with state and local partners.

CISA also worked with the secretaries of state and state election directors on a targeted campaign for local election officials. This effort, known as "the last mile," created county-specific information, including posters, for local election officials to use to identify and mitigate risks to their election systems. It included a checklist of items for each local office to undertake to build a more resilient election process. DHS has delivered or is in the process of creating posters for 27 states.

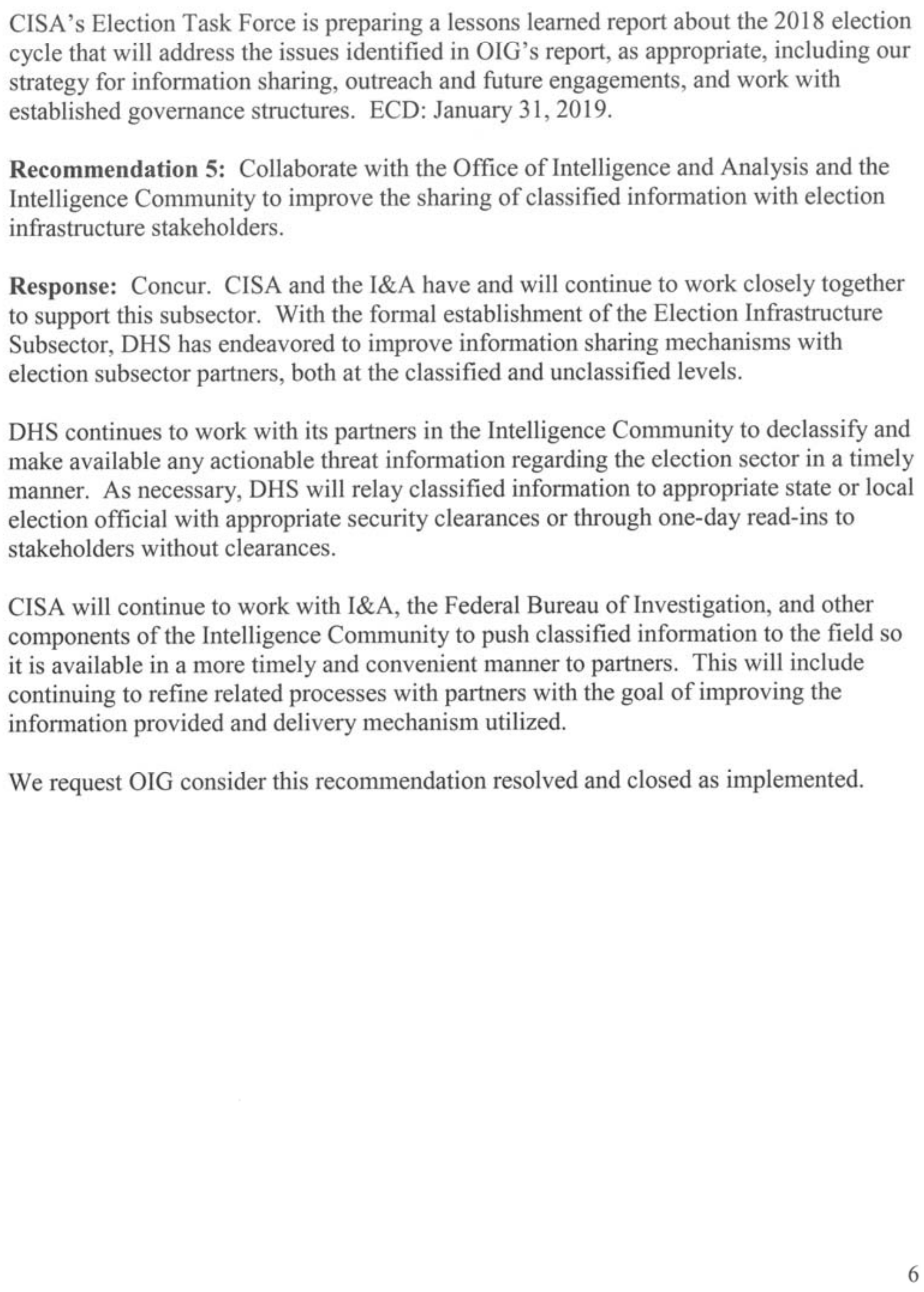
Moving forward, CISA will continue to build on the partnerships it has already created in order to broadly reach the thousands of elections jurisdictions nationwide. This will include another national-level table top exercise during the summer of 2019 followed by others in the months leading up to the 2020 elections; continued expansion of "the last mile" project and more tailored services for local election officials including the continued deployment of remote risk and vulnerability assessments. These tailored and scalable services not only benefit local-level partners in the elections infrastructure subsector, they serve as a foundation to expand outreach and services across all sectors.

CISA's Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address the issues identified in OIG's report, as appropriate, including our strategy for information sharing, outreach and future engagements, and work with established governance structures. ECD: January 31, 2019.

Recommendation 4: Enhance and expand the use of the Election Task Force, Election Infrastructure Information Sharing and Analysis Center (EI-IASC), and other governance structures to share and tailor information that would assist stakeholders in securing the election infrastructure.

Response: Concur. The development and maturation of the EI-ISAC is foundational to the continued work in the election subsector. During calendar year 2018 the EI-ISAC grew at an unprecedented pace. With more than 1,400 members, including all 50 states and private sector partners the EI-ISAC represents the fastest growing ISAC among all critical infrastructure sectors. Throughout 2018 the EI-ISAC regularly shared tailored information with the election community to help them manage risks to their systems. This included the deployment of more than one hundred Albert sensors in more than 40 states covering election systems that support approximately ninety percent of registered voters across the United States. CISA will continue to work with state and local officials to build EI-ISAC membership, deploy additional Albert sensors, and mature information sharing across the subsector.

The ETF mission statement is "To ensure the election stakeholder community has the necessary information to adequately assess risks and to protect, detect, and recover from those risks." In supporting this mission, CISA has moved forward on hiring actions to institutionalize the staff supporting election security in more permanent roles. Additionally, CISA continues to fund the information sharing and analysis function to support election officials. In applying dedicated resources to this mission, these workstreams, and the organizations implementing them, DHS is committed to enhancing and expanding support to stakeholders.



CISA's Election Task Force is preparing a lessons learned report about the 2018 election cycle that will address the issues identified in OIG's report, as appropriate, including our strategy for information sharing, outreach and future engagements, and work with established governance structures. ECD: January 31, 2019.

Recommendation 5: Collaborate with the Office of Intelligence and Analysis and the Intelligence Community to improve the sharing of classified information with election infrastructure stakeholders.

Response: Concur. CISA and the I&A have and will continue to work closely together to support this subsector. With the formal establishment of the Election Infrastructure Subsector, DHS has endeavored to improve information sharing mechanisms with election subsector partners, both at the classified and unclassified levels.

DHS continues to work with its partners in the Intelligence Community to declassify and make available any actionable threat information regarding the election sector in a timely manner. As necessary, DHS will relay classified information to appropriate state or local election official with appropriate security clearances or through one-day read-ins to stakeholders without clearances.

CISA will continue to work with I&A, the Federal Bureau of Investigation, and other components of the Intelligence Community to push classified information to the field so it is available in a more timely and convenient manner to partners. This will include continuing to refine related processes with partners with the goal of improving the information provided and delivery mechanism utilized.

We request OIG consider this recommendation resolved and closed as implemented.

Appendix C
Office of Information Technology Audits Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Brandon Barbee, Audit Manager
Yusuf Lane, Team Lead
Jasmine Raeford, IT Specialist
Michael Gigas, Program Analyst
Charles Twitty, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief 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