



U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-24-52

September 17, 2024

FINAL REPORT

DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced





OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

September 17, 2024

MEMORANDUM FOR: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Ken Wainstein
Under Secretary
Office of Intelligence and Analysis

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

**JOSEPH V
CUFFARI**

Digitally signed by
JOSEPH V CUFFARI
Date: 2024.09.17
18:12:12 -04'00'

SUBJECT: *DHS Improved Election Infrastructure Security, but Its Role in
Countering Disinformation Has Been Reduced*

Attached for your action is our final report, *DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving the security and resilience of the Nation's election infrastructure. Your office concurred with the recommendation.

Based on information provided in your response to the draft report, we consider recommendation 1 open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. 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 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 contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General, Office of Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced

September 17, 2024

Why We Did This Review

The U.S. elections process, which is a cornerstone of American democracy, relies on technology for efficiency and convenience. However, as with other critical infrastructure systems, this can introduce cybersecurity risks that could compromise the integrity of the election process. Prompted by suspicious cyber activities on election systems in 2016, on January 6, 2017, former DHS Secretary Jeh Johnson designated election infrastructure as a critical infrastructure subsector. We conducted this review to assess DHS' actions since 2020 to secure the election infrastructure and counter disinformation campaigns.

What We Recommend

We recommend that CISA develop and implement a risk-based national strategic plan to strengthen the security and resilience of the Nation's 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

Since 2020, the Department of Homeland Security has taken certain actions to address cyber and physical security threats to the election infrastructure but has adjusted its efforts to combat disinformation. The Cybersecurity and Infrastructure Security Agency (CISA) added a new Election Security Advisor position in each of its 10 regions to provide specialized assistance to election infrastructure stakeholders. CISA also continues to provide security resources to state and local partners to improve election infrastructure security, such as cyber and physical security assessments and tabletop exercises.

DHS continued to identify disinformation as a threat to the election infrastructure. However, according to CISA personnel, the component discontinued its efforts to work directly with social media companies to counter disinformation after the 2022 election. Instead, CISA is focused on resources that educate election partners and help to identify disinformation. CISA's reduced role in combating disinformation was due, in part, to DHS not completing plans to address disinformation threats.

Although the Office of Intelligence and Analysis is tasked with delivering intelligence to state, local, and private sector partners, its election intelligence products were not always actionable due to challenges with its review process.

It is important that DHS fulfill its mission to support state and local partners in addressing election security threats. Without effective efforts to combat disinformation, foreign nations could successfully influence elections, mislead voters, or cause Americans to lose trust in the security of elections. Further, if DHS does not provide actionable intelligence to stakeholders, the risks of an incident that adversely impacts the election infrastructure may increase.

CISA Response

CISA concurred with our recommendation. We consider this recommendation open and resolved.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

| | |
|---|----|
| Background | 1 |
| DHS' Responsibility for the U.S. Election Infrastructure | 1 |
| Evolving Challenges in Protecting Elections..... | 2 |
| Prior Office of Inspector General Reporting..... | 3 |
| Results of Review | 4 |
| CISA Provided Election Infrastructure Security Assistance to Its Partners | 5 |
| Changes to CISA's Efforts to Combat Disinformation | 8 |
| Some I&A Election Products Were Not Always Actionable..... | 13 |
| Conclusion..... | 14 |
| Recommendation | 14 |
| Management Comments and OIG Analysis..... | 14 |
| Appendix A: Objective, Scope, and Methodology..... | 16 |
| DHS OIG's Access to DHS Information..... | 17 |
| Appendix B: CISA's Comments on the Draft Report | 18 |
| Appendix C: Major Contributors to This Report Include..... | 22 |
| Appendix D: Report Distribution | 23 |

Abbreviations

| | |
|---------|---|
| CISA | Cybersecurity and Infrastructure Security Agency |
| CSA | Cybersecurity Advisor |
| EI-ISAC | Election Infrastructure Information Sharing and Analysis Center |
| ESA | Election Security Advisor |
| FBI | Federal Bureau of Investigation |
| I&A | Office of Intelligence and Analysis |
| IC | U.S. Intelligence Community |
| IT | information technology |
| PSA | Protective Security Advisor |



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Background

A secure election process is vital to our national interest and U.S. democracy. On January 6, 2017, former Department of Homeland Security Secretary Jeh Johnson designated election infrastructure as a subsector of the existing critical infrastructure for government facilities.¹ In his designation, Secretary Johnson recognized that election infrastructure is vital to our national interest.² Under DHS, the Cybersecurity and Infrastructure Security Agency (CISA) is currently the lead Federal agency for supporting critical infrastructure security and resilience as well as securing cyberspace.

The diversity and decentralization of voting systems and other electronic systems that support election administration provide resilience and security to U.S. elections but can also make it more challenging for election stakeholders to implement effective security controls nation-wide. Additionally, according to a 2023 Pew Research Center study on the transition of the news industry, “from print, television and radio into digital spaces,” more people rely on the internet for information.³ As reliance on internet news sources increases, people are more likely to be exposed to manipulation, disinformation,⁴ and propaganda⁵ campaigns that appear on the internet.⁶ According to several Federal agencies,⁷ adversaries could exploit these vulnerabilities to exacerbate existing social divides, amplify polarization, or push narratives that advance adversarial nation-state objectives.⁸

DHS’ Responsibility for the U.S. Election Infrastructure

Within DHS, CISA coordinates efforts to manage risks to the Nation’s 16 critical infrastructure sectors, one of which includes the election infrastructure subsector. The election infrastructure subsector includes, but is not limited to:

¹ Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, designated DHS and the General Services Administration as co-Sector-Specific Agencies responsible for the Government Facilities Sector. The recently released *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22, replaced Presidential Policy Directive 21 but affirmed DHS’ continued role as a co-Sector Risk Management Agency responsible for the Government Facilities Sector.

² Statement by Secretary Jeh Johnson on the *Designation of Election Infrastructure as a Critical Infrastructure Subsector*, January 6, 2017.

³ <https://www.pewresearch.org/journalism/fact-sheet/news-platform-fact-sheet/>.

⁴ According to the *Homeland Threat Assessment* for 2024, disinformation is false or misleading information that is deliberately created or spread with the intent to deceive or mislead.

⁵ According to the Intelligence Community (IC), propaganda is true, partially true, or false information intended to advance the actor’s interests by influencing the attitudes, perceptions, or behaviors of an audience. Propaganda could be intended to influence a domestic or a foreign audience.

⁶ https://www.cisa.gov/sites/default/files/publications/together-stop-disinformation_508.pdf.

⁷ CISA, the Office of the Director of National Intelligence, and the Federal Bureau of Investigation (FBI).

⁸ <https://www.cisa.gov/resources-tools/resources/securing-election-infrastructure-against-tactics-foreign-malign-influence-operations>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- voter registration databases and associated information technology (IT) systems;
- IT infrastructure and systems 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.⁹

The DHS Office of Intelligence and Analysis (I&A), as part of the U.S. Intelligence Community (IC), is charged with delivering intelligence to state, local, tribal, territorial, and private sector partners, and with developing intelligence from those partners for the Department and the IC.¹⁰ I&A delivers election-related intelligence products to CISA and state and local partners by providing raw and finished intelligence products.

Evolving Challenges in Protecting Elections

Election infrastructure's reliance on technology for efficiency and convenience may introduce cybersecurity risks. For example, in April 2023 a news outlet reported that in 2020, the U.S. Government discovered and disrupted Iranian hackers' attempt to exploit access to a U.S. municipal government's unofficial election results reporting system.¹¹

Additionally, before the 2020 elections, DHS identified disinformation¹² and foreign influence¹³ as evolving challenges in protecting elections. Influence operations refer to hostile efforts by or on behalf of foreign governments to shape U.S. policies, decisions, and discourse. These operations may occur overtly or covertly, taking many forms and using a

⁹ <https://www.cisa.gov/topics/election-security>.

¹⁰ *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting*, OIG-22-50, July 6, 2022, and *IA-1000 Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, Revision 00, January 19, 2017.

¹¹ *US cyberwarriors thwarted 2020 Iran election hacking attempt*, The Associated Press, April 25, 2023.

¹² According to the *DHS Strategic Framework for Countering Terrorism and Targeted Violence*, September 20, 2019, disinformation campaigns aim to shape public opinion or undermine trust, which may lead to strife and division.

¹³ According to the DHS *Homeland Threat Assessment*, October 2020, foreign influence is any covert, fraudulent, deceptive, or unlawful activity of foreign governments — or persons acting on their behalf — undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting U.S. democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives. This includes foreign governments' deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

variety of tactics and techniques to accomplish their goals. Such campaigns aim to erode public trust in our elections and may undermine our democratic processes.¹⁴

Concerns around election interference were further reported in November 2023 when a global technology company stated, “Election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome.”¹⁵ In early February 2024, American news media reported possibly the first known attempt at using artificial intelligence to interfere with a U.S. election by mimicking a Presidential candidate’s voice.¹⁶ The Director of the Federal Bureau of Investigation (FBI) warned that the United States expects to face fast-moving threats to elections this year as artificial intelligence and other technological advances have made interference and meddling easier.¹⁷

In a May 2024 interview, current DHS Secretary Alejandro Mayorkas stated our Nation faces three specific election threats — cybersecurity, physical security (including physical threats to local election officials and poll workers), and disinformation (including the intentional spread of false information to confuse or deceive voters).¹⁸ The Secretary stated the Department was preparing for an “unprecedented array of election threats” and maintained that “the right to vote and the integrity of the right to vote is a fundamental element of our democracy.” The last three Congresses held hearings on election security and foreign influence, including a May 2024 House Committee hearing.¹⁹

Prior Office of Inspector General Reporting

This review continues our oversight of the Department’s efforts to secure election infrastructure and counter disinformation campaigns. In February 2019, we reported that DHS had taken steps

¹⁴ https://www.cisa.gov/sites/default/files/publications/together-stop-disinformation_508.pdf

¹⁵ *Protecting Election 2024 from foreign malign influence: lessons learned help us anticipate the future*, Microsoft Threat Analysis Center Report, November 8, 2023.

¹⁶ *Authorities target two Texas firms in probe of AI-generated robocalls before New Hampshire’s primary*, The Associated Press, February 7, 2024.

¹⁷ *The US is bracing for complex, fast-moving threats to elections this year. FBI director warns*, The Associated Press, February 29, 2024.

¹⁸ *Homeland Security ramping up ‘with intensity’ to respond election threats*, USA TODAY, May 8, 2024.

¹⁹ *American Confidence in Elections: Preventing Noncitizen Voting and Other Foreign Interference: Hearings before the House Committee on Administration*, 118th Congress (2024). In addition, the topic was reviewed by the 117th and 116th Congress: *Securing Democracy: Protecting Against Threats to Election Infrastructure and Voter Confidence: Hearings before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation*, 117th Congress (2022); *Safe, Secure, and Auditable: Protecting the Integrity of the 2020 Elections: Hearings before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation*, 116th Congress (2020).



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

to mitigate risks to the Nation’s election infrastructure.²⁰ We further reported in October 2020,²¹ that DHS had improved coordination efforts to secure the Nation’s systems used for voting but should take additional steps to protect the broader election infrastructure. In August 2022, we reported that some DHS components had taken actions to counter disinformation campaigns that pertained either to the election infrastructure or distinct mission areas.²²

We conducted this review to assess DHS’ actions since 2020 to secure election infrastructure and counter disinformation campaigns.

Results of Review

Since 2020, DHS has taken certain actions to address cyber and physical security threats to election infrastructure but has adjusted its efforts to combat disinformation.

CISA added a new Election Security Advisor (ESA) position in each of its 10 regions to provide specialized assistance to election infrastructure stakeholders. CISA also continues to provide security resources to state and local partners to improve election infrastructure security, such as cyber and physical security assessments and tabletop exercises.

DHS continued to assess that disinformation involving the time and location of polling operations poses a threat to the secure and efficient conduct of the election infrastructure. However, CISA personnel stated the component discontinued its efforts to work directly with social media companies to counter disinformation after the 2022 election. Instead CISA is focused on resources that educate election partners and help to identify disinformation. CISA’s reduced role in combating disinformation was due, in part, to DHS not completing plans to address disinformation threats.

Although I&A is tasked with delivering intelligence to state, local, and private sector partners, its election intelligence products were not always actionable due to challenges with its review process.

It is important that DHS fulfill its mission to support state and local partners in addressing election security threats. Without effective efforts to combat disinformation, foreign nations

²⁰ [Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure](#), OIG-19-24, February 28, 2019. As of April 2020, all five recommendations cited in OIG-19-24 are closed.

²¹ [DHS Has Secured the Nation’s Election Systems, but Work Remains to Protect the Infrastructure](#), OIG-21-01, October 22, 2020. As of July 2024, our recommendation that the Department update its National Infrastructure Protection Plan remains open and resolved. As issued, our recommendation states the Director of CISA should “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.”

²² [DHS Needs a Unified Strategy to Counter Disinformation Campaigns](#), OIG-22-58, August 10, 2022.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

could successfully influence elections, mislead voters, or cause Americans to lose trust in the security of elections. Further, if DHS does not provide actionable intelligence to stakeholders, the risks of an incident that adversely impacts the election infrastructure may increase.

CISA Provided Election Infrastructure Security Assistance to Its Partners

CISA provides no-cost, voluntary assistance to state and local partners for cyber and physical security across critical infrastructure sectors. As of June 2024, according to CISA documentation, it had developed 401 unique products for 2,340 election administrators in 17 states for the 2024 election cycle. For each region, CISA has Cybersecurity Advisors (CSAs) and Protective Security Advisors (PSAs) who work with state, local, tribal, territorial, and private sector critical infrastructure stakeholders across its mission areas, including election infrastructure security. CSAs are infrastructure cybersecurity subject matter experts who offer cyber assessments and assistance. PSAs are physical security subject matter experts who provide assessments and vulnerability mitigation recommendations. Both PSAs and CSAs facilitate delivery of CISA services and capabilities to infrastructure stakeholders in the field and can also provide coordination or support in times of threat or direct attacks.

In 2023, CISA added ESAs to serve as subject matter experts and liaisons to state and local partners and to lead regional election security engagement strategies. As of early 2024, according to CISA personnel, CISA had onboarded ESAs for all 10 regions. During our interviews, the state and local partners that already had ESAs within their region were optimistic about the new role.

We spoke with Election officials from 13 states to obtain feedback on CISA's services and support. Election officials from 12 of 13 states reported they were satisfied with CISA's efforts to secure the election infrastructure, but one did not offer an opinion. Five of the 13 states specifically noted the good quality or value added of CISA's products and services. Four of the 13 states said CISA's services supplemented or expanded the security resources the state could provide on its own. CISA personnel stated their proactive relationship-building and networking efforts enhanced collaboration and awareness with state and local partners.

We also discussed CISA's work to secure the election infrastructure with representatives of other Federal agencies. For example, one FBI representative stated that they worked closely with CISA and referred to CISA as a collaborative partner. The FBI representative also considers the relationship between the FBI and CISA, in terms of election matters, as a "best practice" example of the collaboration that is possible between the two agencies. In addition, a representative from the Office of the Director of National Intelligence said since February 2024, their coordination with CISA had improved substantially.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Cybersecurity

The cybersecurity and information activities impacting the election infrastructure remain a concern for some state and local partners. DHS provides funding for the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)²³ to provide cybersecurity services, such as monitoring network intrusion detection capabilities (i.e., sensors) installed on election networks used by state and local partners. Additionally, according to CISA officials, between May 2020 and February 2024, CISA increased the number of its regional CSA positions from 26 to more than 150 positions. At the time of this review, 135 of these positions were filled, allowing the component to provide more cybersecurity services. For example, CSAs provide cyber hygiene assessments, resilience reviews, and cybersecurity workshops. According to CISA documentation, between January 2020 and December 2023 CISA conducted:

- 588 Cyber Hygiene Vulnerability Scans;
- 203 Cyber Hygiene Web Application Scans;
- 130 Risk and Vulnerability Assessments;²⁴
- 249 Remote Penetration Tests;²⁵
- 8 Validated Architecture Design Reviews;²⁶ and
- 20 Phishing Campaign Assessments.

Physical Security

CISA also helps state and local partners improve physical security for the election infrastructure. State and local partners we interviewed noted concerns around the election infrastructure's physical security. For example, 5 of the 13 states we spoke to specifically mentioned concerns for election worker safety. To help alleviate partner concerns regarding physical safety and security, CISA conducts physical security assessments, such as the Security Assessment at First

²³ The EI-ISAC sits within the Center for Internet Security, which is the current recipient of a Cooperative Agreement funded by CISA. The EI-ISAC is a collective group of 3,759 members, as of February 2024, and is voluntary to join. The EI-ISAC offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products.

²⁴ Risk and vulnerability assessments are one-on-one engagements with stakeholders. These assessments combine open-source national threat and vulnerability information with data that the CISA team collects through remote and onsite stakeholder assessment activities.

²⁵ Remote penetration testing is technical testing to identify remote vulnerabilities in a network or web application, phishing susceptibility, and design issues.

²⁶ The Validated Architecture Design Review is an assessment based on Federal and industry standards, guidelines, and best practices. Assessments can be conducted on IT or Operational Technology infrastructures.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Entry²⁷ and the Infrastructure Survey Tool,²⁸ which provide voluntary options for consideration to improve the security of an election infrastructure facility.

According to CISA personnel, many state and local partners continued to request and use assessments, services, and trainings to support their security efforts during the 2024 election cycle.²⁹ For example, multiple states received training from CISA personnel on active shooters or situational awareness. One state official said the physical security assessment information helps prioritize funding and solicit additional funds. Even though CISA had almost 140 PSAs in the field in 2024, the demand for services occasionally outpaced staff capacity. In one region, the high demand caused delays delivering CISA's assessments and other services. We previously reported similar issues related to CISA being unable to perform timely assessments.³⁰

Tabletop Exercises

CISA conducted tabletop exercises to address cyber, physical, and operational security risks as well as those posed by foreign malign influence operations and disinformation. We reviewed feedback from state and local partners for 18 tabletop exercises.³¹ Sixteen of the 18 states participating in the exercises we reviewed gave a positive score (80 percent or higher). According to the feedback we reviewed, tabletop exercises help state and local partners identify best practices and areas for improvement in incident planning, identification, and response to cybersecurity and physical security threats that could potentially impact election infrastructure.

The tabletop exercises also provided an opportunity to discuss whether state and local election officials were prepared to identify, respond to, and manage cyber and physical security incidents, and whether processes are in place to mitigate the impacts of disinformation on state and local election infrastructure. As part of these tabletop exercises, CISA assisted in the development of state and local-level processes and plans to address elections-related cyber and physical security incidents. State and local partners participating in tabletop exercises said the exercises helped:

²⁷ The Security Assessment at First Entry is designed to assess the current security posture and identify options for facility owners and operators to mitigate future threats.

²⁸ The Infrastructure Survey Tool is a voluntary, web-based assessment that PSAs conduct in coordination with facility owners and operators to identify and document the overall security and resilience of the facility.

²⁹ During our fieldwork, CISA could not provide the specific number of election-related services or assessments conducted by PSAs.

³⁰ [Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure](#), OIG-19-24, February 28, 2019, and [DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure](#), OIG-21-01, October 22, 2020.

³¹ Although CISA provided the review team 44 tabletop exercises with accompanying "After Action" or "Summary" reports, many of those tabletop exercises occurred prior to the 2020 election. Some reports were for tabletop exercises conducted for private companies, not for state and local partners. The team judgmentally reviewed 18 of the reports for tabletop exercises conducted for state and local partners that occurred within the scope of our review.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- enhance preparedness and problem solving;
- share best practices;
- provide networking opportunities; and
- identify vulnerabilities and weaknesses.

Changes to CISA's Efforts to Combat Disinformation

DHS continued to emphasize the threat posed by disinformation in its *2024 Homeland Threat Assessment*.³² The document notes that our electoral processes remain an attractive target for many adversaries, who may attempt to influence or interfere with the 2024 election and may use artificial intelligence technologies to improve the quality and breadth of their influence operations targeting U.S. audiences.

We interviewed state and local election officials from 13 states to identify the biggest threats to the 2024 elections. The officials consistently identified disinformation³³ as the most pressing threat. Seven of the states we met with listed disinformation as a threat to the 2024 election cycle. Four states noted cyber threats, and three states voiced concerns with artificial intelligence. Only two states listed physical violence as their biggest threat(s). Other threats listed by states included, but were not limited to, public perception, election staff morale, and insider threats.

We have conducted prior reviews to assess DHS' actions to counter disinformation campaigns. We reported in August 2022 that, as part of its effort to counter disinformation, CISA notified social media platforms of disinformation identified by election officials, and the social media platforms could independently decide whether to remove or modify the post.³⁴ During this review, CISA program officials stated they stopped communicating directly with social media companies following the November 2022 elections. Two social media companies and a state and local partner we spoke with confirmed they no longer work with CISA on disinformation. According to a senior CISA official, CISA changed its efforts to counter disinformation based on the evolution of the disinformation mission during that time.

³² [Homeland Threat Assessment](#), 2024.

³³ Some of the state and local officials we met with identified multiple threats.

³⁴ [DHS Needs a Unified Strategy to Counter Disinformation Campaigns](#), August 10, 2022, OIG-22-58. Former DHS Secretary Kirstjen Nielsen established the Countering Foreign Influence Task Force to focus on election infrastructure disinformation in 2018. The Task Force comprised CISA's Election Security Initiative division and I&A staff. From 2018 to 2021, the Task Force developed threat intelligence and engaged with stakeholders related to elections. According to CISA's website and an internal document, in 2018, CISA also started notifying social media platforms or appropriate law enforcement officials when voting-related disinformation appeared in social media.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

CISA did not specify why it stopped communicating with social media companies. However, in May 2022, the Attorneys General of Missouri and Louisiana, and several private plaintiffs, alleged in a lawsuit filed in the U.S. District Court for the Western District of Louisiana (“District Court”) that Federal Government officials violated the First Amendment by coercing or threatening social media companies to censor disfavored speakers or viewpoints from their platforms.³⁵ On July 4, 2023, the District Court issued a preliminary injunction that enjoined and restrained certain Federal Government entities and officials, including CISA, from taking the following actions related to social media companies:

- meeting with social media companies for the purpose of urging, encouraging, pressuring, or inducing in any manner the removal, deletion, suppression, or reduction of content containing protected free speech posted on social media platforms;
- specifically flagging content or posts on social media platforms and/or forwarding such to social media companies urging, encouraging, pressuring, or inducing in any manner for removal, deletion, suppression, or reduction of content containing protected free speech;
- emailing, calling, sending letters, texting, or engaging in any communication of any kind with social media companies urging, encouraging, pressuring, or inducing in any manner for removal, deletion, suppression, or reduction of content containing protected free speech; or
- collaborating, coordinating, partnering, and/or jointly working with any project or group for the purpose of urging, encouraging, pressuring, or inducing in any manner removal, deletion, suppression, or reduction of content posted with social media companies containing protected free speech.³⁶

On appeal, the Fifth Circuit Court of Appeals upheld parts of the District Court’s decision, including the finding that the plaintiffs were likely to succeed on the merits of their claim that certain defendants, including CISA, violated the First Amendment, but modified the scope and language of the preliminary injunction.³⁷ On June 26, 2024, the United States Supreme Court issued a decision reversing the Fifth Circuit and remanding the case for further proceedings consistent with the Court’s opinion.³⁸

CISA Used Varied Methods to Help Its Partners Counter Disinformation

CISA’s current role in countering disinformation is focused on educating election stakeholders on misinformation, disinformation, and malign influence tactics and how to mitigate them. This includes providing guidance, informational materials, and related services to help state and local

³⁵ Plaintiff’s Complaint, Case 3:22-cv-01213, filed May 5, 2022, at 75-76.

³⁶ Order Grant in Part and Den. in Part Pl.’s Mot. Prelim. Inj., Case No. 3 :22-cv-01213 (W.D. La. July 4, 2023).

³⁷ *Missouri v. Biden*, 83 F.4th 350 (5th Cir. 2023).

³⁸ *Murthy v. Missouri*, 144 S. Ct. 1972 (2024). This ruling was announced after our fieldwork. As such, we were unable to determine any impact on CISA’s role countering disinformation.

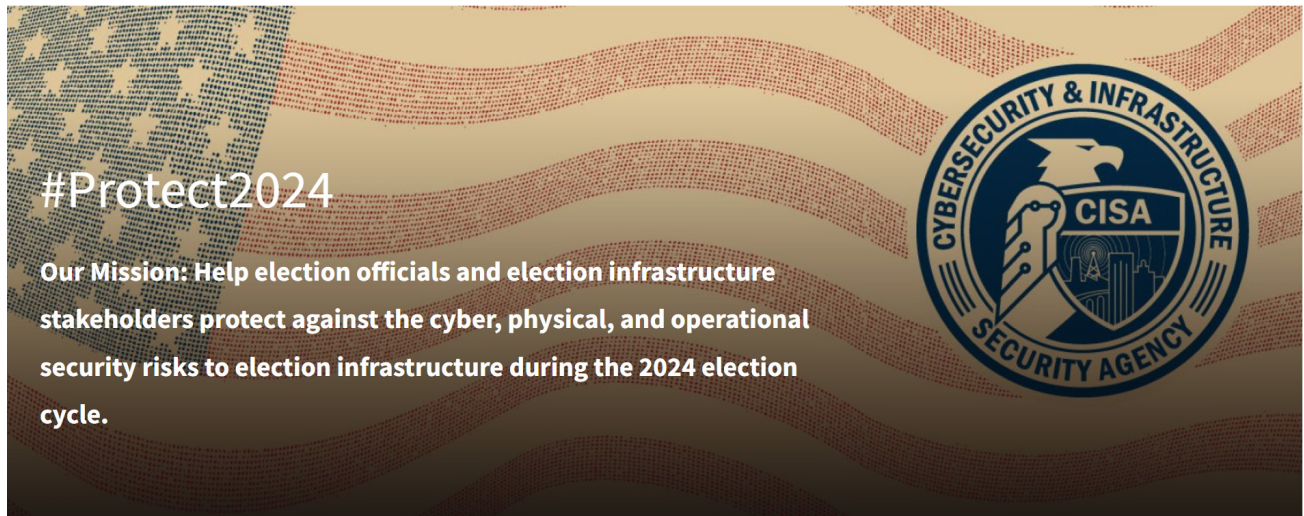


OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

partners and offers an in-person or virtual training on foreign malign influence operations and generative artificial intelligence. For example, CISA established the #Protect2024 initiative to help secure the 2024 elections. The initiative is captured in a website³⁹ that outlines steps to enhance election security, such as encouraging the use of multifactor authentication, promoting CISA’s physical security assessment service, or joining the EI-ISAC.

Figure 1. CISA’s #Protect2024 Website



Source: Captured from <https://www.cisa.gov/topics/election-security/protect2024>⁴⁰

Through our review of the #Protect2024 initiative, Rumor vs. Reality website, and *CISA Strategic Plan 2023-2025*⁴¹ we found CISA’s work related to countering disinformation is now focused on building public awareness. According to a program official, CISA’s goal for the Rumor vs. Reality website, “is to help communicate election security practices and enhance civic literacy to build resilience against foreign interference and disinformation” and mitigate the risks of disinformation narratives that directly target election infrastructure.⁴² CISA also works with Federal partners to release alerts highlighting disinformation tactics used by foreign nations seeking to disrupt critical infrastructure. Other resources within the U.S. Government now help address this challenge. For example, the Office of Director of National Intelligence Foreign Malign Influence Center began operating in September 2022 and serves as the primary U.S. Government organization for integrating intelligence pertaining to foreign malign influence. The Foreign Malign Influence Center also works on U.S. Government efforts to share threat

³⁹ <https://www.cisa.gov/topics/election-security/protect2024>.

⁴⁰ Screenshot obtained May 21, 2024, by the DHS OIG review team.

⁴¹ *CISA Strategic Plan 2023-2025, September 2022*.

⁴² The webpage can be found at [Election Security Rumor vs. Reality](#). From October 2020 to April 2024, CISA posted 27 entries.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

intelligence and information with government, civil society, and private sector partners, including technology companies.

In addition to delivering information via the internet, CISA also provides trainings and guidance to election stakeholders. For example, CISA planned a series of election security webinars on a variety of topics including disinformation. The disinformation webinar included recent examples of various tactics and how to counter them. CISA also provides stakeholders with templates to build out communication plans for elections and lists of resources where stakeholders can obtain additional information. CISA also collaborated with the Office of the Director of National Intelligence and the FBI to publish an eight-page guide to “Securing the Election Infrastructure Against the Tactics of Foreign Malign Influence,” which was released in April 2024.⁴³

CISA measured the effectiveness of its current disinformation strategy by the number of visitors to its sites and the number of partnerships established to counter disinformation. According to a CISA official, its *Election Security Rumor vs. Reality* webpage received more than 9 million visits between October 2020 and April 2024. Also, the Government Coordinating Council and Subsector Coordinating Council worked together to develop the *Rumor Control Page Startup Guide*⁴⁴ to help states start websites similar to the *Election Security Rumor vs. Reality* site. At the time of our review, 47 states had established their own websites focused on combating election-based disinformation.

We could not measure the extent to which CISA’s current efforts are effective in countering disinformation. We previously reported that members of the IC questioned whether CISA’s efforts to educate the public on disinformation efforts were effective.⁴⁵ For example, an IC official voiced concerns about whether CISA’s myth-busting website was doing enough to effectively counter disinformation.⁴⁶

State and local partners we interviewed identified CISA’s briefings, tabletop exercises, flyers/handouts, personalized products, and the CISA website as methods used to counter disinformation efforts. Additionally, 12 of 13 state and local partners we interviewed had developed ways to counter disinformation on their own. Some partners used more than one way to counter disinformation. For example, state and local partners counter disinformation by reaching out to social media directly (11 of 13); working with third-party organizations such as the EI-ISAC, Multi-State Information Sharing and Analysis Center, and National Association of Secretaries of State (6 of 13); and using mainstream media (3 of 13).

⁴³ <https://www.cisa.gov/resources-tools/resources/securing-election-infrastructure-against-tactics-foreign-malign-influence-operations>.

⁴⁴ *Rumor Control Page Startup Guide*.

⁴⁵ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, OIG-22-58, August 10, 2022.

⁴⁶ Ibid.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

DHS Has Not Completed Plans for Addressing Disinformation Threats

While the Supreme Court decision on the Federal Government’s ability to counter disinformation was pending at the time of our review, we also attribute CISA’s diminished effort in countering election-related disinformation to a lack of strategic guidance from the Department for defining DHS’ roles to address this evolving threat. Although DHS continued to identify disinformation as a threat to Federal elections in several key documents, it has taken limited steps that could further help secure election infrastructure. More than 3 years ago, we recommended the Director of CISA, “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.”⁴⁷ DHS still has not updated critical plans to include the specific goals, objectives, milestones, and priorities needed to monitor and secure the election infrastructure and address other emerging threats, such as disinformation.

We identified the same issue in both our 2019⁴⁸ and 2020⁴⁹ reports, stating these updates are necessary to align and prioritize CISA’s efforts and establish metrics for measuring progress for securing election infrastructure. Further, we reported the *Election Infrastructure Subsector-Specific Plan, 2020*,⁵⁰ only briefly mentioned the need to prepare for disaster recovery and foreign influence threats for the election infrastructure subsector. According to the plan, CISA’s primary focus is to promote its cybersecurity services, risk management efforts, and audits. CISA officials said the guidance they use in their efforts to counter disinformation stems from the component’s role as the Sector Risk Management Agency for the election infrastructure subsector.⁵¹ CISA program officials did not provide any additional DHS policies, directives, or mandates to support this mission area. Updating these plans will strengthen and unify the

⁴⁷ [DHS Has Secured the Nation’s Election Systems, but Work Remains to Protect the Infrastructure](#), OIG-21-01, October 22, 2020. As of June 2024, our recommendation to the Department to update the National Infrastructure Protection Plan and other planning documents remains open and resolved.

⁴⁸ [Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure](#), OIG-19-24, February 28, 2019.

⁴⁹ [DHS Has Secured the Nation’s Election Systems, but Work Remains to Protect the Infrastructure](#), OIG-21-01, October 22, 2020.

⁵⁰ Before the 2022 election, the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council’s Joint Subsector-Specific Plan Working Group created the [Election Infrastructure Subsector-Specific Plan: 2022 Status Update](#), which identified CISA’s effort to counter disinformation through its [rumor control website](#). As of May 2024, the working group has not updated the *Election Infrastructure Subsector-Specific Plan, 2020*, to counter disinformation during the 2024 election.

⁵¹ Under Title 6 of the United States Code § 665d(c)(4), the Sector Risk Management Agency is responsible for “facilitating access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through Information Sharing and Analysis Organizations,” and maintaining “real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector.”



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Department's activities to address emerging disinformation-related threats against the subsector.

Some I&A Election Products Were Not Always Actionable

I&A is responsible for delivering intelligence to state, local and private sector partners, as well as developing intelligence from those partners for the Department and the IC. As part of the U.S. Government's approach to informing partners of threats to election security, agencies have jointly coordinated the release of unclassified, public-facing alerts and notifications through the Office of the Director of National Intelligence's new Foreign Malign Influence Center. I&A also works jointly with IC partners to produce joint-seal classified products on election security topics to inform Federal and cleared intergovernmental public-facing security agencies in their efforts to counter disinformation.

IC Directive 203 outlines five analytic standards, which demand that analysis be objective, independent of political consideration, timely, based on all available sources, and "implement and exhibit" nine analytic tradecraft standards.⁵² One of those analytic tradecraft standards states that products should demonstrate customer relevance and address implications. As such, analytic products should provide information and insight on issues relevant to IC customers and address the implications of the offered information and analyses. Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.

I&A's election intelligence products are disseminated to state and local partners. Some election stakeholders/recipients we interviewed noted I&A's information was not always useful. Some stakeholders stated intelligence products do not demonstrate customer relevance or opportunities for action. One customer cited a lack of the "so what," or context, stating the products they received merely contained information instead of actionable intelligence. An internal I&A memo also stated some customers found I&A products were of little value, difficult to understand, and not useful or actionable. Two of the 13 states we met with voiced concerns about intelligence products. Another stakeholder noted intelligence products they received were not always timely.

Challenges within I&A's Policies and Processes

Before providing intelligence products to state and local partners, I&A subjects these products to extensive internal reviews. Similar to the rest of the IC, finished intelligence products are reviewed by at least two separate qualified product reviewers at increasing levels of seniority. I&A products are also reviewed by four separate oversight offices to ensure compliance with legal, privacy, and civil rights and civil liberties equities. I&A disseminates the final products to

⁵² [IC Directive 203](#).



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

authorized communities of interest. The creation and distribution of intelligence products are subject to IC and Department standards and policies, including that the products be provided in a timely manner.

Although I&A had a review policy and process, it did not always capture all changes and could not track all reviewer comments. I&A identified inconsistencies in its own review process as it did not provide assurance for identifying compliance issues to improve deficiencies. According to I&A personnel, the review process is largely dependent on the quality of individual reviews. I&A previously identified gaps in its oversight process, training, and overarching policy framework for its intelligence products and functions and has worked to update some of its standard operating procedures. We previously reported similar issues related to other I&A products and their associated processes.⁵³ I&A recently revised its internal review guidance in June 2023 and standard operating procedures on finished intelligence production in September 2023. We are not making a recommendation on this topic, but we plan to conduct future work to determine if I&A's updated policies have improved its products, including those related to election infrastructure security.

Conclusion

DHS continues to improve election infrastructure security by providing cyber and physical security services and intelligence information to state and local partners. While DHS has identified disinformation as a threat to election security, it is unclear if CISA's current efforts to counter disinformation are effective. Without effective efforts to combat disinformation, foreign nations could successfully influence elections, mislead voters, or cause Americans to lose trust in the security of elections. DHS must take all necessary actions to support state and local partners to address election security threats.

Recommendation

Recommendation 1: We recommend the Director of CISA develop and implement a risk-based national strategic plan that addresses current and evolving risks, to enhance the security and resilience of the Nation's election infrastructure, including disinformation and the use of artificial intelligence.

Management Comments and OIG Analysis

CISA provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments from DHS on the draft report,

⁵³ [DHS Actions Related to an I&A Intelligence Product Deviated from Standard Procedures](#) (Redacted), OIG-22-41, April 26, 2022, and [The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting](#), OIG-22-50, July 6, 2022.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

and we revised the report as appropriate. CISA concurred with our recommendation, which we consider open and resolved. A summary of CISA's response and our analysis follows.

CISA Response to Recommendation 1: Concur. CISA is developing both a risk assessment and risk management plan for the election infrastructure. This effort is consistent with, though not bound by, NSM-22, *National Security Memorandum on Critical Infrastructure and Resilience*,⁵⁴ published by the White House National Security Council on April 30, 2024, which updates the national-level guidance related to protecting critical infrastructure. Although NSM-22 does not specify guidance for subsectors, CISA agrees that developing a subsector risk assessment and subsector risk management plan is crucial to support the significant and ongoing efforts to address election infrastructure risks. CISA plans to work with the subsector to develop and review the subsector risk assessment in 2025, with subsequent updates planned to ensure maximum participation from election officials. The new risk assessment and risk management plan will serve as the foundation for future updates to election infrastructure subsector planning documents. Estimated Completion Date: June 30, 2025.

OIG Analysis: We consider CISA's actions responsive to the recommendation, which is open and resolved. The recommendation will remain open until CISA develops and implements a risk-based national strategic plan to enhance the security and resilience of U.S. election infrastructure.

⁵⁴ <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix A: Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency.

Our review objective was to assess DHS’ actions since 2020 to secure election infrastructure and counter disinformation campaigns. Specifically, we assessed DHS’s actions from November 2020 to June 2024. Our review focused on the requirements, recommendations, and goals outlined in key documents, such as:

- *Critical Infrastructure Security and Resilience*, National Security Memorandum 22, April 30, 2024;
- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 2013; and
- *Homeland Threat Assessments of 2020 and 2024*.

To conduct our review, we interviewed 10 CSAs, 10 PSAs, 10 Regional Directors, and additional CISA and I&A staff. Additionally, we met with state and local partners in 13 states covering 9 of the 10 CISA regions. We selected states based on the timing of primary elections. We do not identify these states or the officials with whom we met to protect their anonymity. This approach is consistent with our prior election infrastructure security work.

We also met with representatives from selected agencies and organizations that work with CISA on election security, such as the:

- Department of Justice’s FBI;
- EI-ISAC;
- Office of the Director of National Intelligence;
- Joint Cyber Defense Collaborative;
- National Association of State Election Directors; and
- National Association of Secretaries of States.

The team reviewed and analyzed legal documents and filings, court rulings, congressional testimony, and state election funding documents along with other products and documentation provided by CISA headquarters and regional personnel, as well as state and local election officials we interviewed.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

To answer our objective, 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 since 2020. We also contacted eight different social media companies for their feedback on flagging and removing disinformation. Of the three companies that responded, one agreed to meet with us, another agreed to provide a written response, and the third declined a meeting.

As part of our review, we assessed the internal and external coordination efforts the Department has taken to counter disinformation in social media. Because we did not obtain any computer-processed data related to disinformation, we did not conduct any data reliability tests.

We conducted this review from October 2023 through June 2024 under the authority of the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG’s Access to DHS Information

During this review, CISA and I&A provided timely responses to our requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix B: CISA's Comments on the Draft Report

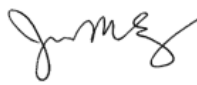


U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

BY ELECTRONIC SUBMISSION

September 6, 2024

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

FROM: Jen Easterly 
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "DHS Improved
Election Infrastructure Security but Its Role in
Countering Disinformation Has Been Reduced"
(Project No. 23-068-AUD-CISA, I&A)

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 remains committed to enhancing the security and resilience of America's election infrastructure and assisting election infrastructure stakeholders such as election vendors and the state and local election officials that administer, manage, and secure election processes. CISA leadership is pleased that OIG recognized that the Department of Homeland Security, to include CISA, took several actions to address the cybersecurity and physical security threats to election infrastructure. Since the beginning of 2023, for example, CISA has supported election infrastructure stakeholders by conducting approximately 700 cybersecurity assessments, 1,000 physical security assessments, more than 120 tabletop exercises, and over 380 trainings, reaching more than 21,000 participants.

CISA also remains committed to assisting election infrastructure stakeholders, including state and local partners, defend election infrastructure against the risk of foreign malign influence operations and disinformation, and it is important that the OIG's report reflect the full scope of CISA's work related to countering foreign influence operations and disinformation. The Office of the Director of National Intelligence's (ODNI) 2024 Annual Threat Assessment¹ highlighted this threat, assessing that how China, Russia, and

¹ "ODNI 2024 Annual Threat Assessment," dated February 5, 2024;
<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Iran are leveraging malign influence operations to target the U.S. elections process, with the aim of exploiting perceived sociopolitical divisions to undermine confidence in U.S. democratic institutions. CISA is part of a larger U.S. government-wide effort to counter foreign malign influence operations, through the work of entities such as the Foreign Malign Influence Center, which was established by the ODNI in September 2022 to serve as the coordinator of the U.S. government efforts to share threat intelligence and information with civil society and private sector partners. CISA works to mitigate the threat posed by foreign malign influence operations and disinformation in three distinct ways, complementing our federal partners' efforts in the mission space:

1. Developing publicly available security guidance for election officials, as needed, that addresses tactics and techniques employed in foreign adversary influence operations, so election infrastructure stakeholders are better postured to identify and respond to these incidents. This guidance includes products such as the "Securing Election Infrastructure against the Tactics of Foreign Influence Operations" guide,² and this work is augmented by in-person and virtual trainings.
2. Providing context to common narratives and themes that relate to the security of election infrastructure and related processes, via CISA's "Election Security Rumor vs. Reality website,"³ to complement election officials' voter education and civic literacy efforts by addressing common disinformation narratives through accurate information related to election security and similar processes.
3. Amplifying accurate election security-related information shared by state and local officials, who understand their processes and systems best. This is achieved through efforts such as talking points in public engagements that emphasize the role of state and local election officials as the trusted sources of information related to the elections process and security. CISA also highlights efforts like the #TrustedInfo2024 initiative launched by the National Association for Secretaries of State, which is a public education effort to promote election officials as the trusted sources of election information during the 2024 election cycle and beyond.⁴

The draft report contained one recommendation with which CISA concurs. Attached, please find our detailed response to the recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration, as appropriate.

² "Securing Election Infrastructure against the Tactics of Foreign Influence Operations," dated in April 2024; <https://www.cisa.gov/resources-tools/resources/securing-election-infrastructure-against-tactics-foreign-malign-influence-operations>.

³ [www.CISA.gov/topics/election-security/rumor-vs-reality](https://www.cisa.gov/topics/election-security/rumor-vs-reality).

⁴ <https://www.nass.org/initiatives/trustedinfo>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Attachment: Management Response to Recommendation Contained in OIG 23-068-AUD-CISA, I&A

OIG recommended that the Director of CISA:

Recommendation 1: Develop and implement a risk-based national strategic plan that addresses current and evolving risks to enhance the security and resilience of the Nation's election infrastructure, including disinformation and the use of artificial intelligence.

Response: Concur. CISA has already begun work developing both a risk assessment and risk management plan for the Election Infrastructure Subsector that will address this recommendation, and both are anticipated to be complete by the end of June 2025. This effort is consistent with, though not bound by, NSM-22, "National Security Memorandum on Critical Infrastructure and Resilience,"⁵ published by the White House National Security Council on April 30, 2024, which updates the national-level guidance related to protecting critical infrastructure.

Specifically, NSM-22 outlines how the U.S. Government will collaborate with key stakeholders to safeguard critical infrastructure, including partnering with relevant departments and agencies, the private sector and state, local, tribal, and territorial partners. The NSM-22 mandates each Sector Risk Management Agency, in consultation with the Sector's Councils, produce a sector risk assessment and sector risk management plan addressing a wide range of risk to critical infrastructure. Although NSM-22 does not specify guidance for subsectors, CISA agrees that developing a Subsector risk assessment and Subsector risk management plan is crucial to support the significant and ongoing efforts to address election infrastructure risks.

Therefore, CISA will work with the Subsector to develop and review the Subsector Risk Assessment in 2025, with subsequent updates planned for odd years to ensure maximum participation from election officials. The new risk assessment and risk management plan will serve as the foundation for future updates to Election Infrastructure Subsector planning documents.

Estimated Completion Date: June 30, 2025.

⁵ <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix C: Major Contributors to This Report Include

Chiu-Tong Tsang, Director
Anna Hamlin, Audit Manager
Stuart Josephs, Auditor
Brendan Burke, Auditor
Kevin Dolloson, Communications Analyst



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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