

**CISA Made Progress but  
Resources, Staffing, and  
Technology Challenges  
Hinder Cyber Threat  
Detection and Mitigation**





**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

March 3, 2023

MEMORANDUM FOR: The Honorable Jen Easterly  
Director  
Cybersecurity and Infrastructure Security Agency

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

SUBJECT: *CISA Made Progress but Resources, Staffing, and  
Technology Challenges Hinder Cyber Threat Detection  
and Mitigation – For Official Use Only*

Digitally signed by JOSEPH  
V CUFFARI  
Date: 2023.03.02 16:11:46  
-07'00'

For your action is our final report, *CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving CISA's cyber intrusion detection and mitigation. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendation 2 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 the 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, 3, and 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. Please send your response or closure request to [OIGTAuditsFollowup@oig.dhs.gov](mailto:OIGTAuditsFollowup@oig.dhs.gov).



## **OFFICE OF INSPECTOR GENERAL**

### Department of Homeland Security

---

Consistent with our responsibility under the *Inspector General Act of 1978, as amended*, 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.

If you have any questions, please call me at (202) 981-6000, or your staff may call Bruce Miller, Deputy Inspector General for Audits, at the same number.

Attachment



# **DHS OIG HIGHLIGHTS**

## ***CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation***

**March 3, 2023**

### **Why We Did This Review**

The Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead for Federal cybersecurity, responsible for coordinating cyber incident response and mitigation. In December 2020, CISA issued an emergency directive about an advanced cyberattack that had caused a breach of SolarWinds software and Federal computing networks. We conducted this review to determine CISA's ability to detect and mitigate risks from major cyberattacks based on lessons learned after the SolarWinds breach.

### **What We Recommend**

We are making four recommendations to address CISA's resource needs and improve technology to enhance cyber detection and mitigation.

#### **For Further Information:**

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

### **What We Found**

Following the SolarWinds breach discovery in 2020, CISA improved its ability to detect and mitigate risks from major cyberattacks, but work remains to safeguard Federal networks. CISA coordinates Federal agencies' defense against cyberattacks, but the SolarWinds response revealed that CISA did not have adequate resources — backup communication systems, staff, or secure space — to effectively respond to threats. This occurred because CISA's continuity, strategic workforce, and workspace allocation plans were not complete or did not meet mission needs.

In response to the May 2021 *Executive Order on Improving the Nation's Cybersecurity*, CISA is improving its ability to detect and mitigate cyber intrusions. CISA completed most of the required tasks in the Executive Order, and it improved its information sharing and coordination.

CISA's after-action reports on the SolarWinds response identified gaps in the technologies and capabilities needed for cyber incident prevention, detection, and mitigation. Before the breach, CISA had begun to bolster its automated cyber threat detection and to develop its malware analysis and data analytics capabilities. However, CISA still needs to receive all the necessary cybersecurity data from other Federal agencies' dashboards and complete its plans for development of malware and data analytics capabilities. Until these efforts are completed, CISA may not always be able to effectively detect and mitigate major cyberattacks or meet the Government's demand for cyber capabilities that protect Federal networks and systems.

### **CISA's Response**

CISA concurred with all four recommendations. Appendix B includes CISA's response memo. Recommendations will remain open pending evidence of CISA's corrective actions.



# OFFICE OF INSPECTOR GENERAL

## Department of Homeland Security

### Table of Contents

Background .....	1
Results of Review .....	4
CISA Did Not Have Adequate Resources to Support SolarWinds Cyberattack Response and Mitigation Efforts.....	5
CISA Took Steps to Improve Management and Operations Following the SolarWinds Cyberattack.....	9
Moving Forward, CISA Needs to Address Remaining Technology Gaps to Support Cyber Intrusion Detection and Mitigation Responsibilities.....	12
Conclusion.....	15
Recommendations.....	16
Management Comments and OIG Analysis .....	17

### Appendixes

Appendix A: Objective, Scope, and Methodology .....	20
Appendix B: CISA Response to the Draft Report.....	21
Appendix C: CISA Employee Climate Survey Results.....	25
Appendix D: Required EO Tasks for CISA .....	26
Appendix E: Office of Audit Major Contributors to This Report.....	27
Appendix F: Report Distribution.....	28

### Abbreviations

CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations
CSD	Cybersecurity Division
EO	Executive Order
GAO	U.S. Government Accountability Office
NCPS	National Cybersecurity Protection System
OMB	Office of Management and Budget





## OFFICE OF INSPECTOR GENERAL

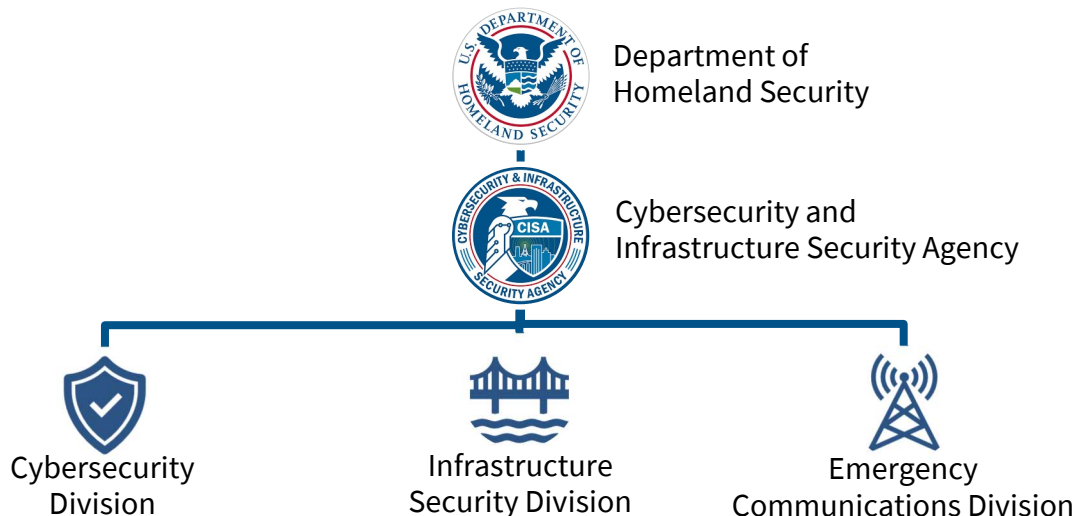
Department of Homeland Security

### Background

The United States faces persistent and increasingly sophisticated malicious cyberattack campaigns that threaten the public and private sectors and ultimately the American people's security and privacy. Federal agencies, including the Department of Homeland Security, depend on information technology systems to carry out operations. However, cyberspace and its infrastructure are vulnerable to a wide range of risks stemming from physical and cyber threats and hazards. Malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead for Federal cybersecurity and heads the national effort to understand, manage, and reduce risks to cyber and physical infrastructure.<sup>1</sup> CISA coordinates government-wide cybersecurity efforts, issues operational and emergency directives detailing ways for agencies to improve cybersecurity, and provides operational and technical assistance to agencies. CISA also provides resources, analysis, and tools to help Federal agencies build resilient network security. Figure 1 depicts CISA's three statutorily required divisions.<sup>2</sup>

**Figure 1. CISA Divisions**



Source: DHS Office of Inspector General analysis of CISA's organizational chart

<sup>1</sup> *Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. 115-278, November 16, 2018.

<sup>2</sup> *Ibid.*






## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

CISA's Cybersecurity Division (CSD) builds the Nation's capacity to defend against cyberattacks. CSD collaborates with public and private entities to identify, mitigate, and respond to cyber threats. It also works with other Federal agencies to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the Federal networks that support its partner agencies' essential operations.

CSD has seven functional areas that, together, facilitate the integration of cybersecurity technologies, products, and services. One of these areas, Capability Delivery, develops cyber intrusion detection and mitigation capabilities that protect Federal networks and systems. Threat Hunting and other CISA divisions use these cyber capabilities to find, analyze, and share information about malicious activity. Table 1 describes three CSD functional areas discussed in this report.

**Table 1. Three CISA CSD Functional Areas and Their Responsibilities**

	<b>Capacity Building</b>	Develops and delivers cybersecurity shared services. Supports civilian agencies and evaluates agency progress towards defined security goals. Manages the Federal Continuous Diagnostics and Mitigation program and the Vulnerability Disclosure Policy Platform.
	<b>Capability Delivery</b>	Builds, acquires, engineers, and provides lifecycle support for the capabilities needed to fulfill CSD's mission. Responsible for the National Cybersecurity Protection System.
	<b>Threat Hunting</b>	Assesses and responds to cyber threats. An analytical component with duties that include cyberattack response, triage, and remediation.

Source: DHS OIG analysis based on CISA website

### SolarWinds Breach

In 2019, a threat actor, later identified as the Russian Foreign Intelligence Service, carried out a campaign of cyberattacks that breached computing networks at SolarWinds, a Texas-based network management software company. The threat actor conducted a software supply chain attack, taking advantage of security vulnerabilities to plant malware (malicious code) in a



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

software update that SolarWinds sent to its clients. When a client installed an infected update, the malware would spread, allowing access to the client's networks and systems. The attack was highly sophisticated and used new techniques and advanced tradecraft to remain undetected for more than a year.

Because the Federal Government widely uses SolarWinds software to monitor network activity on Federal systems, this incident allowed the threat actor to breach infected agency information systems. SolarWinds estimated that nearly 18,000 of its customers could have received a compromised software update. Of those, the threat actor targeted a subset of high-value customers to exploit, including DHS and multiple other Federal agencies, primarily for espionage. The operation was first detected and reported to CISA by a private sector cybersecurity firm.

CISA participated in a task force with other Federal agencies<sup>3</sup> to coordinate a government-wide response to the SolarWinds breach. The task force worked from December 2020 through April 2021 to discover the impact and mitigate the effects of the cyberattack. After CISA completed its SolarWinds response, it prepared several after-action reports that identified lessons learned, capability gaps, and areas for improvement. CISA reported it needed a better communication process, more visibility into Federal agencies' networks, and increased authority to find cyber threats on Federal networks.

The U.S. Government Accountability Office (GAO) also reported in 2022<sup>4</sup> on agencies' actions and lessons learned while responding to the SolarWinds breach. For example, GAO noted a need to invest in technology that aligns with operational priorities and for better information sharing among Federal agencies. GAO also noted that government-wide, 900 of its recommendations addressing cybersecurity shortcomings were still open.

### **Executive Order to Improve Cybersecurity**

The lessons learned from the SolarWinds response helped inform President Biden's administration and Congress of the need to improve cybersecurity. In May 2021, President Biden signed the *Executive Order on Improving the Nation's Cybersecurity*,<sup>5</sup> to support cybersecurity and protect the Nation's critical infrastructure and Federal networks. The Executive Order (EO) requires agencies to take specific actions such as developing procedures to share cyber threat information and standardizing response efforts. The EO

---

<sup>3</sup> The task force, the Cyber Unified Coordination Group, coordinates the investigation and remediation of significant cyber incidents involving Federal networks.

<sup>4</sup> *Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746, January 2022.

<sup>5</sup> EO 14028.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

intends to remove barriers to information sharing, improve cybersecurity, and standardize Federal responses to cyber incidents. Additionally, the Office of Management and Budget (OMB) issued several memos<sup>6</sup> to establish guidance on detecting vulnerabilities, protecting critical software, and improving investigation, assessment, and remediation of cyber incidents.

Congress' fiscal year 2022 omnibus spending bill contained a \$2.6 billion appropriation for CISA. Congress also appropriated \$650 million to CISA in the *American Rescue Plan Act of 2021*. The funding should help CISA enhance its cybersecurity tools, hire experts, and obtain support services to protect and defend Federal information technology systems. CISA planned to spend \$257.5 million to provide critical cyber tools to enhance network visibility and detections government-wide. Another \$733 million was dedicated to improving two programs in CSD for building malware and data analysis capabilities, as well as improving the government-wide program for continuous diagnostics and mitigation, which provides tools and services to help Federal agencies improve their cybersecurity.

We conducted this review to determine CISA's ability to detect and mitigate risks from major cyberattacks based on lessons learned after the SolarWinds breach.

### Results of Review

Following the SolarWinds breach discovery in 2020, CISA improved its ability to detect and mitigate risks from major cyberattacks, but work remains to safeguard Federal networks. CISA coordinates Federal agencies' defense against cyberattacks, but the SolarWinds response revealed that CISA did not have adequate resources — backup communication systems, staff, or secure space — to effectively respond to threats. This occurred because CISA's continuity, strategic workforce, and workspace allocation plans were not complete or did not meet mission needs.

In response to the May 2021 EO, CISA is improving its ability to detect and mitigate cyber intrusions. CISA completed most of the required tasks in the EO, and it improved its information sharing and coordination.

CISA's after-action reports on the SolarWinds response identified gaps in the technologies and capabilities needed for cyber incident prevention, detection,

---

<sup>6</sup> *Protecting Critical Software Through Enhanced Security Measures*, OMB-M-21-30, August 2021; *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, OMB-M-21-31, August 2021; and *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, OMB M-22-01, October 2021.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

and mitigation. Before the breach, CISA had begun to bolster automated cyber threat detection and develop its malware analysis and data analytics capabilities. However, CISA still needs to receive all the necessary cybersecurity data from other Federal agencies' dashboards and complete its plans for development of malware and data analytics capabilities. Until these efforts are completed, CISA may not always be able to effectively detect and mitigate major cyberattacks or meet the Government's demand for cyber capabilities that protect Federal networks and systems.

### **CISA Did Not Have Adequate Resources to Support SolarWinds Cyberattack Response and Mitigation Efforts**

The SolarWinds breach revealed that CISA was not well-equipped to meet its current and evolving cyber intrusion detection and mitigation responsibilities. Specifically, CISA did not have an alternative communication system to use when its main network was compromised, enough staff to achieve its mission, or the secure space required to effectively work with available intelligence. This occurred because CISA's continuity, strategic workforce, and workspace allocation plans were either not complete or did not meet functional mission needs. As a result, CISA could not effectively coordinate its Federal response efforts or use intelligence information from partner agencies.

### **CISA Did Not Have Adequate Backup Communication Systems for Continuity of Operations**

CISA relies on an unclassified network for email and data communication to achieve its day-to-day cybersecurity mission, including vulnerability management, incident response, and information and data sharing. This network was compromised during the SolarWinds breach, creating a risk that CISA's actions on the network could be monitored in real time, hindering response efforts. CISA did not have a secure unclassified system to use in the network's place.

To effectively respond to the breach, CISA employees needed a secure communication system to coordinate internally and communicate vital information with external partners. With no alternative unclassified network available, CISA staff improvised, using a variety of communication methods, such as alternative messaging platforms and removable media.

According to CISA, this resulted in the frequent loss or delayed delivery of critical information throughout its response, which led to significant confusion, inefficient operations, and a reduction in leadership's ability to manage the response effort. In an after-action report, CISA identified its inability to



## OFFICE OF INSPECTOR GENERAL

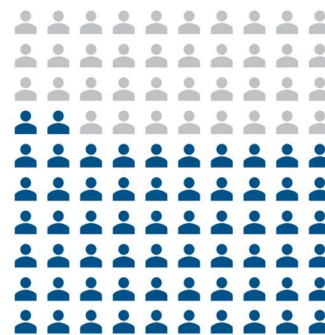
### Department of Homeland Security

effectively communicate during the SolarWinds response as an area for improvement.

Agencies are required to put comprehensive and effective capabilities in place to ensure uninterrupted performance of their mission.<sup>7</sup> To facilitate this, agencies must develop a Continuity of Operations (COOP) Plan along with information system contingency plans. At CISA, employees must communicate effectively to mitigate cyberattacks — an essential function of CISA’s mission. During the SolarWinds response, CISA did not have plans or procedures to ensure uninterrupted communication and operations if a communication network was compromised.<sup>8</sup> At the end of our fieldwork, CISA had not yet updated its COOP Plan or created a supplemental communication plan to ensure redundant systems, capabilities, and communication methods would be available if the network hosting its primary systems was compromised.

### CISA Did Not Have Enough Staff to Execute Its Mission

CISA’s mission execution depends on a properly staffed organization with the skills, competencies, and performance capabilities necessary to meet cybersecurity challenges. However, CISA has struggled to maintain sufficient staffing levels. For example, CSD, the CISA division primarily responsible for defending against cyberattacks and responding to cyber incidents, was 33 percent understaffed at the close of FY 2021. By August 2022, the number of vacancies in CSD had increased to 38 percent. CISA as a whole was also understaffed. In August 2022, 1,201 of the 3,620 full-time positions CISA was authorized were unfilled.



**38%**  
of CISA CSD's  
positions were  
vacant in  
August 2022

In Fall 2021, CISA surveyed its employees about their work environment and found that most respondents were concerned about staffing. A total of 736 CISA employees completed the 21-question survey, a response rate of about 30 percent. Although the CISA workforce generally responded positively, one question had a distinctly negative answer — 61 percent of the respondents said CISA did not have enough people to complete its mission. When answers were broken out by division, 64 percent of CSD’s employees responded negatively to this question. Figure 2 shows the two most positive and two most negative survey responses, and Appendix C shows all 21 survey questions and responses.

<sup>7</sup> Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, July 2016.

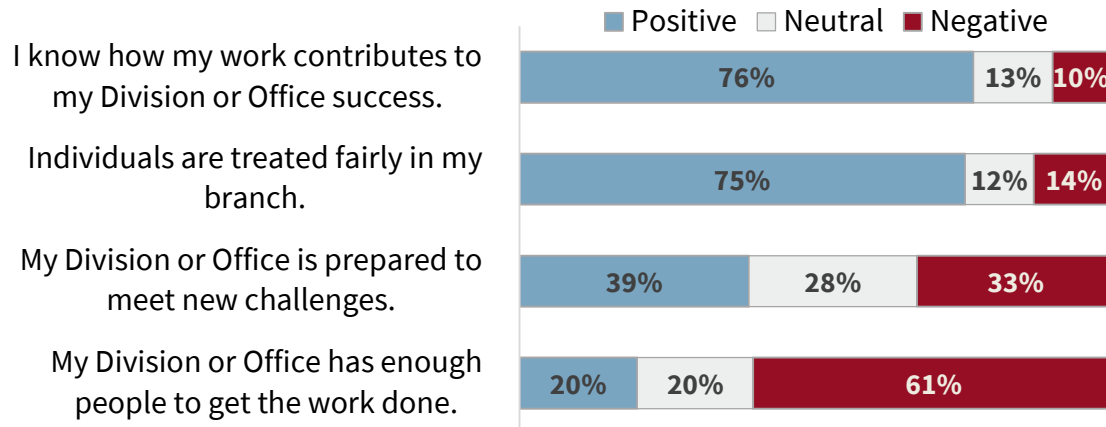
<sup>8</sup> CISA’s *Continuity of Operations Plan*, December 2020.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

**Figure 2. CISA Employee Responses to Survey Questions about Mission, Culture, Staffing, and Preparedness**



Source: DHS OIG-prepared, based on CISA's Fall 2021 survey results

To corroborate these results, we interviewed CISA management officials between January and August 2022 about their staffing levels, and all said they were understaffed. According to the CISA officials, this was due to several factors:

- Attracting personnel with the right experience and training who are willing to accept the pay scale (typically half of the industry standard), and able to obtain a security clearance, is difficult.
- Hiring can take 6 to 12 months for Government employees and contractors with the hard-to-find cyber-specific skillsets required.
- CISA does not have enough hiring managers and support staff, further prolonging the hiring process. Like other CISA divisions, those in charge of hiring are also short staffed.
- After employees do get hired, they work extra hours, burn out quickly, and often leave, which starts the hiring cycle over again.

Despite its hiring difficulties, CISA does not have a multiyear strategic workforce plan to help ensure it hires staff with the right knowledge, skills, and abilities to achieve goals and address workforce needs. In a strategy document, CISA recognized a strategic workforce plan is both an urgent need and a requirement.<sup>9</sup> However, CISA's Office of the Chief Human Capital Officer has not completed a plan that would identify workforce gaps and develop strategies and implementation plans, as required.<sup>10</sup>

<sup>9</sup> CISA Agency Workforce Planning Strategy, FY 2022–FY 2026, June 2021.

<sup>10</sup> Office of Personnel Management, *Human Capital Operating Plan Guidance FYs 2022–2026*, December 2021.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

#### **CISA Facilities and Intelligence Access Did Not Meet Operational Needs for Information Sharing**

CISA staff reported they did not have enough, or the correct type of, secure space to effectively use available intelligence during the SolarWinds response (December 2020 to April 2021). Employees must use secure (classified) facility space when they work with sensitive information, and the type of facility determines what an employee can do with information in that facility. Depending on the facility, employees may read information; read and discuss information; or read, discuss, analyze, and process information.

Access to classified facilities is even more critical when responding to a significant cyber incident. During such times, CISA requires a rapid increase in resources, including additional staff assigned to response activities and additional access to classified space. To overcome this limitation during the SolarWinds response (which was further complicated by the COVID-19 pandemic), staff worked in shifts to ensure everyone could access secure spaces. This reduced the facility time available to analysts working on critical aspects of CISA's response for at least 5 months.

Secure space was also not configured effectively, leaving teams unable to discuss, analyze, and process sensitive information as needed. For example, CISA staff reported that analysts did not have sufficient classified workspace, areas for private conversations, or appropriate access to some classified information. CISA officials told us this occurred because officials from CSD and CISA's facilities division disagreed about classified workspace allocation and functional mission needs. However, facilities personnel acknowledged that access to some secure space is limited and noted that, over time, CISA's mission size and staff numbers had increased faster than its facility space.

In addition, some staff did not have necessary access to intelligence information during the SolarWinds response, while others had access they did not need or could not use effectively. Access to intelligence was limited to a specific number of people, including executives who had a need to know but could not mitigate threats. As a result, some employees who could use the intelligence to mitigate threats did not have access to it, and the executives who did have access could not share it with these employees. This created delays that negatively affected CISA's response.

As a result of the facility configuration and intelligence access issues, CISA sometimes could not effectively use intelligence from its partners in a timely manner. According to CISA officials, they have partially resolved the intelligence access issues, and some critical analysts now have the necessary





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

access. Additionally, the classified workspace and facility configuration issues remain unresolved. Following the release of our draft report, CISA officials informed us that some existing capacity restrictions were discontinued.

### **CISA Took Steps to Improve Management and Operations Following the SolarWinds Cyberattack**

After the SolarWinds breach in 2020 and numerous other cyberattacks during 2021, the focus on Federal cybersecurity protections increased. CISA received more funding and authority and took steps to improve management and operational functions that support its partnerships and cyber capabilities. CISA also launched a platform for public disclosure of system vulnerabilities and obtained funding for improved network visibility and analysis capabilities.

### **CISA Completed Most Tasks the Executive Order Required**

The May 2021 EO requires agencies to complete specific actions to improve cybersecurity. In part, the EO's goal was to improve the Federal Government's access to cyber threat information, to increase information sharing among Federal agencies, and to obtain information from private entities. The EO also sought to modernize Federal cybersecurity and increase the network visibility (the awareness of a network's components and data) needed to identify and mitigate threats.

CISA was partially or fully responsible for completing 14 tasks from the EO, including developing procedures for sharing incident reports, creating standardized response playbooks, and issuing requirements for cyber initiatives. (See Appendix D for the complete task list.) CISA completed 13 of the tasks but it did not complete one task — developing a collaboration framework for cybersecurity and incident response activities for Federal cloud technology. Although the deadline for this final task was August 2021, CISA was still developing the framework when we completed our review.

### **CISA's Authorities Increased**

The SolarWinds breach and other recent cyberattacks highlighted the significant cyber threats facing the Nation and the consequences these attacks pose, including disruption of critical operations and physical infrastructure. Accordingly, CISA received two additional authorities in 2021.<sup>11</sup> First, CISA can hunt for threats and identify vulnerabilities on Federal networks without agencies' advanced notification or authorization. Second, CISA was granted

---

<sup>11</sup> *National Defense Authorization Act for FY 2021*, Pub. L. 116–283, Sections 1705 and 1716, January 1, 2021.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

administrative subpoena authority to obtain information from internet service providers about vulnerabilities and notify the associated system owners about the vulnerabilities.

### **CISA Strengthened Collaboration with Its Partners**

In response to the increasing cyber threat landscape, CISA has begun to strengthen cybersecurity coordination, collaboration, and reporting, as well as vulnerability disclosure. In August 2021, CISA established the Joint Cyber Defense Collaborative<sup>12</sup> to reinforce its relationships with private sector and interagency partners. The goal is to strengthen the Nation's cyber defenses through collaboration, advanced preparation, and information sharing. This includes analyzing and combining cybersecurity information along with sharing guidance to reduce cyber risks that affect National Critical Functions.<sup>13</sup>

In addition, CISA integrated liaisons from other agencies into its operations and created new ways to rapidly communicate with private and Federal partners. CISA also helped create internal guidance for Federal agencies on sharing cyber incident reports to strengthen communication among agencies on these incidents. The guidance contains roles and responsibilities for CISA, the National Security Agency, and Federal Cyber Centers, outlining:

- what information each agency should share;
- what sensitive data CISA should remove before sharing; and
- timeliness standards for information sharing.

Finally, CISA developed *Cybersecurity Incident & Vulnerability Response Playbooks*<sup>14</sup> to assist with cyber response. The playbooks provide standard procedures for agencies to identify, coordinate, remediate, recover, and track cyber incidents.

### **CISA Launched Platform for Public Disclosure of System Vulnerabilities**

To encourage collaboration between Federal agencies and the public, CISA issued binding operational directives for agencies to develop and publish a

---

<sup>12</sup> <https://www.cisa.gov/jcdc>.

<sup>13</sup> National Critical Functions are Government and private sector functions so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

<sup>14</sup> [https://www.cisa.gov/sites/default/files/publications/Federal\\_Government\\_Cybersecurity\\_Incident\\_and\\_Vulnerability\\_Response\\_Playbooks\\_508C.pdf](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

vulnerability disclosure policy and remediation process.<sup>15</sup> These directives support OMB's 2020 guidance for identifying vulnerabilities<sup>16</sup> and require Federal agencies to develop and publish consistent policies on disclosing and remediating vulnerabilities. These policies are meant to encourage members of the public to find and report vulnerabilities legally — essentially allowing the public to make ethical hacking disclosures to Federal agencies.<sup>17</sup> CISA was also required to catalog known exploited vulnerabilities and alert agencies when updates and actions are needed.

To help agencies find vulnerabilities, in January 2022, CISA launched a vulnerability disclosure platform — a website giving members of the public a way to report vulnerabilities and issues to DHS and other participating agencies. Participating Federal agencies can use the platform to collect reports for their vulnerability disclosure programs. The platform is intended to improve information sharing between Federal agencies and the public and improve agencies' ability to remediate vulnerabilities before they can be exploited. The platform:

- provides automated metrics and notifications;
- links reports by vulnerability type or reporting party;
- helps agencies match submissions with cataloged known exploited vulnerabilities; and
- provides a way for the agency and reporting party to communicate.

Since it was launched, 32 agencies started using the platform to support various disclosure programs. Although CISA maintains visibility into disclosure activity, it does not actively remediate disclosures. Agencies address vulnerabilities that are reported by the public, and in some cases an agency may pay a reward to the reporting party.

### **DHS Invested in CISA's Network Visibility and Analysis Capabilities**

CISA's mission depends on innovative technology to defend the Federal cyber infrastructure. DHS spent \$93 million in FY 2022 to mitigate effects of the SolarWinds breach, support recovery solutions, and reduce vulnerabilities. An

---

<sup>15</sup> *Develop and Publish a Vulnerability Disclosure Policy*, Binding Operational Directive 20-01, September 2, 2020; *Reducing the Significant Risk of Known Exploited Vulnerabilities*, Binding Operational Directive 22-01, November 3, 2021.

<sup>16</sup> *Improving Vulnerability Identification, Management, and Remediation*, OMB M-20-32, September 2, 2020.

<sup>17</sup> In ethical hacking, a hacker attempts to break into a system, simulating a malicious cyberattack, and then reports vulnerabilities and weaknesses in the hacked system. White hat hackers are ethical hackers. Gray hat hackers may act without malicious intent and inform the system owner of vulnerabilities.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

internal analysis<sup>18</sup> by CISA found that CISA needed additional capabilities to provide network visibility and allow analysis of malicious activity. In response, to address CISA's needs, DHS funded three activities:

1. obtain enhanced network monitoring tools;
2. increase CISA's cyber threat hunting capability (detecting threats that have not been discovered by normal security monitoring); and
3. purchase identity authentication tools and Microsoft licensing that includes history logs used to investigate incidents.

These investments help ensure CISA and DHS can make informed decisions using data analytics and visualization. They also help safeguard Federal networks against malicious threats spread by email messages, links, and collaboration tools.

### **Moving Forward, CISA Needs to Address Remaining Technology Gaps to Support Cyber Intrusion Detection and Mitigation Responsibilities**

The SolarWinds breach demonstrated the need for significant improvements in CISA's network visibility and threat identification technology. CISA was already developing many cyber defense capabilities before the breach, but some were not completed. This occurred because CISA has not received all the data it needs from other Federal agencies' Continuous Diagnostics and Mitigation (CDM) programs, nor has it fully developed plans for its Malware NextGen analysis tool or the data analytics capability in the National Cybersecurity Protection System (NCPS). CISA must complete these efforts to ensure it can meet the Government's demand for cyber capabilities that protect Federal networks and systems.

### **Continuous Diagnostics and Mitigation Program Has Not Provided Sufficient Information**

The Federal CDM program was established in 2013<sup>19</sup> to support government-wide and agency-specific efforts to provide cybersecurity solutions to protect Federal civilian networks. The program delivers cybersecurity tools, services, and dashboards that help participating agencies improve their security posture by monitoring network devices and activity. When fully implemented and with appropriate access granted, CDM will allow CISA and other Federal agencies to monitor vulnerabilities and reduce threats to their systems in near-real time.

---

<sup>18</sup> CISA's *Authorities Gap Analysis*, September 2021.

<sup>19</sup> *Enhancing the Security of Federal Information and Information Systems*, OMB Memorandum M-14-03, November 18, 2013, required that agencies establish programs for managing information security risk on a continuing basis.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

As part of its management of CDM, CISA is responsible for a key feature of the program, a Federal CDM dashboard, that consolidates and displays summary information from each Federal agency. The dashboard should inform decision makers about cybersecurity risks across the Federal Government, with a focus on managing the highest priority and most serious risks.

For the Federal CDM dashboard to work, agencies must install network tools and sensors that gather data and feed an agency-level dashboard. Agency programs then feed this information to the Federal CDM dashboard. This collective information helps CISA gain situational awareness and visibility so it can better identify and respond to risks. However, CISA's December 2021 *Operational Visibility Strategy* states that CDM gives CISA only minimal visibility into agency environments and vulnerabilities.

When an agency's CDM program is incomplete or does not provide quality data, it affects CISA's ability to respond to cyber threats. In recent audits, GAO<sup>20</sup> and our office<sup>21</sup> found that some Federal agencies, including DHS, did not fully implement key CDM requirements or provide needed network visibility to CISA's Federal CDM dashboard. Further, CISA did not have access to the quality and quantity of data necessary for effective cyber capabilities.

Because some agency programs provided only limited information to the dashboard, CISA could not use CDM data effectively during the SolarWinds response. According to CISA personnel, the information CDM was supposed to provide would have been helpful when responding to the SolarWinds breach and other cyber events. Until agency CDM capabilities are complete, CISA cannot effectively use the Federal dashboard data to manage, prioritize, and respond to cyber risks in real time.

Although some of the program implementation is not within CISA's control, CISA has continued to develop capabilities for CDM since the SolarWinds breach. For example:

- CISA launched the Endpoint Detection Response capability to monitor Federal networks and detect threat activity, which will improve CDM's network security management capability.
- CISA is refreshing CDM dashboard technology across the Federal civilian executive branch agencies, which should provide access to previously unavailable stored network data.

---

<sup>20</sup> *DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598, August 2020.

<sup>21</sup> *DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program*, OIG-21-38, June 2021.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

- CISA will provide data to OMB to facilitate a new OMB requirement to score agencies' CDM performance and compliance data. OMB will begin scoring agencies' progress implementing CDM in December 2022, and the scores will assess each agency's ability to report automated data in CDM.

### **CISA Is Developing Automated Malware Analysis Capability**

CISA began developing Malware NextGen in May 2019 to help achieve its mission of providing operational and technical assistance to its partner agencies. Malware NextGen is a flexible cloud-based platform for analyzing malicious code<sup>22</sup> received from agencies and partners. CISA analysts extract the code for manual analysis, allowing them to quickly prioritize, investigate, and resolve malware analysis requests.

The Malware NextGen capability is still under development, even though the program was authorized to operate in March 2022 and is the only viable malware analysis option for many of CISA's mission partners. CISA is developing additional functionality for Malware NextGen, with updated technology to improve timely and effective identification of malicious activity and exploitation. According to CISA, when the next development phase is complete, Malware NextGen will automate analysts' ability to reverse engineer malware to analyze code, identify potential adversaries' behavior, and mitigate threats. It will also incorporate automated data and trend analysis tools.

CISA has not yet determined when it expects to finish the program's analysis functions. If additional requirements are met, the Authority to Operate will continue after its current expiration date of 2025. Until these functions are complete, CISA cannot fully automate analysis of how malware incidents affect its systems and those of its partners. It also cannot understand and mitigate the tactics of adversaries to prevent future incidents.

### **CISA Is Developing Data Analytics Capability for the National Cybersecurity Protection System without a Comprehensive Plan**

CISA has identified a need for additional data analytics capability in its NCPS, which would enable CISA to identify trends and critical vulnerabilities. CSD's Capability Delivery Division develops these cyber capabilities for CSD and other CISA divisions to use. CISA specifically wants to build detection and other data analytics capabilities for cyber analysts to use to assess and interpret information about threats and vulnerabilities on Federal networks. These

---

<sup>22</sup> Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Malicious code includes viruses, worms, Trojan horses, and malicious data files.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

improvements would enable CISA to obtain alert information, correlate it with other available data, and derive information needed to identify and mitigate cyber risks. According to CISA, CSD also needs a cloud analytic environment to support data analysis. CISA expects the cloud environment to help automate analysis, significantly increasing efficiency and effectiveness.

At the time of our review, CSD had not fully planned the requirements for the data analytics capability it is developing. According to CISA officials, this was partly because CISA was restructuring some Capability Delivery programs to better align with operational changes within the agency. Additionally, at the time of our review, CSD had not completed strategic initiatives or decided which Division would own, operate, or maintain the legacy NCPS data analytics capabilities.

CISA started the planning process and received \$25 million in the FY 2023 budget as “bridge funding” to allow continued investment in infrastructure and analytics capabilities until the FY 2024 budget is appropriated. CISA officials told us the comprehensive plan will be completed before FY 2024. Until then, CISA is developing analytics capabilities using the legacy NCPS program without an approved program structure or plan describing how the new project meets strategic priorities. Without the new structure and plan, CISA risks wasting resources, delivering solutions that do not align with CISA’s mission needs, and impacting CISA’s ability to detect cyber incidents.

### **Conclusion**

CISA’s ability to execute its mission depends on its people, processes, and technology. CISA’s SolarWinds response efforts were impacted by not having needed resources, staffing, and plans. Although CISA’s capabilities have improved since the SolarWinds breach, any operational or technological gaps may reduce its ability to detect and mitigate cyber threats. Staffing shortages also affect CISA’s future development of cyber capabilities.

Unless resource, staffing, and planning issues are corrected, CISA will remain heavily dependent on old or unfinished systems, a scarce cybersecurity talent pool, and tools that do not provide necessary visibility into persistent cyber threats. Further, until CISA’s cyber capabilities are fully operational, the Federal Government cannot fully benefit from the cybersecurity protections CISA provides. As a result, the confidentiality, integrity, and availability of Federal data and networks remain at risk at a time when the United States is facing a growing number of increasingly sophisticated cyber threats.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

### Recommendations

**Recommendation 1:** We recommend the CISA Director update CISA's Continuity of Operations Plan and develop and implement an information system contingency plan, to ensure availability of redundant systems, capabilities, and communication methods to use if primary systems or networks are compromised.

**Recommendation 2:** We recommend the CISA Director require the facility and operations staff conduct an assessment to determine whether secure facility space is appropriately sized and configured to meet operational needs and document any changes necessary for staff to obtain and maintain appropriate access to intelligence information.

**Recommendation 3:** We recommend the CISA Director require an assessment to document the levels of staffing, resources, and intelligence access needed for operational divisions, cyber detection and mitigation capabilities, and support functions.

**Recommendation 4:** We recommend the CISA Director create and implement a long-term plan for the Cybersecurity Division that includes provisions for ownership, operations, and maintenance of the National Cybersecurity Protection System's data analytics capabilities.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Management Comments and OIG Analysis

CISA concurred with all four recommendations. Appendix B contains a copy of CISA's response memo. We also received technical comments under separate cover, and we revised the report as appropriate. A summary of CISA's memo and recommendation responses, along with our analysis follows.

In its response, CISA leadership thanked the OIG for recognizing CISA's efforts to identify and respond to lessons learned after the SolarWinds supply chain compromise. However, CISA asserted it had completed all 14 required tasks assigned through EO 14028. Specifically, CISA believes it has established a framework to collaborate on cybersecurity and incident response activities by issuing *Cybersecurity Incident & Vulnerability Response Playbooks* on November 16, 2021. According to CISA, the playbooks act as a framework for response activities for Federal cloud technology.

The OIG does not agree with this assertion, as we determined CISA completed 13 of 14 required tasks. We credited CISA for issuance of the playbooks but concluded that this addressed a separate EO 14028 requirement to "develop a standard set of operational procedures to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting [Federal Civilian Executive Branch] Information Systems." The playbooks include an expectation that cloud service providers report incidents, but we do not believe the playbooks meet the intent of the EO requirement to establish a framework for collaboration specific to cloud technology, ensuring effective information sharing between agencies and cloud service providers. Additionally, during our fieldwork, CISA officials told the OIG they were developing a different deliverable to satisfy this EO requirement. Therefore, we did not consider this task complete.

**CISA Response to Recommendation 1:** Concur. CISA Readiness and Continuity (Continuity) will update and issue a revised COOP Plan in 2023. Additionally, CISA Continuity, in collaboration with CISA's Chief Information Officer, Cybersecurity Division, and other CISA organizations, as appropriate, will define requirements, resourcing, development and implementation of a separate information systems contingency plan to address availability of redundant systems, capabilities, and communications methods. Following this effort, CISA will assess the need for any potential procurement of redundant systems and related resource implications. Estimated Completion Date (ECD): October 31, 2023.

**OIG Analysis of CISA Comments:** CISA's corrective action is responsive to the recommendation. This recommendation will remain open and resolved until



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

CISA provides a copy of the COOP Plan, information systems contingency plan, and needs assessment.

**CISA Response to Recommendation 2:** Concur. Based on recent assessments of security facility space, CISA Facilities increased capacity, to include adding seats in the National Capital Region in June 2022. In FY 2022, CISA Facilities also initiated and funded projects to address additional mission-specific space needs identified in an assessment of a nearby facility. Going forward, CISA will continue to explore potential space and furniture configurations to increase the number of seats, as appropriate. ECD: December 29, 2023.

**OIG Analysis of CISA Comments:** CISA's response is partially responsive to the recommendation. The intent of this recommendation is for CISA's facility and operations staff to collaborate on an assessment to determine whether secure facility space is appropriately sized and configured to meet operational needs and document any changes necessary for staff to obtain and maintain appropriate access to intelligence information. Although CISA Facilities has made improvements in the region, this recommendation will remain open and unresolved until CISA provides documentation showing the collaboration and assessment results.

**CISA Response to Recommendation 3:** Concur. CISA leadership is already conducting assessments to ensure it documents and maintains sufficient staffing and resources to meet mission operations. Since mid-2021, the CISA Office of Strategy, Policy, and Plans has led a CISA-wide effort to conduct high-level force structure and capabilities assessments to better understand its gaps and support congressional requirements. The final report is expected by the end of 2023. In addition, as previously noted, CISA is conducting an assessment to understand and plan for necessary access to intelligence. ECD: December 29, 2023.

**OIG Analysis of CISA Comments:** CISA's corrective action is responsive to the recommendation. This recommendation will remain open and resolved until CISA provides a copy of the plan or plans that address staffing, resources, and intelligence access needs.

**CISA Response to Recommendation 4:** Concur. The Capability Delivery subdivision of the Cybersecurity Division is developing program documentation to support formal establishment of the Cyber Analytic and Data System program, which will include the data analytics capabilities of the National Cybersecurity Protection System. The program documentation will include operational mission needs, a cost assessment, and initial delivery schedule for the Cyber Analytic and Data System program, which will be submitted to the





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Department's Office of Program Accountability and Risk Management for review and approval by March 31, 2023. ECD: May 31, 2023.

**OIG Analysis of CISA Comments:** CISA's corrective action is responsive to the recommendation. This recommendation will remain open and resolved until CISA provides a copy of the approved program documentation.



## OFFICE OF INSPECTOR GENERAL

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*.

The objective of our evaluation was to determine CISA's ability to detect or mitigate risks from major cyberattacks based on lessons learned after the SolarWinds breach. This evaluation focused on CISA's roles, responsibilities, authorities, policies, and procedures for detecting and mitigating cybersecurity incidents. We specifically evaluated the CSD.

To answer our objective, we conducted interviews, obtained documents, and assessed information relevant to our objective. For example, we:

- held teleconferences with DHS and CISA officials;
- interviewed relevant CISA personnel;
- observed the workspace environment at CISA's office in Arlington, VA; and
- determined compliance with CISA requirements and other applicable policies, procedures, and standards.

During fieldwork, our team reviewed and applied criteria such as:

- Executive Order 14028: *Improving the Nation's Cybersecurity*
- Applicable Federal laws, regulations, and guidance
- Applicable NIST special publications Department policies and guidance, specifically DHS 4300A Policy
- *CISA Agency Workforce Planning Strategy*, FY 2022–FY 2026, June 2021
- Office of Personnel Management, *Human Capital Operating Plan Guidance FYs 2022–2026*, December 2021
- Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, July 2016

We conducted this evaluation between January 2022 and August 2022 under the authority of the *Inspector General Act of 1978, as amended*, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix B**  
**CISA Response to the Draft Report**

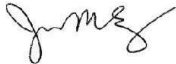
U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

February 3, 2023

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

FROM: Jen Easterly   
Director  
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "CISA Made  
Progress but Must Address Resource, Staffing, and  
Technology Challenges"  
(Project No. 22-026-AUD-CISA)

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

CISA leadership is pleased to note OIG's recognition of CISA's efforts to identify and respond to lessons learned after the SolarWinds supply chain compromise. However, while the OIG report credits CISA with completing 13 of 14 required tasks assigned through Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," dated May 12, 2021, CISA believes it has completed all 14 tasks. This includes issuance of the "Cybersecurity Incident and Vulnerability Response Playbooks" on November 16, 2021<sup>1</sup>, which provide agencies with operational procedures for planning and conducting cybersecurity incident and vulnerability response activities, and act as a framework for response activities for Federal cloud technology. CISA is building on these successes through transformational cultural, organizational, and technological changes to continue to make meaningful progress toward protecting Federal networks and systems.

OIG also recognized the continued need for additional resources to significantly improve CISA's network visibility and threat identification capabilities. CISA plans to leverage current and future investments to drive expedited and informed risk decisions using data analytics and visualization, as well as maximize our ability to safeguard Federal networks

<sup>1</sup> <https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability>



## **OFFICE OF INSPECTOR GENERAL**

### **Department of Homeland Security**

---

against malicious threats. CISA remains committed to improving its ability to detect and mitigate risks from major cyberattacks in order to safeguard Federal networks.

The draft report contained four recommendations with which CISA concurs. Enclosed find our detailed response to each recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, sensitivity and other issues under a separate cover for OIG's consideration.

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

Enclosure



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

#### Enclosure: Management Response to Recommendations Contained in 22-026-AUD-CISA

OIG recommended that the CISA Director:

**Recommendation 1:** Update CISA’s Continuity of Operations Plan, or develop and implement an information system contingency plan, to ensure availability of redundant systems, capabilities, and communication methods to use if primary systems or networks are compromised.

**Response:** Concur. CISA Readiness and Continuity (Continuity) will update and issue a revised Continuity of Operations (COOP) Plan in 2023. However, it is important to note that the COOP Plan only identifies capabilities that enable “Mission Essential Functions” to continue. Accordingly, CISA Continuity, in collaboration with CISA’s Chief Information Officer, Cybersecurity Division, and other CISA organizations, as appropriate, will work to define requirements, resourcing, development and implementation of a separate information systems contingency plan to address availability of redundant systems, capabilities, and communications methods. Following this effort, this community of CISA organizations will then assess the need for any potential procurement of redundant systems, and related resource implications. Estimated Completion Date (ECD): October 31, 2023.

**Recommendation 2:** Require the facility and operations staff conduct an assessment to determine whether secure facility space is appropriately sized and configured to meet operational needs and document any changes necessary for staff to obtain and maintain appropriate access to intelligence information.

**Response:** Concur. Based on recent assessments of security facility space, CISA Facilities increased Sensitive Compartmented Information Facility (SCIF) capacity, to include adding further SCIF seats in the National Capital Region in June 2022. In Fiscal Year (FY) 2022, CISA Facilities also initiated and funded projects to address additional mission specific space needs. Going forward, CISA will continue to explore potential space and furniture configurations to increase the number of SCIF seats that are Compartmented Area compliant depending on mission needs, as appropriate. ECD: December 29, 2023.

**Recommendation 3:** Require an assessment to document the levels of staffing, resources, and intelligence access needed for operational divisions, cyber detection and mitigation capabilities, and support functions.

**Response:** Concur. CISA leadership is already conducting assessments to ensure that it documents and maintains sufficient staffing and resources to meet mission operations.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Since mid-2021, the CISA Office of Strategy, Policy, and Plans has led a CISA-wide effort to conduct high-level force structure and capabilities assessments to better understand its gaps and support Congressional requirements. The final report is expected by the end of calendar year 2023. In addition, as noted in a previous response, CISA is conducting SCIF assessment to understand and plan for necessary access to intelligence . ECD: December 29, 2023.

**Recommendation 4:** Create and implement a long-term plan for the Cybersecurity Division that includes provisions for ownership, operations, and maintenance of the National Cybersecurity Protection System's data analytics capabilities.

**Response:** Concur. The Capability Delivery subdivision of the Cybersecurity Division is developing the program documentation to support the formal establishment of the Cyber Analytic and Data System (CADS) program, which will include the data analytics capabilities of the National Cybersecurity Protection System. The program documentation will further detail: (1) the operational mission needs; (2) a rough order of magnitude cost assessment; and (3) initial schedule for the continuous delivery of the CADS program, which will be submitted to the Department's Office of Program Accountability and Risk Management (PARM) for review and approval by March 31, 2023. Moreover, the Continuous Diagnostics and Mitigation (CDM) Program supports the evolution of this analytics capability through improved host-level visibility acquired through enhanced logging agents, rapid Federal Civilian Executive Branch adoption and operationalization of Endpoint Detection and Response (EDR), as well as through object level data access. These initiatives give CISA analysts the ability to search, extract, and load more detailed cyber information through CDM to enable our cyber defense operations, including by integrating these data sets into the CADS program for the purposes of developing advanced analytics. ECD: May 31, 2023.

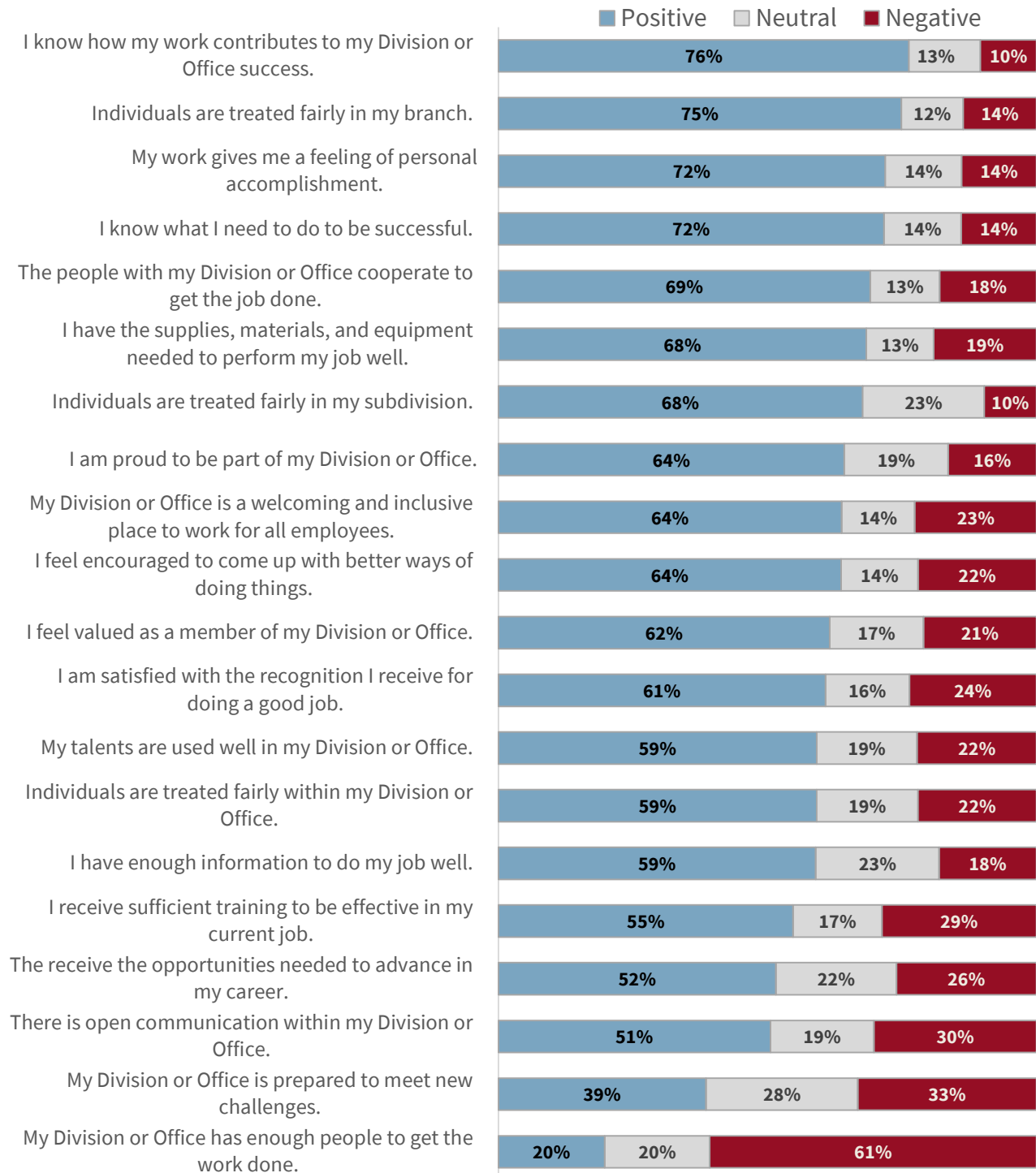


## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

## Appendix C

### CISA Employee Climate Survey Results



Source: DHS OIG-prepared, based on CISA's climate survey results



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Appendix D

#### Required EO Tasks for CISA

The May 2021 EO required that multiple agencies enhance cybersecurity through a variety of initiatives related prevention, detection, assessment, and remediation of cyber intrusions. These initiatives included:

- Removing Barriers to Sharing Threat Information
- Modernizing Federal Government Cybersecurity
- Enhancing Software Supply Chain Security
- Establishing a Cyber Safety Review Board
- Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Improving the Federal Government's Investigative and Remediation Capabilities

CISA was partially or fully responsible for completing 14 tasks from the EO. We determined that CISA met 13 of the tasks:

- ✓ Ensure service providers share data.
- ✓ Develop procedures for cyber incident report sharing.
- ✓ Recommend contract language regarding cyber information and reporting, and privacy protections.
- ✓ Recommend standardized contract language.
- ✓ Issue cloud-security architecture documentation.
- ✓ Issue a cloud-service governance framework.
- ✓ Develop operational procedures (playbooks).
- ✓ Issue recommendations for Endpoint Detection and Response.
- ✓ Develop information sharing procedures.
- ✓ Provide recommendations on requirements for logging events.
- ✓ Recommend standardized contract language for cybersecurity requirements.
- ✓ Manage the Cyber Safety Review Board.
- ✓ Ensure adequate resources to comply with Endpoint Detection and Response requirements.
- ✗ Establish a framework to collaborate and ensure effective information sharing with cloud service providers on cybersecurity and incident response activities related to cloud technology for the Federal civilian executive branch.



## **OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

---

### **Appendix E**

#### **Office of Audit Major Contributors to This Report**

Richard Harsche, Director  
Priscilla Cast, Audit Manager  
Nathaniel Nicholson, Auditor in Charge  
Garrick Greer, Auditor  
Brian Smythe, Auditor  
Stefanie Tynes, Auditor  
Susan Parrott, Communications Analyst  
Terrell Washington, Independent Referencer



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix F**  
**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

**Other**

SolarWinds Corporation



## **Additional Information and Copies**

To view this and any of our other reports, please visit our website at:  
[www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General  
Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto: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](http://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