United States Government Accountability Office

Report to Congressional Committees

March 2024

CYBERSECURITY

Improvements Needed in Addressing Risks to Operational Technology

Accessible Version

GAO-24-106576

GAO Highlights

View GAO-24-106576. For more information, contact Marisol Cruz Cain (202) 512-5017 or CruzCainM@gao.gov.
Highlights of GAO-24-106576, a report to congressional committees
March 2024

CYBERSECURITY

Improvements Needed in Addressing Risks to Operational Technology

Why GAO Did This Study

Much of the nation's critical infrastructure relies on OT—systems that interact with the physical environment—to provide essential services. However, malicious cyber actors pose a significant threat to these systems. Federal law designates CISA as the lead agency in helping critical infrastructure owners and operators address cyber risks to OT.

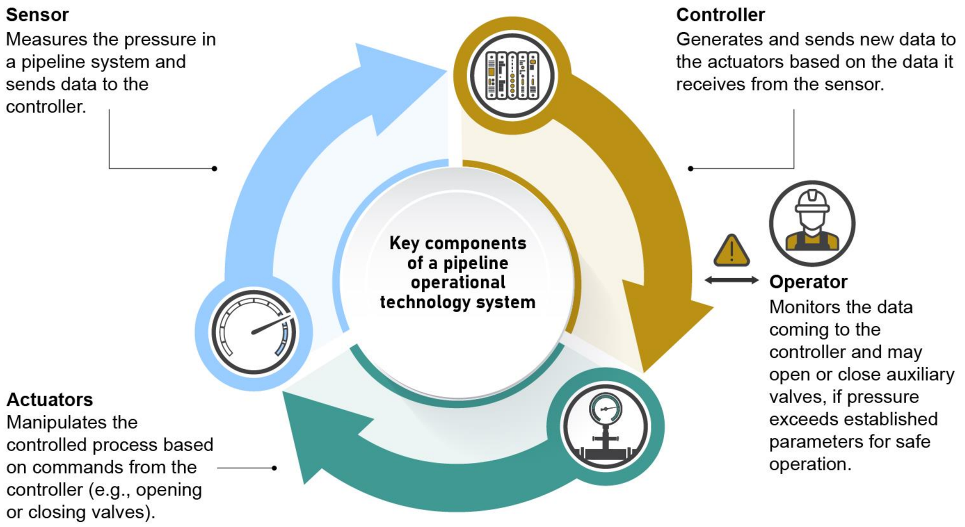
The National Defense Authorization Act of Fiscal Year 2022 includes a provision for GAO to report on CISA’s support for industrial control systems. Federal guidance now addresses these systems under the broader category of OT. Accordingly, this report examines, among other things: (1) challenges in delivering CISA’s OT products and services, and (2) challenges to collaborating between CISA and the seven selected agencies.

GAO reviewed documentation describing CISA’s 13 OT cybersecurity products and services. GAO also asked officials from CISA and 13 selected nonfederal entities to identify any challenges with the OT products and services. The selected entities included (1) councils representing one sector and three subsectors where OT was prevalent and the intelligence community highlighted their infrastructures as being at risk from cyber threat actors, (2) OT vendors who joined a CISA OT collaboration group, and (3) cybersecurity researchers that contributed to the development of CISA’s OT advisories. GAO then compared CISA’s efforts to address those challenges against leading practices regarding measuring customer service and workforce planning.

What GAO Found

Operational technology (OT) systems and devices are used to control, among other things, distribution processes (e.g., oil and natural gas pipelines) and production systems (e.g., electric power generation). Figure 1 shows the key components of an OT system using a pipeline system as an illustrative example.

Key Components of a Pipeline Operational Technology (OT) System



Sensor
Measures the pressure in a pipeline system and sends data to the controller.

Controller
Generates and sends new data to the actuators based on the data it receives from the sensor.

Operator
Monitors the data coming to the controller and may open or close auxiliary valves, if pressure exceeds established parameters for safe operation.

Actuators
Manipulates the controlled process based on commands from the controller (e.g., opening or closing valves).

Sources: GAO (analysis and icons); staratel/stock.adobe.com (icons); iconlauk/stock.adobe.com (icon). | GAO-24-106576

Accessible Text for Key Components of a Pipeline Operational Technology (OT) System

Key components of a pipeline operational technology system
• **Sensor:** Measures the pressure in a pipeline system and sends data to the controller. • **Controller:** Generates and sends new data to the actuators based on the data it receives from the sensor. • **Operator:** Monitors the data coming to the controller and may open or close auxiliary valves, if pressure exceeds established parameters for safe operation. • **Actuators:** Manipulates the controlled process based on commands from the controller (e.g., opening or closing valves).

Sources: GAO (analysis and icons); staratel/stock.adobe.com (icons); iconlauk/stock.adobe.com (icon). | GAO-24-106576

Although 12 of the 13 selected nonfederal entities cited examples of positive experiences with the Cybersecurity and Infrastructure Security Agency's (CISA) OT products and services, CISA and seven of the nonfederal entities identified two types of associated challenges. Specifically:

- Seven selected nonfederal entities identified **negative experiences using CISA's products and services** as a challenge. For example, one nonfederal entity told GAO that vulnerabilities reported through CISA's process often take more than a year between the initial report of a vulnerability and public disclosure (see figure 2).

- CISA officials and one nonfederal entity identified the **insufficient CISA staff with requisite OT skills** as a challenge. For example, CISA officials stated

that its four federal employees and five contractor staff on the threat hunting and incident response service are not enough staff to respond to significant attacks impacting OT systems in multiple locations at the same time.

To address these types of challenges, best practices highlight the importance of (1) measuring customer service and (2) performing effective workforce planning. However, CISA has not fully addressed these practices. Until CISA does so, the agency will not be optimally positioned to deliver products and services needed to address OT risks.

In addition, GAO reviewed documentation describing CISA's efforts to collaborate with seven selected agencies to mitigate cyber OT risks. The seven selected agencies are: (1) Department of Defense's (DOD) Defense Cyber Crime Center (DC3); (2) DOD's National Security Agency (NSA); (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER); (4) Department of Homeland Security's (DHS) Transportation Security Administration (TSA); (5) DHS's U.S. Coast Guard (USCG); (6) Department of Transportation's (DOT) Federal Railroad Administration (FRA); and (7) DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA). GAO focused on these agencies or departmental components because each was (1) within agencies designated as the lead for helping to protect the selected sector and three subsectors and (2) responsible for helping critical infrastructure owners and operators to mitigate cyber OT risks. GAO also asked officials from seven selected agencies to identify any challenges in collaborating with CISA to mitigate cyber OT risks. GAO then compared documentation from the seven agencies and CISA against five selected leading collaboration practices.

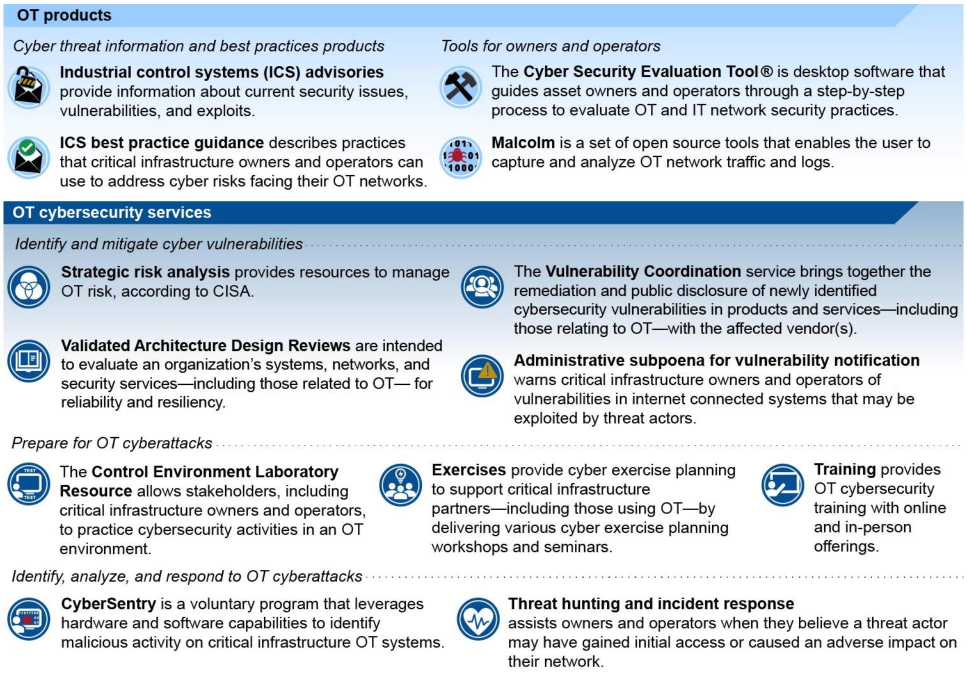
What GAO Recommends

GAO is making four recommendations to CISA to implement processes and guidance to improve its OT products and services and collaboration. Specifically, GAO is recommending that CISA

1. measure customer service for its OT products and services,
2. perform effective workforce planning for OT staff,
3. issue guidance to the sector risk management agencies on how to update their plans for coordinating on critical infrastructure issues, and
4. develop a policy on agreements with sector risk management agencies with respect to collaboration.

DHS concurred with the four recommendations to CISA and described actions that the agency plans to take to implement them.

Cybersecurity and Infrastructure Security Agency (CISA) Operational Technology (OT) Cybersecurity Products and Services



OT products

Cyber threat information and best practices products

Industrial control systems (ICS) advisories provide information about current security issues, vulnerabilities, and exploits.

ICS best practice guidance describes practices that critical infrastructure owners and operators can use to address cyber risks facing their OT networks.

Tools for owners and operators

The **Cyber Security Evaluation Tool®** is desktop software that guides asset owners and operators through a step-by-step process to evaluate OT and IT network security practices.

Malcolm is a set of open source tools that enables the user to capture and analyze OT network traffic and logs.

OT cybersecurity services

Identify and mitigate cyber vulnerabilities

Strategic risk analysis provides resources to manage OT risk, according to CISA.

Validated Architecture Design Reviews are intended to evaluate an organization's systems, networks, and security services—including those related to OT— for reliability and resiliency.

The **Vulnerability Coordination** service brings together the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services—including those relating to OT—with the affected vendor(s).

Administrative subpoena for vulnerability notification warns critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors.

Prepare for OT cyberattacks

The **Control Environment Laboratory Resource** allows stakeholders, including critical infrastructure owners and operators, to practice cybersecurity activities in an OT environment.

Exercises provide cyber exercise planning to support critical infrastructure partners—including those using OT—by delivering various cyber exercise planning workshops and seminars.

Training provides OT cybersecurity training with online and in-person offerings.

Identify, analyze, and respond to OT cyberattacks

CyberSentry is a voluntary program that leverages hardware and software capabilities to identify malicious activity on critical infrastructure OT systems.

Threat hunting and incident response assists owners and operators when they believe a threat actor may have gained initial access or caused an adverse impact on their network.

Source: CISA (documentation and icons). | GAO-24-106576

Accessible Text for Cybersecurity and Infrastructure Security Agency (CISA) Operational Technology (OT) Cybersecurity Products and Services

Category	Subcategory	Subcategory member
OT products	Cyber threat information and best practices products	Industrial control systems (ICS) advisories provide information about current security issues, vulnerabilities, and exploits.
OT products	Cyber threat information and best practices products	ICS best practice guidance describes practices that critical infrastructure owners and operators can use to address cyber risks facing their OT networks.
OT products	Tools for owners and operators	The Cyber Security Evaluation Tool® is desktop software that guides asset owners and operators through a step-by-step process to evaluate OT and IT network security practices.

Category	Subcategory	Subcategory member
OT products	Tools for owners and operators	Malcolm is a set of open source tools that enables the user to capture and analyze OT network traffic and logs.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Strategic risk analysis provides resources to manage OT risk, according to CISA.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Validated Architecture Design Reviews are intended to evaluate an organization's systems, networks, and security services—including those related to OT— for reliability and resiliency.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	The Vulnerability Coordination service brings together the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services—including those relating to OT—with the affected vendor(s).
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Administrative subpoena for vulnerability notification warns critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors.
OT cybersecurity services	Prepare for OT cyberattacks	The Control Environment Laboratory Resource allows stakeholders, including critical infrastructure owners and operators, to practice cybersecurity activities in an OT environment.
OT cybersecurity services	Prepare for OT cyberattacks	Exercises provide cyber exercise planning to support critical infrastructure partners—including those using OT—by delivering various cyber exercise planning workshops and seminars.
OT cybersecurity services	Prepare for OT cyberattacks	Training provides OT cybersecurity training with online and in-person offerings.

Category	Subcategory	Subcategory member
OT cybersecurity services	Identify, analyze, and respond to OT cyberattacks	CyberSentry is a voluntary program that leverages hardware and software capabilities to identify malicious activity on critical infrastructure OT systems.
OT cybersecurity services	Identify, analyze, and respond to OT cyberattacks	Threat hunting and incident response assists owners and operators when they believe a threat actor may have gained initial access or caused an adverse impact on their network.

Source: CISA (documentation and icons). | GAO-24-106576

Six of the seven selected agencies cited examples of where their collaboration with CISA yielded positive outcomes to addressing cyber OT risks. However, four agencies also identified two challenges in coordinating with CISA: (1) CISA ineffectively sharing information with critical infrastructure owners and operators, and (2) CISA and the Pipeline and Hazardous Materials Safety Administration lacking a process to share cyber threat information with owners and operators.

To address these types of challenges, it is important to adopt leading collaboration practices. However, CISA did not fully address any of five selected leading collaboration practices when coordinating with seven selected agencies (see table).

Extent to Which the Cybersecurity and Infrastructure Security Agency (CISA) Addressed Selected Leading Collaboration Practices with Seven Selected Agencies to Mitigate Cyber Operational Technology Risks to Critical Infrastructure

Collaboration practices	CESER	DC3	FRA	NSA	PHMSA	TSA	USCG
Define common outcomes	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Ensure accountability	not addressed	not addressed	partially addressed	not addressed	partially addressed	partially addressed	partially addressed
Bridge organizational cultures	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Clarify roles and responsibilities	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed

Collaboration practices	CESER	DC3	FRA	NSA	PHMSA	TSA	USCG
Develop and update written guidance and agreements	not addressed	partially addressed	not addressed	not addressed	not addressed	not addressed	partially addressed

Source: GAO analysis of agency information. | GAO-24-106576

Legend: ●=Generally addressed. ◑=Partially addressed. ○=Not addressed.

Note: CESER (Cybersecurity, Energy Security, and Emergency Response), DC3 (Department of Defense Cyber Crime Center), FRA (Federal Railroad Administration), NSA (National Security Agency), PHMSA (Pipeline and Hazardous Materials Safety Administration), TSA (Transportation Security Administration), and USCG (U.S. Coast Guard).

The practices were not fully addressed, in part, because of the lack of (1) guidance from CISA to the sector risk management agencies on how to update their plans for coordinating on critical infrastructure issues and (2) a CISA policy for developing agreements with sector risk management agencies with respect to collaboration. Until CISA takes action to address these weaknesses, it and the selected agencies will not be well-positioned to coordinate on mitigating cyber OT risks.

Contents

Tables

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CESER	Cybersecurity, Energy Security, and Emergency Response
CSET	Cyber Security Evaluation Tool®
FRA	Federal Railroad Administration
DC3	DOD Cyber Crime Center
DOE	Department of Energy
DOD	Department of Defense
DHS	Department of Homeland Security
DOT	Department of Transportation
NIST	National Institute of Standards and Technology

NSA	National Security Agency
OT	operational technology
PHMSA	Pipeline and Hazardous Materials Safety Administration
PPD-21	Presidential Policy Directive-21
PPD-41	Presidential Policy Directive-41
SRMA	Sector Risk Management Agency
TSA	Transportation Security Administration
USCG	U.S. Coast Guard

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

March 7, 2024

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The nation's 16 critical infrastructure sectors provide the essential services (e.g., transportation and oil and gas distribution) that underpin American society.[1] Many of these sectors rely on operational technology (OT)—programmable systems and devices that interact with the physical environment—to support their missions.

OT used by critical infrastructure owners and operators faces significant and increasing cybersecurity risks. In particular, threat actors (e.g., nation states and transnational criminal organizations) are becoming increasingly capable of carrying out attacks on critical infrastructure, including OT.

At the same time, OT systems are becoming more vulnerable to attacks in light of their increasing interconnections with IT systems. Such

[1] The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater systems. In addition, several sectors have subsectors (e.g., the Education Facilities and Elections Infrastructure subsectors within the Government Facilities subsector).

vulnerabilities could be exploited by threat actors and result in serious harm to human safety, the environment, and the economy. To illustrate, cyberattacks on OT systems used to operate foreign electric grid systems have resulted in localized power outages, such as an October 2022 cyberattack in Ukraine.[2] In addition, in November 2023 a cyber threat actor gained access to OT equipment used to monitor and regulate water pressure for two townships in Pennsylvania.[3]

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and other OT stakeholders are positioned to play a critical role in helping to address cyber OT risks to critical infrastructure. For example:

- As the national coordinator for infrastructure protection, CISA's key responsibilities include responding to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance, as well as coordinating with federal and nonfederal entities on OT security. Further, in December 2021, Congress and the President enacted legislation that defined CISA's leadership role more explicitly in addressing cyber risks to OT systems.[4]
- A Sector Risk Management Agency (SRMA) is a federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise for a particular sector. A SRMA is also responsible for leading, facilitating, or supporting security and resilience programs and associated activities within their designated critical infrastructure

[2] Mandiant, *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, accessed Nov. 29, 2023, https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology/.

[3] Water Information Sharing and Analysis Center (ISAC), *(TLP:CLEAR) Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (Updated November 30, 2023)* (Nov. 30, 2023); *CISA, Alert: Exploitation of Unitronics PLCs used in Water and Wastewater Systems* (Nov. 28, 2023).

[4] National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 1541, 135 Stat. 1541, 2054 (Dec. 27, 2021).

sectors, such as helping to address cyber risks to OT systems supporting these sectors.[5]

- Private sector stakeholders own and operate the majority of critical infrastructure (e.g., electricity grid). Therefore, it is vital that the public and private sectors work together to protect assets and systems, including OT systems.

The National Defense Authorization Act of Fiscal Year 2022 includes a provision for us to review CISA's efforts to mitigate cyber threats to industrial control systems—a subset of OT.[6] This report examines (1) CISA's OT cybersecurity products and services and challenges in delivering them, and (2) how CISA and selected federal agencies work together to mitigate cyber OT risks and the collaboration challenges they face. For each area, we also evaluated CISA's efforts to address any challenges.

To address our first objective, we reviewed CISA's 13 OT cybersecurity products and services that were offered to critical infrastructure owners and operators between October 2018 and October 2023. To identify these products and services, we reviewed CISA's *Industrial Control Systems Security Offerings*,[7] which lists 17 OT cybersecurity products

[5] See 6 U.S.C. § 650(23). In 2013, Presidential Policy Directive-21 (PPD-21) named these federal entities sector-specific agencies. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified sector-specific agencies as SRMAs. PPD-21 categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as a SRMA for the sector, although the number of sectors and SRMA assignments are subject to review and modification. Those initial sector designations are still in effect. Additionally, some sectors have subsectors, such as the Education subsector within the Government Facilities sector, with the Department of Education having a lead risk management role for the subsector.

[6] Pub. L. No. 117-81, § 1541(c), 135 Stat. at 2055. Due to NIST's expansion of its guidance on industrial control systems security to include OT security, we addressed the statutory mandate by focusing on OT. Specifically, NIST replaced the former guidance issued in 2015, *Guide to Industrial Control Systems (ICS) Security,* SP 800-82, Rev. 2 (Gaithersburg, MD.: May 2015), with the current guidance issued in September, *Guide to Operational Technology (OT) Security*, NIST SP-800-82, Rev. 3 (Gaithersburg, MD.: September 2023).

[7] CISA's website describes this document as containing the "full catalog" of CISA's OT cybersecurity products and services. See https://www.cisa.gov/topics/industrial-control-systems. In September 2023, the National Institute of Standards and Technology (NIST) expanded the scope of its guidance on industrial control systems security to include OT security and changed how it characterizes industrial control systems with the third revision to NIST SP-800-82. NIST, *Guide to Operational Technology Security*, NIST Special Publication 800-82, Rev. 3 (Gaithersburg, MD.: September 2023). For our report, we generally use the term "operational technology" in place of "industrial control systems" to align our report language with shifts to industry practices.

and services. We then removed one product that does not help critical infrastructure owners and operators to address cyber OT risks, and one product and two services that CISA had retired.

After identifying these products and services, we asked (1) CISA officials responsible for them and (2) officials from 13 selected nonfederal entities that use CISA's OT cybersecurity products and services to describe any challenges with the products and services. We selected these nonfederal entities from sector coordinating councils, OT vendors, and cybersecurity researchers.[8] We then conducted a content analysis on the responses from CISA and the selected nonfederal entities to identify any frequently reported challenges. We totaled the number of times each challenge was identified and chose to report on the types of challenges that were identified by three or more entities.

In addition, we conducted interviews with or obtained written responses from CISA to identify efforts it has taken to address these challenges. We then compared CISA's efforts to address the challenges against leading practices in customer service[9] and workforce planning.[10]

To address our second objective, we described how CISA and seven selected federal agencies work together to mitigate cyber OT risks and the extent to which they addressed selected leading interagency collaboration practices. We selected the federal agencies that are tasked with helping critical infrastructure owners and operators address cyber OT

[8] More specifically, we interviewed or obtained written responses from: (1) three sector coordinating councils representing select critical infrastructure sectors and subsectors: specifically, the Defense Industrial Base, the Freight Rail, the Oil and Natural Gas, and Pipeline sector coordinating councils; (2) seven OT vendors who joined CISA's Joint Cyber Defense Collaborative in April 2022 when CISA expanded this group to focus on OT cyber issues; and (3) four cybersecurity researchers that contributed to the development of CISA's OT-related alerts and advisories. Of note, one of the selected research organizations was also a selected OT vendor.

[9] GAO, *Taxpayer Service: IRS Could Improve the Taxpayer Experience by Using Better Service Performance Measures*, GAO-20-656 (Washington, D.C.: Sept. 23, 2020).

[10] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

risks to certain sectors and subsectors at risk from malicious cyber actors.[11]

In particular, we reviewed documentation and interviewed officials from CISA and seven selected federal agencies to determine what mechanisms, if any, CISA used to collaborate with each of the agencies to mitigate cyber OT risks. We also asked the seven agencies to identify any challenges they experienced when collaborating with CISA to mitigate cyber OT risks. Using this information, we conducted a content analysis to identify challenges frequently reported by the selected federal agencies. We then totaled the number of times each challenge was identified and chose to report on all challenges.

We then compared CISA's efforts to address the challenges against the selected leading practices for enhancing interagency collaboration when collaborating with the seven selected agencies to mitigate cyber OT risks. In particular, we gathered and reviewed documentation describing CISA's and the agencies' collaborative efforts to mitigate cyber OT risks. We then evaluated these collaborative efforts against the selected interagency collaboration practices[12] to determine the extent to which CISA and the agencies addressed these practices. See appendix I for more details on or objectives, scope, and methodology.

[11] To select the federal agencies, we first selected the Defense Industrial Base, Energy, and Transportation Systems sectors. Within the Energy and Transportation Systems sectors, we selected the Oil and Natural Gas, Freight Rail, and Pipeline subsectors. We selected these sector and subsectors because (1) OT is prevalent in the sector and subsectors and (2) the 2023 *Annual Threat Assessment of the U.S. Intelligence Community* highlighted their infrastructures as at risk from malicious cyber actors. We then focused on seven agencies within designated sector risk management agencies who are tasked with responsibilities for helping critical infrastructure owners and operators to address cyber OT risks to the selected sector and subsector. Specifically, we selected: (1) Department of Defense's (DOD) Defense Cyber Crime Center (DC3); (2) DOD's National Security Agency (NSA); (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response; (4) Department of Homeland Security's (DHS) Transportation Security Administration; (5) DHS's U.S. Coast Guard; (6) Department of Transportation's (DOT) Federal Railroad Administration; and (7) DOT's Pipeline and Hazardous Materials Safety Administration.

[12] GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges U.S. GAO,* GAO-23-105520 (Washington, D.C.: May 24, 2023). To do this, we selected five of the eight identified leading practices that are most relevant for CISA's coordination with other SRMAs: (1) defining common outcomes, (2) ensuring accountability, (3) bridging organizational cultures, (4) clarifying roles and responsibilities, and (5) developing and updating written guidance and agreements.

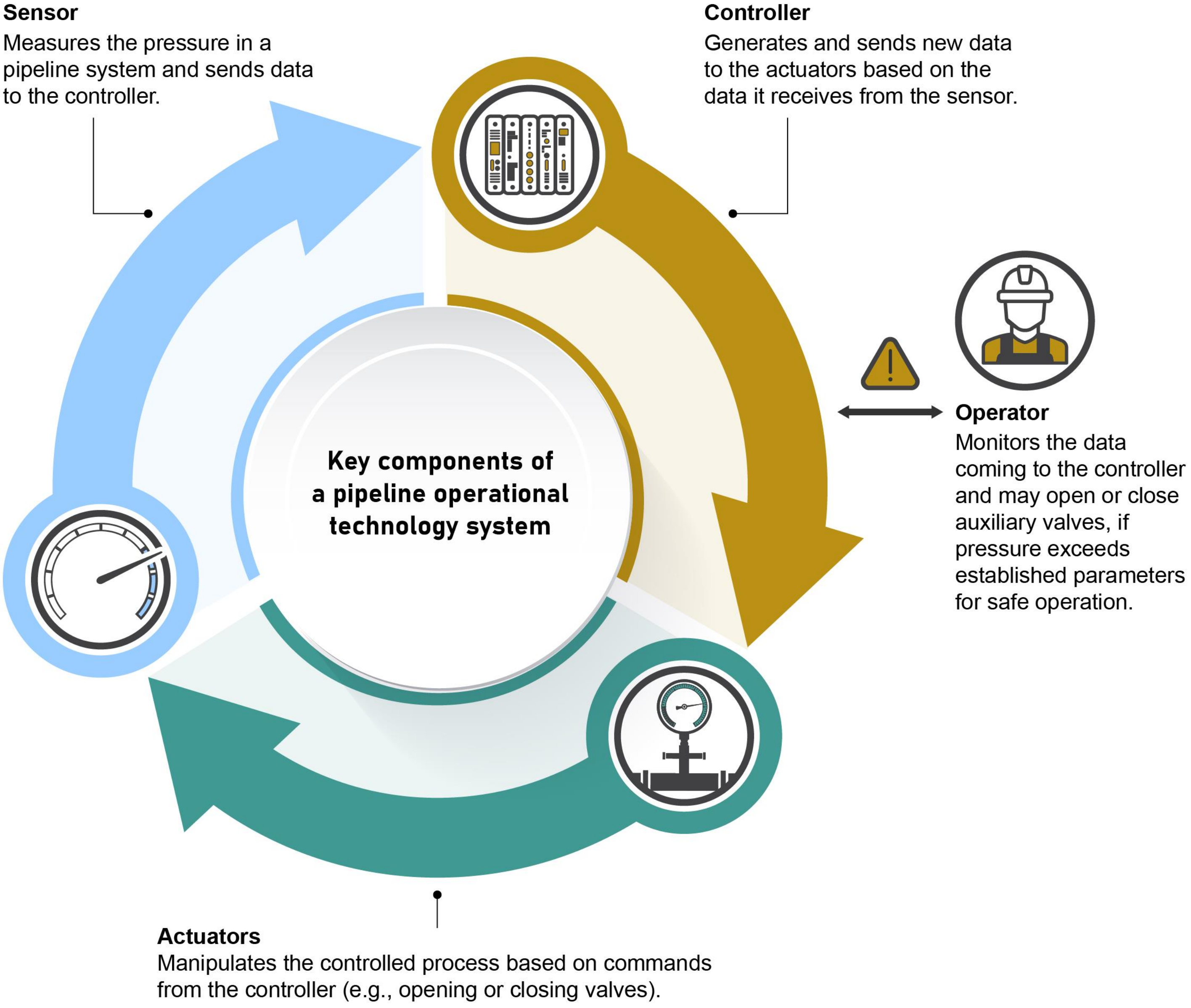
We conducted this performance audit from January 2023 to March 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The National Institute of Standards and Technology (NIST) describes OT as a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment).[13] These systems and devices detect or cause a direct change through monitoring and/or control of devices, processes, and events. Figure 1 shows the key components of an OT system using a pipeline system as an illustrative example.

[13] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, Special Publication 800-82, Rev. 3 (Gaithersburg, MD: September 2023).

Figure 1: Key Components of a Pipeline Operational Technology (OT) System



Sensor
Measures the pressure in a pipeline system and sends data to the controller.

Controller
Generates and sends new data to the actuators based on the data it receives from the sensor.

Operator
Monitors the data coming to the controller and may open or close auxiliary valves, if pressure exceeds established parameters for safe operation.

Actuators
Manipulates the controlled process based on commands from the controller (e.g., opening or closing valves).

Sources: GAO (analysis and icons); staratel/stock.adobe.com (icons); iconlauk/stock.adobe.com (icon). | GAO-24-106576

Accessible Text for Figure 1: Key Components of a Pipeline Operational Technology (OT) System

Key components of a pipeline operational technology system
• **Sensor:** Measures the pressure in a pipeline system and sends data to the controller. • **Controller:** Generates and sends new data to the actuators based on the data it receives from the sensor. • **Operator:** Monitors the data coming to the controller and may open or close auxiliary valves, if pressure exceeds established parameters for safe operation. • **Actuators:** Manipulates the controlled process based on commands from the controller (e.g., opening or closing valves).

Sources: GAO (analysis and icons); staratel/stock.adobe.com (icons); iconlauk/stock.adobe.com (icon). | GAO-24-106576

According to NIST, examples of OT include supervisory control and data acquisition systems, distributed control systems, and building automation systems.

- Supervisory control and data acquisition systems are used to control dispersed assets where centralized data acquisition is as important as control. These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.
- Distributed control systems are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation, chemical manufacturing, automotive production, and pharmaceutical processing.
- Building automation systems are a type of OT used to control many systems used in a building, including heating, ventilation, and air conditioning; fire; electrical; lighting; physical access control; physical security; and other utility systems.

Because there are many types of OT systems and devices and they are often unique to a particular process or environment, staff responsible for managing and securing OT often require specialized knowledge, skills, and abilities. Relatedly, staff with IT knowledge and expertise often lack knowledge and experience with OT. The President’s National Security Telecommunications Advisory Committee explained that IT cybersecurity professionals are educated and trained to deal with data confidentiality, integrity, and availability of systems that focus on user interaction within an environment.[14] By contrast, the advisory committee noted that OT professionals focus on physical processes' availability, safety, and reliability in systems that use machine-to-machine communications within the environment. As a result, the advisory committee concluded these IT and OT professionals possess vastly different skills and functions and historically had little interaction.

Cyber OT Risks

We have previously reported that OT supporting the nation's critical infrastructure sectors and subsectors face significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts.[15]

- **Threat actors.** According to the 2023 *Annual Threat Assessment of the U.S. Intelligence Community*, China, Iran, North Korea, and Russia possess the ability to launch cyberattacks that could have disruptive effects on critical infrastructure.[16] Further, the assessment stated that transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause disruptions of critical services worldwide. In addition, we have previously reported that hackers and hacktivists, as well as insiders, pose significant cyber threats to OT used by critical infrastructure owners and operators.[17]
- **Vulnerabilities.** OT used by critical infrastructure owners and operators is becoming increasingly vulnerable to cyberattacks. Most notably, OT systems were once largely isolated from internet and business IT systems. However, OT systems are more vulnerable now that they are more frequently connected with business IT systems both within a company and accessible by internet systems globally.

[14] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President: Information Technology and Operational Technology Convergence* (Aug. 23, 2022).

[15] See, for example, GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure,* GAO-23-105789 (Washington, D.C.: Oct. 26, 2022).

[16] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (February 2023).

[17] See, e.g., GAO-23-105789, GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks,* GAO-22-104256 (Washington, D.C.: June 21, 2022); and *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021).

Further, older legacy OT systems were not designed with cybersecurity protections because they were not intended to connect to networks such as the internet.[18] As a result, cyberattacks are more likely to originate in business IT systems and migrate to OT.[19]

In addition, we have reported that OT system components often must be taken offline so that critical infrastructure owners and operators can apply security patches to address known cybersecurity vulnerabilities.[20] However, this may not happen in a timely manner for certain sectors (such as the Energy sector) because the devices must remain highly available to support critical functions (reliable operation of the grid).

- **Impacts.** Successful cyberattacks against critical infrastructure OT could have a range of consequences. These consequences may include the disruption of critical operations and loss of productivity, revenue, or safety. As a result, these cybersecurity incidents can threaten national security, economic well-being, and public health and safety. Table 1 describes five publicly reported examples of impacts from cyberattacks on OT in multiple critical infrastructure sectors.

Table 1: Potential Impacts of Cyberattacks on Critical Infrastructure Operational Technology (OT)

Impact	Description[a]	Example
Damage to property	Malicious actors may damage or destroy infrastructure, equipment, and the surrounding environment when attacking control systems. This may result in device and operational equipment breakdown or represent tangential damage from other techniques used in an attack.	In 2014, a cyberattack resulted in the improper operation of an OT system, including the improper shutdown of a furnace and physical damage to a German steel mill's facilities.[b]
Loss of productivity and revenue	Attackers may cause loss of productivity and revenue by damaging or disrupting the availability or integrity of industrial control systems operations, devices, and related processes.	In 2019, a form of ransomware named EKANS infected various OT devices, reportedly in the U.S., Europe, and Japan, by encrypting files and displaying a ransom note, which impaired operations.[c]

[18] For example, many legacy devices are not able to authenticate commands to ensure that they have been sent from a valid user and may not be capable of running modern encryption protocols. In addition, some legacy devices do not have the capability to log commands sent to the devices, making it more difficult to detect malicious activity. Further, older legacy systems often rely on unsupported operating systems that no longer receive modern software security patches to address vulnerabilities.

[19] GAO-23-105789.

[20] GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure,* GAO-23-105789 (Washington, D.C.: Oct. 26, 2022).

Impact	Description[a]	Example
Loss of safety	Attackers may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.	In 2017, Russian cyber actors manipulated a foreign oil refinery's safety devices, which resulted in the refinery shutting down for several days.[d]
Loss or denial of control	Malicious actors may seek to prevent operators and engineers from interacting with process controls.	In 2015, Russian attackers uploaded malicious software to certain devices in Ukraine, with the intent of ensuring that utility operators could not issue remote commands to bring electricity substations back online.[e]
Manipulation of control	Command messages may be used in OT networks to give direct instructions to devices. Attackers may send unauthorized command messages to instruct industrial control systems devices to perform actions outside their desired functionality for process control.	In the 2015 attacks on Ukraine, Russian attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers.[e]

Sources: Prior GAO work, and MITRE. | GAO-24-106576

[a] These tactics that affect OT are not mutually exclusive. Some tactics may be used in conjunction with one another.

[b] SANS Industrial Control Systems, ICS CP/PE (Cyber-to-Physical or Process Effects) (case study paper): German Steel Mill Cyber Attack (Rockville, MD: Dec. 30, 2014).

[c] Dragos, EKANS Ransomware and ICS Operations, accessed Sept. 16, 2023, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[d] Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Energy, Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector, Alert (AA22-083A) (Mar. 24, 2022).

[e] Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid (Washington, D.C.: Mar. 18, 2016).

Due to the cyber-based threats to federal and critical infrastructure systems (including OT systems), we first designated federal information security as a government-wide high-risk area in our biennial report to Congress in 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information. We continue to highlight the importance of protecting critical cyber infrastructure, as shown in our recent work highlighting risks to OT,[21] and the April 2023 high-risk update on major cybersecurity challenges.[22]

[21] See, e. g., GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure,* GAO-23-105789 (Washington, D.C.: Oct. 26, 2022); *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, GAO-23-105327 (Washington, D.C.: Dec. 1, 2022); and *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021).

[22] GAO*, High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

Critical Infrastructure Protection Policies and Guidance

Three of the most widely recognized policy and guidance documents regarding critical infrastructure protection are Presidential Policy Directive-21 (PPD-21),[23] the 2013 *National Infrastructure Protection Plan* (National Plan),[24] and Presidential Policy Directive-41 (PPD-41).[25]

- **PPD-21** shifted the focus from protecting critical infrastructure against terrorism toward protecting and securing critical infrastructure and increasing its resilience against all hazards, including cyber incidents. It identified 16 critical infrastructure sectors, designated specific federal agencies as sector-specific agencies—now referred to as SRMAs—and specified their roles and responsibilities.[26] Further, it required DHS to update the *National Infrastructure Protection Plan* to articulate how this policy directive is to be implemented. While OT can be found in all critical infrastructure sectors, it is most prevalent in 13 of the nation's 16 critical infrastructure sectors, as shown in figure 2.

[23] The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[24] DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

[25] The White House, *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination* (Washington, D.C.: Feb. 12, 2013).

[26] Each of the 16 sectors have at least one federal agency designated as lead for the sector based on authorities and capabilities specific to that sector. Some sectors have co-lead agencies where more than one agency shares SRMA responsibilities. DHS is unique among the other SRMAs in that it has lead responsibility for eight of the 16 sectors and co-leads two other sectors.

Figure 2: Critical Infrastructure Sectors and Related Sector Risk Management Agencies

🟩 **Chemical** — DHS
Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The sector produces essential products for a range of necessities, including automobiles, pharmaceuticals, food supply, water treatment, and health.

🟩 **Commercial facilities** — DHS
Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.

🟦 **Communications** — DHS
Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.

🟩 **Critical manufacturing** — DHS
Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.

🟩 **Dams** — DHS
Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.

🟩 **Defense industrial base** — DOD
Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.

🟩 **Emergency services** — DHS
Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.

🟩 **Energy** — DOE
Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.

🟦 **Financial services** — TREASURY
Provides the financial infrastructure of the nation. This sector consists of institutions like commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.

🟩 **Food and agriculture** — USDA, HHS
Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.

🟩 **Government facilities** — DHS, GSA
Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

🟩 **Healthcare and public health** — HHS
Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.

🟦 **Information technology** — DHS
Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.

🟩 **Nuclear reactors, materials, and waste** — DHS
Provides nuclear power and materials used in a range of settings. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.

🟩 **Transportation systems** — DHS, DOT
Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.

🟩 **Water and wastewater systems** — EPA
Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.

🟩 Reflects the sectors where operational technology is most prevalent.

🟦 Reflects the sectors where operational technology is less prevalent.

USDA (Department of Agriculture), **DOD** (Department of Defense), **DOE** (Department of Energy), **HHS** (Department of Health and Human Services), **DHS** (Department of Homeland Security), **DOT** (Department of Transportation), **Treasury** (Department of the Treasury), **EPA** (Environmental Protection Agency), **GSA** (General Services Administration).

Sources: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013, and summary of the National Institute of Standards and Technology's SP 800-82 Rev. 3; motorama/stock.adobe.com (icons). | GAO-24-106576

Accessible Text for Figure 2: Critical Infrastructure Sectors and Related Sector Risk Management Agencies

Category	Category member
Reflects the sectors where operational technology is most prevalent	Chemical: Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The sector produces essential products for a range of necessities, including automobiles, pharmaceuticals, food supply, water treatment, and health.
Reflects the sectors where operational technology is most prevalent	Commercial facilities: Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
Reflects the sectors where operational technology is less prevalent	Communications: Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.
Reflects the sectors where operational technology is most prevalent	Critical manufacturing: Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.
Reflects the sectors where operational technology is most prevalent	Dams: Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
Reflects the sectors where operational technology is most prevalent	Defense industrial base: Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Reflects the sectors where operational technology is most prevalent	Emergency services: Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.
Reflects the sectors where operational technology is most prevalent	Energy: Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.

Category	Category member
Reflects the sectors where operational technology is less prevalent	Financial services: Provides the financial infrastructure of the nation. This sector consists of institutions like commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.
Reflects the sectors where operational technology is most prevalent	Food and agriculture: Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.
Reflects the sectors where operational technology is most prevalent	Government facilities: Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.
Reflects the sectors where operational technology is most prevalent	Healthcare and public health: Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.
Reflects the sectors where operational technology is less prevalent	Information technology: Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
Reflects the sectors where operational technology is most prevalent	Nuclear reactors, materials, and waste: Provides nuclear power and materials used in a range of settings. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.
Reflects the sectors where operational technology is most prevalent	Transportation systems: Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Reflects the sectors where operational technology is most prevalent	Water and wastewater systems: Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.

Sources: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013, and summary of the National Institute of Standards and Technology's SP 800-82 Rev. 3; motorama/stock.adobe.com (icons). | GAO-24-106576

- **The National Plan.** Consistent with PPD-21, DHS updated this plan in 2013 to provide the overarching approach for integrating the nation’s critical infrastructure protection and resilience activities. The

National Plan details federal roles and responsibilities in protecting the nation's critical infrastructures and how sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. It also emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments. In addition, the National Plan called for SRMAs to develop plans that identified actions needed to address sector-specific risks and challenges, known as sector-specific plans.[27] Most SRMAs completed their respective plans for their sectors by 2015.[28]

- **PPD-41** sets forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities,[29] to achieve unity of effort and coordination.[30] PPD-41 is intended to provide a framework or guiding principles for supporting policies, procedures, and mechanisms established by relevant federal agencies. Further, an annex to PPD-41 provided further details concerning the federal government's coordination on cyber incidents deemed to be significant and prescribed additional

[27] Of note, at the time the National Plan was updated, SRMAs were referred to as sector-specific agencies. Since then, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified sector-specific agencies as SRMAs, stating that the term "sector risk management agency" holds the meaning previously given to the term "sector-specific agency". 6 U.S.C. § 652a.

[28] We have previously reported on the need for sector specific plans to be updated. For example, in November 2021, we recommended that CISA update its Communications Sector-Specific Plan to, among other things, address new and emerging threats and risks to the Communications Sector. GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of Its Actions to Support the Communications Sector*, GAO-22-104462 (Washington, D.C.: Nov. 23, 2021).

[29] The Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted on March 15, 2022, Division Y of the Consolidated Appropriations Act, 2022, requires "covered entities" across critical infrastructure sectors to report "covered incidents" to CISA within 72 hours of reasonably determining a "covered incident" occurred. CISA has 24 months from the date the law enacted to publish a notice of proposed rulemaking to implement this requirement, and an additional 18 months after the notice to issue a final rule. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y, § 103(a)(2), 136 Stat. 49, 1043-44 (March 15, 2022) codified at 6 U.S.C. § 681b.

[30] A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

principles for agencies to implement.[31] Among other things, the directive called for federal agencies to respond to cyber incidents by implementing coordination principles that are applicable to federal agencies when mitigating cyber OT risks. These principles include implementing the roles of designated lead federal agencies for asset response[32] and threat response[33] activities, and agency coordination to provide unity of effort on threat response and asset response activities.

Sector Risk Management Agencies

SRMAs are federal departments or agencies, designated by law or presidential directive, with specific responsibilities for their designated critical infrastructure sectors.[34] In coordination with CISA, SRMAs are to provide specialized expertise to critical infrastructure owners within the relevant sector and provide support to sector programs and activities. In carrying out these responsibilities, SRMAs are to coordinate with DHS and, as appropriate, other federal agencies; critical infrastructure owners and operators within their sectors; and state, local, tribal, and territorial partners.

SRMA responsibilities include working with CISA in prioritizing and performing vulnerability and risk assessments, coordinating intelligence, information, and data sharing activities, and conducting incident response and preparedness activities. The departments and agencies designated

[31] A significant cyber incident is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[32] Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources.

[33] Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity’s site, collecting evidence, and gathering intelligence.

[34] 6 U.S.C. § 650(23). Although sector-specific plans identify specific departments, agencies, or components within departments or agencies as having lead or co-lead responsibilities for carrying out critical infrastructure protection activities, other offices within the SRMA departments and agencies also support sector critical infrastructure protection efforts.

as SRMAs often task component agencies or offices to carry out their responsibilities.

As previously mentioned, we selected the one sector (Defense Industrial Base) and three subsectors (Freight Rail, Oil and Natural Gas, and Pipeline subsectors).[35] The four SRMAs responsible for the sector and subsectors have tasked seven component agencies with carrying out SRMA responsibilities for OT (see table 2).

Table 2: The Selected Sector and Subsectors, Sector Risk Management Agencies (SRMA), and Component Agencies Tasked with SRMA Responsibilities for Operational Technology (OT)

Selected sector/subsector	SRMA(s)	Component agencies tasked with SRMA responsibilities for OT
Defense Industrial Base sector	Department of Defense (DOD)	• The National Security Agency's (NSA) Cybersecurity Collaboration Center aims to prevent and eradicate threats to U.S. national security systems with a focus on the Defense Industrial Base and the improvement of U.S. weapons security. In particular, the NSA's Cybersecurity Collaboration Center provides services to members of the sector aimed at improving network defenses, providing cyber threat intelligence, and providing guidance to mitigating cyber vulnerabilities. • The DOD Cyber Crime Center (DC3) serves as the operational focal point for DOD's Defense Industrial Base Cybersecurity Program. In particular, DC3 operates the DOD Defense Industrial Base Collaborative Information Sharing Environment, which aims to protect intellectual property and safeguard DOD content residing on, or transiting through, contractor unclassified IT and OT networks.
Freight Rail subsector	Departments of Homeland Security (DHS) and Transportation (DOT)	• DHS's Transportation Security Administration (TSA) works with industry leaders and other government partners to reduce threats to the freight rail network by producing security actions, procedures, and informational materials for the rail industry. In October 2022, TSA issued a new security directive with cybersecurity requirements for regulating designated freight and passenger railroad carriers. TSA renewed this directive in October 2023. • Within DOT, Federal Railroad Administration's (FRA) mission is to enable the safe, reliable, and efficient movement of people and goods for a strong America, now and in the future. To carry this out, FRA regulates the safety of the nation's railroad system and development of intercity passenger rail, to include the cybersecurity standards for electronic display systems used for worker safety.
Oil and Natural Gas subsector	Department of Energy	• The Office of Cybersecurity, Energy Security, and Emergency Response's (CESER) mission is to strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions. To carry this out, CESER advances research, development, and deployment of technologies, tools, and techniques to reduce risks to the nation's critical energy infrastructure posed by cyber and other emerging threats.

[35] We selected this sector and subsectors because (1) OT is prevalent in this sector and subsector and (2) the *2023 Annual Threat Assessment of the U.S. Intelligence Community* highlighted their infrastructures as at risk from malicious cyber actors. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (February 2023).

Selected sector/subsector	SRMA(s)	Component agencies tasked with SRMA responsibilities for OT
Pipeline subsector	DOT and DHS	• Within DHS, TSA is responsible for the security of the nation's hazardous liquid and natural gas pipeline systems. Starting in May 2021, TSA issued a security directive with cybersecurity requirements for certain pipeline owners and operators. In July 2022, TSA issued another security directive with performance-based requirements. TSA renewed this directive in July 2023. • Within DHS, the U.S. Coast Guard (USCG) has broad legal authorities, including oversight of the outer continental shelf associated with maritime transportation, hazardous materials shipping, oil spill response, pilotage, and vessel construction and operation. With respect to offshore pipelines, USCG is responsible for taking action to control, contain, and clean up oil discharges. • Within DOT, the Pipeline and Hazardous Materials Safety Administration's (PHMSA) mission is to protect people and the environment by advancing the safe transportation of energy and other hazardous materials. To do this, PHMSA develops and enforces regulations for the safe, reliable, and environmentally sound operation of the nation's 3.3 million mile pipeline transportation system (among other areas for which PHMSA regulates).

Source: GAO analysis of agency documentation. | GAO-24-106576

CISA's Role as National Coordinator and Lead for OT Cybersecurity

Since CISA's creation in 2018, the White House has designated it to be the lead for cyber and physical infrastructure security within DHS.[36] CISA is responsible for ensuring a unified approach to risk management that addresses the full spectrum of risks to critical infrastructure. The Cybersecurity and Infrastructure Security Agency Act of 2018 assigned CISA specific responsibilities to focus on related to cybersecurity and critical infrastructure protection efforts, including:[37]

- coordinating a national effort to secure and protect against critical infrastructure risks;
- providing analyses, expertise, and other technical assistance upon request to critical infrastructure owners and operators and, when appropriate, coordinating with SRMAs and other federal departments to do so;

[36] White House, *National Cybersecurity Strategy* (March 1, 2023). Prior to CISA's statutory creation in November 2018, PPD-21 directed DHS to operate two national critical infrastructure centers—i.e., one for physical infrastructure and another for cyber infrastructure.

[37] 6 U.S.C. § 652(c).

- developing and using mechanisms for active and frequent collaboration between the agency and SRMAs; and
- providing education, training, and capacity development to federal and nonfederal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security.

In December 2021, Congress recognized the need to define CISA's leadership role more explicitly in addressing cyber risks to OT systems. Specifically, provisions in the National Defense Authorization Act for Fiscal Year 2022 made CISA responsible for[38]

- maintaining capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes;
- leading federal efforts, in consultation with SRMAs, as appropriate, to identify and mitigate cybersecurity threats to OT systems;
- maintaining threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;
- providing cybersecurity technical assistance to industry end users, product manufacturers, SRMAs, other federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities; and
- collecting, coordinating, and providing vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end users, product manufacturers, SRMAs, other federal agencies, and other industrial control systems.

CISA Delivered OT Cybersecurity Products and Services, but Has Not Fully Addressed Challenges

CISA provided 13 OT cybersecurity products and services to critical infrastructure owners and operators. However, CISA and seven of the 13 selected nonfederal entities identified two types of challenges associated with the delivery of OT products and services. These challenges are related to: (1) negative experiences using CISA's products and services,

[38] 6 U.S.C. § 659(q).

and (2) insufficient CISA staff with the requisite OT skills. To address these types of challenges, best practices recommend (1) measuring customer service and (2) performing effective workforce planning. However, CISA has not fully (1) measured customer service for its OT products and services or (2) performed effective workforce planning for its OT workforce.

CISA Provided OT Cybersecurity Products and Services to Owners and Operators

CISA provided 13 OT cybersecurity products and services between October 2018 and November 2023 at no cost to critical infrastructure owners and operators. (CISA retired three other products and services during this period. See appendix III for more details on these retired products and services.) More specifically:

- **OT cybersecurity products.** CISA provided four OT cybersecurity products to critical infrastructure owners and operators. Two of these products were aimed at sharing cyber threat information and best practices pertaining to OT. The remaining two OT products were tools that owners and operators can use to evaluate their OT security practices and analyze their OT network traffic and logs.
- **OT cybersecurity services.** CISA provided nine OT cybersecurity services to critical infrastructure owners and operators. Specifically, of the nine services:
  - Four services were focused on helping owners and operators to identify cyber vulnerabilities in their OT networks and steps that can be taken to mitigate them.
  - Three services were aimed at providing critical infrastructure owners and operators with training, exercises, and other information needed to prepare for cyberattacks on their OT networks.
  - Two services were focused on helping to identify, analyze, or respond to malicious cyber activity on owner and operator OT networks.

In addition, to help enhance these products and services, in April 2022 CISA established the Industrial Control Systems working group as part of its Joint Cyber Defense Collaborative.[39] CISA explained that the working group is intended to help plan for how best to protect the nation's OT, inform the government's guidance on OT cybersecurity, and contribute to information sharing across private and public partners in the OT space. (See appendix IV for a detailed summary of this group.)

Figure 3 describes CISA's four OT cybersecurity products and nine services. (See appendix V for additional details on the four OT cybersecurity products and appendix VI for additional details on the nine cybersecurity services.)

[39] In August 2021, CISA founded the Joint Cyber Defense Collaborative as a public-private sector partnership, including many industry partners from multiple critical infrastructure sectors. The organization is intended to drive cybersecurity collaboration across sectors.

Figure 3: The Cybersecurity and Infrastructure Security Agency's (CISA) 13 Operational Technology (OT) Cybersecurity Products and Services

OT products

Cyber threat information and best practices products

Industrial control systems (ICS) advisories provide information about current security issues, vulnerabilities, and exploits.

ICS best practice guidance describes practices that critical infrastructure owners and operators can use to address cyber risks facing their OT networks.

Tools for owners and operators

The **Cyber Security Evaluation Tool®** is desktop software that guides asset owners and operators through a step-by-step process to evaluate OT and IT network security practices.

Malcolm is a set of open source tools that enables the user to capture and analyze OT network traffic and logs.

OT cybersecurity services

Identify and mitigate cyber vulnerabilities

Strategic risk analysis provides resources to manage OT risk, according to CISA.

Validated Architecture Design Reviews are intended to evaluate an organization's systems, networks, and security services—including those related to OT— for reliability and resiliency.

The **Vulnerability Coordination** service brings together the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services—including those relating to OT—with the affected vendor(s).

Administrative subpoena for vulnerability notification warns critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors.

Prepare for OT cyberattacks

The **Control Environment Laboratory Resource** allows stakeholders, including critical infrastructure owners and operators, to practice cybersecurity activities in an OT environment.

Exercises provide cyber exercise planning to support critical infrastructure partners—including those using OT—by delivering various cyber exercise planning workshops and seminars.

Training provides OT cybersecurity training with online and in-person offerings.

Identify, analyze, and respond to OT cyberattacks

CyberSentry is a voluntary program that leverages hardware and software capabilities to identify malicious activity on critical infrastructure OT systems.

Threat hunting and incident response assists owners and operators when they believe a threat actor may have gained initial access or caused an adverse impact on their network.

Source: CISA (documentation and icons). | GAO-24-106576

Accessible Text for Figure 3: The Cybersecurity and Infrastructure Security Agency's (CISA) 13 Operational Technology (OT) Cybersecurity Products and Services

Category	Subcategory	Subcategory member
OT products	Cyber threat information and best practices products	Industrial control systems (ICS) advisories provide information about current security issues, vulnerabilities, and exploits.
OT products	Cyber threat information and best practices products	ICS best practice guidance describes practices that critical infrastructure owners and operators can use to address cyber risks facing their OT networks.
OT products	Tools for owners and operators	The Cyber Security Evaluation Tool® is desktop software that guides asset owners and operators through a step-by-step process to evaluate OT and IT network security practices.
OT products	Tools for owners and operators	Malcolm is a set of open source tools that enables the user to capture and analyze OT network traffic and logs.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Strategic risk analysis provides resources to manage OT risk, according to CISA.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Validated Architecture Design Reviews are intended to evaluate an organization's systems, networks, and security services—including those related to OT— for reliability and resiliency.
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	The Vulnerability Coordination service brings together the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services—including those relating to OT—with the affected vendor(s).
OT cybersecurity services	Identify and mitigate cyber vulnerabilities	Administrative subpoena for vulnerability notification warns critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors.

Category	Subcategory	Subcategory member
OT cybersecurity services	Prepare for OT cyberattacks	The Control Environment Laboratory Resource allows stakeholders, including critical infrastructure owners and operators, to practice cybersecurity activities in an OT environment.
OT cybersecurity services	Prepare for OT cyberattacks	Exercises provide cyber exercise planning to support critical infrastructure partners—including those using OT—by delivering various cyber exercise planning workshops and seminars.
OT cybersecurity services	Prepare for OT cyberattacks	Training provides OT cybersecurity training with online and in-person offerings.
OT cybersecurity services	Identify, analyze, and respond to OT cyberattacks	CyberSentry is a voluntary program that leverages hardware and software capabilities to identify malicious activity on critical infrastructure OT systems.
OT cybersecurity services	Identify, analyze, and respond to OT cyberattacks	Threat hunting and incident response assists owners and operators when they believe a threat actor may have gained initial access or caused an adverse impact on their network.

Source: CISA (documentation and icons). | GAO-24-106576

Twelve nonfederal entities identified positive experiences using nine of CISA's products and services.[40] Examples of positive experiences highlighted by selected nonfederal entities include:

- The **industrial control system advisories and best practice guidance** products are effective and have helped consumers stay informed of threats and find vulnerabilities in their environment.

[40] More specifically, nine nonfederal entities identified positive experiences in using six services: (1) CyberSentry, (2) exercises, (3) threat hunting and incident response, (4) training, (5) validated architecture design reviews, and (6) vulnerability coordination. In addition, 10 nonfederal entities identified positive experiences using three products: (1) Cyber Security Evaluation Tool®, (2) ICS advisories, and (3) ICS best practice guidance. The selected 13 nonfederal entities did not identify positive experiences using the remaining three services and one product.

- The **Cyber Security Evaluation Tool®** was user friendly and useful in explaining the risk assessment to customers who may not have extensive cyber literacy.
- The **Validated Architecture Design Review** had a positive impact in supporting compliance efforts.
- With respect to the **Vulnerability Coordination service**, CISA is an excellent partner in the process of coordinating vulnerability disclosures and can help with contacting impacted vendors.
- CISA's OT **training** is among the best training on the subject.
- The skill sets, tools, and capabilities of the CISA staff engaged in the **threat hunting and incident response** service have been of high quality.

CISA Has Not Addressed Negative Experiences Identified Using Certain OT Services

Seven selected nonfederal entities identified negative experiences in using six of CISA's OT cybersecurity products and services.[41] Examples of negative experiences highlighted by selected nonfederal entities include:

- **Validated architecture design reviews.** CISA does not have enough staff to provide the reviews to all that requested it.[42] Demand for this service increased after the Transportation Security Administration (TSA) (1) required that certain pipeline owners and operators conduct architecture design reviews of their OT systems, and (2) stated that

[41] More specifically, six nonfederal entities identified negative experiences in using four services: (1) threat hunting and incident response, (2) training, (3) validated architecture design reviews, and (4) vulnerability coordination. In addition, two nonfederal entities identified negative experiences using two products: (1) ICS advisories and (2) ICS best practice guidance. The selected 13 nonfederal entities did not identify negative experiences using the remaining five services and two products.

[42] CISA officials explained that many entities that have historically requested validated architecture design reviews did not have the technical maturity to benefit from the assessment and did not possess applicable OT systems. CISA officials added that, in fiscal year 2023, CISA modernized its assessment sign-up model to have CISA regional offices direct the right vulnerability service to critical infrastructure owners and operators. CISA officials noted that alternative services are available to entities that are not good candidates for these validated architecture design reviews.

validated architecture design reviews conducted by CISA would satisfy this requirement.[43]

- **Vulnerability coordination service.** Vulnerabilities reported through CISA's process often take more than a year between the initial report of a vulnerability and public disclosure.[44] This process can be lengthy because CISA (1) waits for the vendor to develop a patch for the vulnerability before public disclosure and (2) believes that it does not have authority to force vendors to patch these vulnerabilities in a timely manner. In addition, CISA accidentally added a security researcher to an email thread regarding a vulnerability for which the researcher had no prior knowledge.[45] This mistake could have led to the sale of this vulnerability on the black market for exploitation.

To address the challenge of negative experiences in using products and services, we have previously reported on the importance of measuring customer service.[46] Taking a portfolio-based approach to measuring customer service can position agencies to determine whether allocated resources are yielding the intended results across a portfolio of projects, products, or services. In addition, this approach can allow agencies to reallocate resources as needed within the portfolio to achieve an optimal

[43] TSA officials noted that their security directives require certain pipeline and railroad owners and operators to have a qualified third party to conduct a cybersecurity architecture design review every 2 years and that CISA's validated architecture design review meets the security directive requirements. Those officials added that TSA did not intend for CISA to be the only provider of these reviews to all entities covered under the directives.

[44] CISA officials stated that they believe that this characterization of CISA's disclosure process is inaccurate. They explained that CISA has a 45-day disclosure policy. They added that if a case involving a vulnerability is not progressing for any reason (e.g., vendor or researcher becoming unresponsive), then CISA will work with the remaining stakeholders to agree on an appropriate timeline. Nevertheless, CISA officials also noted that they do not have the authority to enforce specific time frames for vendors to develop patches to address OT vulnerabilities. Those officials added that it may not be feasible or realistic for some vendors to patch their vulnerabilities within a fixed deadline due to technical constraints (e.g., complex changes to a codebase or requirements for testing patches prior to release).

[45] CISA officials acknowledged that such mistakes do occur. Those officials added that CISA's coordinated vulnerability disclosure team recommends that researchers submit vulnerability reports through the agency's secure platform to facilitate coordination in a secure environment. CISA officials explained that the use of this platform—as opposed to email—can help to avoid these types of mistakes.

[46] GAO, *Taxpayer Service: IRS Could Improve the Taxpayer Experience by Using Better Service Performance Measures*, GAO-20-656 (Washington, D.C.: Sept. 23, 2020).

return on investment. In particular, we have previously highlighted the importance of agencies adopting the following practices:

- measure customer service, and
- analyze the results of customer service measures and make needed improvements.

However, CISA has not addressed these practices across the agency's portfolio of 13 OT cybersecurity products and services. Specifically:

- **Measure customer service.** CISA measured customer service for one of its 13 products and services—its training service. Specifically, CISA measured training and instructor effectiveness for its instructor-led courses.

  However, CISA did not measure customer service for any of its other 12 products and services. CISA officials stated they have begun measuring customer service in targeted pockets of the organization—including for various OT products and services.[47] However, CISA did not provide documentation demonstrating that it is measuring customer service for these OT products and services.

- **Analyze the results of customer service measures and make needed improvements.** CISA did not measure customer service for its products and services; as such, it also did not analyze the results of any such measurements and use those results to make needed improvements.[48]

CISA officials explained that they are in the early stages of hiring customer experience specialists, implementing key customer experience metrics, and redesigning processes to support strong customer feedback loops.[49] Until CISA (1) measures customer service for all of its OT

[47] Specifically, CISA officials stated they measure customer service for its validated architecture design reviews, industrial control systems advisories, Control Environment Laboratory Resource, Malcolm, and CISA's exercises. For example, CISA officials stated that they have contracted the support of the Office of Personnel Management to conduct voluntary customer satisfaction surveys to recipients of validated architecture design reviews since 2018.

[48] Although CISA measured customer service for its training service, it did not demonstrate that it analyzed the results of those measures and made needed improvements.

[49] CISA officials noted that this work is consistent with the goals of Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* and the recent DHS Policy Statement 076-02, *Designing and Delivering Improved Customer Experience for the Public*.

products and services and (2) uses the results of such measures to make improvements to the products and services, CISA will not have information on how its OT products and services are performing.

CISA Has Not Addressed Concerns with Insufficient Staff That Have the Requisite OT Skills

CISA officials and one nonfederal entity identified concerns with insufficient CISA staff with the requisite OT skills as a challenge to delivering or using three services. Specifically:

- As previously mentioned, CISA does not have enough staff to provide the validated architecture design reviews to all that requested them. Specifically, CISA stated that since the agency began comprehensively tracking these reviews in 2019, it has only been able to fulfill 125 of the 572 OT-related requests for these reviews, as of May 2023.[50]

  Demand for this service increased after TSA (1) required that certain pipeline and railroad owners and operators conduct architecture design reviews of their OT systems every 2 years, and (2) stated that validated architecture design reviews conducted by CISA would satisfy this requirement.[51] CISA officials acknowledged this challenge and explained that these reviews require substantial personnel time and resources to conduct. As a result, CISA officials explained that the agency is only able to conduct a limited number of reviews each year.

- CISA officials stated that it is a continual challenge to ensure that the administrative subpoena service remains adequately staffed in terms of the quantity of personnel and the personnel's knowledge, skills, and abilities.[52] CISA's administrative subpoena service seeks to warn

[50] CISA officials also noted that some of the entities that requested these reviews were not eligible to receive this service.

[51] TSA, *Security Directive Pipeline-2021-02D: Pipeline Cybersecurity Mitigation Action, Contingency Planning, and Testing* (July 27, 2023); and *Rail Cybersecurity Mitigation Actions and Testing, Security Directive* 1580/82-2022-01A (Springfield, VA: Oct. 24, 2023).

[52] This authority applies when CISA identifies a system connected to the internet with a specific security vulnerability and has reason to believe the security vulnerability relates to critical infrastructure and affects a covered device or system but is unable to identify the entity at risk.

critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors using its administrative subpoena authority. In cases where CISA does not know the owner of a vulnerable system, CISA uses its authority to issue administrative subpoenas to obtain information necessary to proactively identify and notify an entity at risk.

CISA explained that although the agency has identified several enhancements to the service (e.g., developing and implementing a communications plan for external stakeholders), the agency is not currently staffed to implement these enhancements. CISA officials noted that it remains committed to the program's success and will seek the resources and staffing required to maximize the program's impact and keep pace with its growth.

- CISA officials noted that the cyber OT forensics portion of the Threat Hunting and Incident Response service is new and is experiencing growth issues, to include resourcing issues. As of November 2023, CISA stated that it relied on four federal employees and five contractor staff to carry out threat hunting and incident response for OT systems. CISA officials stated that this is not enough staff to respond to significant attacks impacting OT systems in multiple locations at the same time.[53] Those officials noted that they have requested additional federal staff and funding for contractor staff travel to incident response operations. They added that the agency has agreements with other federal partners, including the Department of Defense (DOD), to augment CISA's OT incident response capabilities.[54]

We have previously reported that effective workforce planning can position federal agencies to have the essential balance of skills, knowledge, and experience needed to execute their missions and

[53] We have previously highlighted the possibility of cyber incidents that can spill over from the initial target to other organizations and coordinated attacks on distributed targets (e.g., a coordinated attack on multiple electricity generation or transmission utilities). See, e.g., GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, GAO-22-104256 (Washington, D.C.: June 21, 2022); and *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[54] However, CISA did not provide documentation of these agreements with other federal partners describing the staff with OT expertise from other agencies that would be available in the event of a significant OT-related incident.

program goals.[55] We have also stressed the importance of performing an organization-wide workforce assessment to ensure that leadership has insight into all units, products, and services, and can ensure effective allocation of resources across those areas.[56]

In particular, we have previously highlighted the need for agencies to develop competency and staffing requirements, assess gaps in competencies and staffing, and develop strategies for filling the gaps.[57] Taking such steps is consistent with activities outlined in human capital management guidance developed by the Office of Personnel Management, the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, and the Office of Management and Budget.[58]

To its credit, CISA's human capital management practices call for the agency to develop competency and staffing requirements, assess gaps in competencies and staffing, and develop strategies for filling the gaps. However, CISA has not implemented these practices for its OT workforce.

CISA officials acknowledged the lack of workforce planning for staff with OT expertise and outlined three efforts they are taking to address this weakness:

[55] See, e.g., GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019) and *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[56] See, e.g., GAO, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

[57] See, e.g., GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019) and *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[58] Office of Personnel Management, *Human Capital Framework*, 5 C.F.R. pt. 250, subpt. B.; Office of Personnel Management and the Chief Human Capital Officers Council Subcommittee for Hiring and Succession Planning, *End-to-End Hiring Initiative* (March 2017); Office of Personnel Management, *Workforce Planning Model*, https://www.opm.gov/policy-data-oversight/human-capital-framework/reference-materials/strategic-alignment/workforceplanning.pdf (accessed Dec. 12, 2023).

- CISA officials explained that they are currently developing the *CISA Workforce Framework*, which is a collection of documents and tools that are intended to allow the agency to plan, recruit, and develop a robust, sustainable workforce to meet its mission. CISA officials stated that this framework will allow the agency to standardize work roles, including those for positions relating to OT.[59] However, as of September 2023 the draft *CISA Workforce Framework* that we reviewed did not address OT competencies and staffing requirements.
- In November 2023, CISA officials stated that the agency had hired an OT subject matter expert who is tasked with (1) providing OT expertise for CISA's research and development projects and products and services, and (2) increasing coordination between the teams managing those products. Those officials added that the agency has made a tentative job offer for an Industrial Control Systems strategist. However, CISA did not provide documentation describing the responsibility for either position to carry out key human capital planning and analysis practices for its OT workforce, such as developing competency and staffing requirements, assessing gaps in competencies and staffing, and developing strategies for filling the gaps.
- In January 2024, CISA officials stated that the agency has scheduled the development of an OT work role in fiscal year 2024 using workforce planning practices highlighted by the National Initiative for Cybersecurity Education.[60] CISA expected the approval of the OT work role and respective position descriptions by September 2024.

Until CISA (1) develops OT competency and staffing requirements, (2) assesses OT competency and staffing gaps, and (3) develops strategies for filling any gaps, the agency will likely not allocate optimal resources to providing its OT services. Consequently, CISA may not effectively deliver services needed to address OT risks facing critical infrastructure owners and operators.

[59] CISA officials explained that initial implementation of the framework is expected to occur by October 2024 with full implementation by October 2026.

[60] The National Initiative for Cybersecurity Education is a partnership among the industry, academia, and government sectors to help strengthen cybersecurity education, training, and development.

CISA Worked with Agencies to Mitigate OT Risks, but Did Not Fully Address Leading Collaboration Practices

CISA and the seven selected agencies primarily collaborated using coordination calls when mitigating OT risks to critical infrastructure owners and operators.[61] Although the seven selected agencies cited examples of where their collaboration with CISA yielded positive outcomes to cyber OT risks, four agencies also identified two challenges in coordinating with CISA to address such risks. To address these types of challenges, it is important for agencies to adopt leading collaboration practices; however, CISA and the agencies have not fully addressed them.

CISA and Selected Agencies Primarily Collaborated Using Coordination Meetings to Mitigate Cyber OT Risks

Six of the seven selected agencies identified regularly scheduled coordination calls as the primary mechanism they use to collaborate with CISA in helping to mitigate cyber OT risks to critical infrastructure. Specifically,

- Two of the selected agencies—Pipeline and Hazardous Materials Safety Administration (PHMSA) and National Security Agency (NSA)—highlighted their participation in regular infrastructure protection council and committee meetings. For example, PHMSA reported that it participated in the Oil and Natural Gas Sector Coordinating Council leadership meetings and the Surface Transportation Security Advisory Committee quarterly meetings.[62] Additionally, NSA officials told us that its Critical Networks Defense Office and Cybersecurity Collaboration Center participate in monthly

[61] The seven selected agencies are: (1) DOD's Defense Cyber Crime Center (DC3), (2) DOD's National Security Agency (NSA), (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), (4) DHS's Transportation Security Administration (TSA), (5) DHS's U.S. Coast Guard (USCG), and (6) DOT's Federal Railroad Administration (FRA), and (7) DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA).

[62] CISA officials stated that they agency participated in the Oil and Natural Gas Sector Coordinating Council monthly leadership meetings as well as the council's joint meetings with the Energy Sector Government Coordinating Council.

meetings with CISA's Joint Cyber Defense Collaborative. NSA officials added that these offices helped develop the 2024 cyber planning agenda for the Joint Cyber Defense Collaborative.

- The remaining four agencies highlighted the use of other weekly or bi-weekly coordinating calls with CISA. For example, a U.S. Coast Guard (USCG) official stated that their agency participated in weekly phone calls with CISA (as well as with the Department of Transportation (DOT) and TSA) to coordinate the different activities within their SRMA responsibilities (e.g., sharing information on new vulnerabilities). In addition, TSA officials stated that CISA hosted a bi-weekly cyber policy collaboration group meeting with the goal of harmonizing cybersecurity policy efforts across various sectors and subsectors.

Further, each of these six agencies cited examples of how their other collaboration efforts with CISA helped to address cyber OT risks. For example:

- Federal Railroad Administration (FRA) officials stated that they have collaborated with CISA to provide cyber threat assessments to freight railroad owners and operators. In addition, CISA and FRA collaborated with TSA in developing a security directive aimed at enhancing cybersecurity resilience of freight and passenger rail systems.[63]
- TSA officials highlighted their collaboration with CISA to update their pipeline security directive relating to the cybersecurity of certain pipeline owners and operators.[64] TSA officials stated they closely collaborated with CISA in order to update the directive to include performance-based cybersecurity mitigation actions.

[63] TSA, *Rail Cybersecurity Mitigation Actions and Testing*, Security Directive 1580/82-2022-01 (Springfield, VA: Oct. 24, 2022); *Rail Cybersecurity Mitigation Actions and Testing*, Security Directive 1580/82-2022-01A (Springfield, VA: Oct. 24, 2023). The security directive required that TSA-specified passenger and freight railroad carriers take action to prevent disruption and degradation to their infrastructure to achieve the certain critical security outcomes. In addition, the directive requires passenger and freight railroad carriers to (1) establish and execute a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures the passenger and freight rail carriers are utilizing to achieve the security outcomes set forth in the security directive, and (2) establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve vulnerabilities within devices, networks, and systems.

[64] TSA, *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*, Security Directive Pipeline-2021-02D (Springfield, VA: July 26, 2023).

- In September 2022, NSA and CISA published a joint cybersecurity advisory about threats to OT and steps that can be taken to address those threats.[65]

Officials representing the remaining agency—DOD Cyber Crime Center (DC3)—told us that it generally has not collaborated with CISA to address OT. These officials added that they met with CISA's threat hunt team in August 2023 to discuss, among other topics, threat hunt and incident response deployments, operational priorities, personnel assignments, and training.

Four Selected Agencies Identified Challenges to Effectively Collaborating with CISA to Address Cyber OT Risks

Four of the six selected agencies—Cybersecurity, Energy Security, and Emergency Response (CESER), FRA, PHMSA, and USCG—identified two challenges in collaborating with CISA to address cyber OT risks: (1) CISA ineffectively sharing information with critical infrastructure owners and operators, and (2) CISA and PHMSA lacking a process to share cyber threat and vulnerability information with pipeline owners and operators. Specifically:

- **CISA ineffectively sharing information with critical infrastructure owners and operators.** Three selected agencies—CESER, FRA, and USCG—identified CISA's information sharing efforts with critical infrastructure owners in their subsectors as a challenge. For example, CESER officials stated that CISA has, on occasion, shared cybersecurity information with the oil and natural gas industry before connecting with CESER to perform due diligence as to whether the information should be shared and with whom. In particular, these officials explained that they have found that some of the information shared was (1) not critical and (2) should have been shared with a narrower audience.[66] In addition, FRA officials told us that CISA independently conducted outreach to the Association with American

[65] NSA, CISA, *Control System Defense: Know the Opponent,* Cybersecurity Advisory PP-22-1413, Ver. 1.0 (September 2022).

[66] CESER officials added they would like CISA to work collaboratively with the SRMAs to engage private sector stakeholders.

Railroads[67] on a cybersecurity issue without informing FRA. This resulted in duplicative outreach to the association when FRA contacted it on the same issue.

- **CISA and PHMSA lacking a process to share cyber threat and vulnerability information with pipeline owners and operators.** PHMSA officials told us it has been challenging to develop a process with CISA for sharing cyber threat and vulnerability information with pipeline owners and operators. In particular, PHMSA officials explained that it has been challenging to develop such a process that leverages their existing relationships with liquefied natural gas facilities and related state partners. The same officials further explained that CISA lacks the daily interaction with pipeline owners and operators that PHMSA has. PHMSA officials told us that they would like CISA to leverage their expertise and daily interaction with the sector to help increase communication of threats to all pipeline operators and their OT systems.[68]

CISA Partially Addressed Most Selected Leading Collaboration Practices When Addressing Cyber OT Risks with Selected Agencies

To address coordination challenges, we have previously reported on the importance of addressing eight leading practices for effective interagency collaboration.[69] We selected five of these practices as most relevant for CISA's coordination (see table 3).

Table 3: Selected Leading Interagency Collaborations Practices and Key Considerations

Leading collaboration practices	Selected key considerations
Define common outcomes	• Have the short- and long-term outcomes been clearly defined?

[67] The Association of American Railroads is a trade organization focused on the safety and productivity of the U.S. freight rail industry.

[68] PHMSA officials added that they have provided this feedback to CISA and offered to connect CISA with pipeline operators during cyber incidents.

[69] GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

Leading collaboration practices	Selected key considerations
Ensure accountability	• What are the ways to assess progress toward the short- and long-term outcomes?
Bridge organizational cultures	• Have participating agencies established compatible policies, procedures, and other means to operate across agency boundaries?
Clarify roles and responsibilities	• Have the roles and responsibilities of the participants been clarified?
Develop and update written guidance and agreements	• If appropriate, have agreements regarding the collaboration been documented? • Have ways to continually update or monitor written agreements been developed?

Source: GAO-23-105520. | GAO-24-106576

CISA partially addressed three of the five selected leading practices when collaborating with the seven selected agencies in addressing OT risks: define common outcomes, bridge organizational cultures, and clarify roles and responsibilities. Regarding the practice of ensuring accountability, CISA partially addressed this practice when collaborating with four agencies and did not address this practice with the remaining three agencies. Further, regarding the practice of developing and updating written guidance, CISA partially addressed the practice with two agencies and did not implement the practice with the remaining five agencies.

Table 4 summarizes the extent to which CISA addressed the five selected practices when collaborating with the seven selected agencies to mitigate OT risks.

Table 4: Extent to Which the Cybersecurity and Infrastructure Security Agency (CISA) Addressed Selected Leading Collaboration Practices with Seven Selected Agencies to Mitigate Cyber Operational Technology Risks to Critical Infrastructure

Collaboration practices	CESER	DC3	FRA	NSA	PHMSA	TSA	USCG
Define common outcomes	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Ensure accountability	not addressed	not addressed	partially addressed	not addressed	partially addressed	partially addressed	partially addressed
Bridge organizational cultures	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed

Collaboration practices	CESER	DC3	FRA	NSA	PHMSA	TSA	USCG
Clarify roles and responsibilities	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Develop and update written guidance and agreements	not addressed	partially addressed	not addressed	not addressed	not addressed	not addressed	partially addressed

Legend: ●=Generally addressed: CISA and the selected federal entity provided complete evidence that addressed the key considerations associated with the selected practice; ◑=Partially addressed: CISA and the selected federal entity provided evidence that addressed some, but not all, of the key considerations associated with the selected practice. ○=Not addressed: CISA and the selected federal entity did not provide evidence that addressed the key considerations associated with the selected practice.

Source: GAO analysis of agency information. | GAO-24-106576

Note: CESER (Cybersecurity, Energy Security, and Emergency Response), DC3 (Department of Defense Cyber Crime Center) FRA (Federal Railroad Administration), NSA (National Security Agency), PHMSA (Pipeline and Hazardous Materials Safety Administration), TSA (Transportation Security Administration), and USCG (U.S. Coast Guard).

- **Define common outcomes.** CISA partially addressed this practice when collaborating with the seven selected agencies in addressing OT risks. Specifically, DHS and the departments for the six selected agencies developed sector-specific plans that highlighted the need (i.e., common outcome) to address cyber risks facing the selected sector and selected subsectors.[70] However, these plans did not specifically define outcomes related to cyber risks to OT.[71]

- **Ensure accountability.** CISA partially addressed this practice when collaborating with four of the selected agencies to address OT risks and did not implement this practice when collaborating with the two other agencies to address such risks. In particular,

  - CISA partially addressed the practice of ensuring accountability when collaborating with FRA, PHMSA, TSA, and USCG. Specifically, the sector-specific plan associated with those four selected agencies—DOT and DHS's *Transportation Systems Sector Specific Plan*—called for an assessment of the extent to which critical infrastructure owners and operators have adopted the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter referred to as the "Cybersecurity

[70] The departments and agencies designated as SRMAs (e.g., Department of Energy) often task component agencies or offices (e.g., CESER) to carry out their responsibilities.

[71] DHS developed these plans prior to the creation of CISA in 2018.

Framework").[72] DOT, in coordination with DHS, developed and distributed a survey to the Transportation Systems sector from March 2021 to June 2021 to obtain insight into the sector's adoption of the Cybersecurity Framework.[73] Although the survey collected information on 857 sector entities' awareness, implementation, and usage of the Cybersecurity Framework, DOT and DHS were unable to determine the level of adoption of specific practices from the framework—including those pertaining to securing OT.

  - CISA did not address the practice of ensuring accountability when collaborating with CESER, DC3, and NSA. In particular, while the Energy and Defense Industrial Base sector-specific plans called for measuring efforts to address cyber risks, the plans did not identify specific federal or industry standards or guidelines that were to be used to measure these efforts—including ones that can be used to measure efforts to address OT risks.

- **Bridge organizational cultures.** CISA partially addressed the practice of bridging organizational cultures when collaborating with the seven selected agencies in addressing OT risks. Specifically, DHS and the departments representing the selected agencies (DOD, DOE, and DOT) developed sector-specific plans that described methods for coordinating on critical infrastructure protection issues, such as government coordinating councils. However, these plans did not describe specific policies, procedures, and other means to operate across agency boundaries for OT.[74]
- **Clarify roles and responsibilities.** CISA partially addressed the practice of clarifying roles and responsibilities when collaborating with the seven selected agencies in addressing OT risks. Presidential policy and agency plans identified roles and responsibilities for DHS

[72] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. (April 16, 2018). The Cybersecurity Framework is intended to provide critical infrastructure owners and operators with cybersecurity principles and best practices for improving the security and resilience of IT and OT systems supporting the nation's critical infrastructure.

[73] This work was done in response to a priority recommendation we made in GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018). Transportation has taken steps to address this recommendation.

[74] CISA officials noted that the agency's Cybersecurity Division maintains the Control Systems Interagency Working Group which serves as a vehicle to coordinate OT-specific policy activities. However, none of the seven selected agencies highlighted this working group and CISA did not provide any documentation describing this group's responsibilities or accomplishments.

and the departments representing the selected agencies (DOD, DOE, and DOT) with regard to addressing cyber risks to their respective sectors. In particular:

- PPD-21 designated DHS and DOT as the lead departments for the Transportation Systems sector, DOE was designated as the lead department for the Energy sector, and DOD was designated as the lead department for the Defense Industrial Base sector. In addition, the sector-specific plans for those sectors expanded on this framework by, among other things, identifying responsibilities for DHS and the three departments representing the selected agencies to collaborate in order to help address cyber risks facing the sectors and subsectors.
- PPD-41 identified high-level roles for responding to cyber incidents, including roles for DHS and the other three departments representing the selected agencies. In particular, the directive designated DHS as the lead agency for asset response. As such, DHS is to provide technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents. In addition, the directive called for SRMAs to coordinate federal efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

However, the sector-specific plan did not discuss (1) responsibilities relating to OT or (2) the responsibilities of CISA and five selected agencies (CESER, DC3, FRA, NSA, and PHMSA). In addition, CISA and the seven selected agencies have not developed policies, procedures, or mechanisms to expand on the framework established in PPD-41 for purposes of clarifying roles and responsibilities for responding to OT attacks on the selected sectors and subsectors.

- **Develop and update written guidance and agreements.** CISA partially addressed this practice for two agencies, DC3 and USCG. In particular, although CISA entered into agreements with these agencies for detailing staff to CISA, sharing information, and responding to incidents, these agreements did not relate to or discuss OT. However, CISA did not implement the practice of developing and updating written guidance and agreements for collaborating with five of the agencies (e.g., clarifying and documenting roles and responsibilities for communicating with critical infrastructure owners and operators or for responding to incidents).

The incomplete adoption of the five selected leading collaboration practices is due, in part, to a lack of (1) guidance from CISA to the

SRMAs on how to update their sector-specific plans regarding collaboration and (2) a CISA policy for developing agreements with SRMAs with respect to collaboration. Specifically:

- **Lack of guidance from CISA to the SRMAs on how to update their sector-specific plans regarding collaboration.** According to the 2013 *National Infrastructure Protection Plan*, all sectors are to update their sector-specific plans every 4 years based on guidance developed by DHS. However, CISA has not issued such guidance to the SRMAs (nor has any other agency within DHS)—including guidance on collaboration with other agencies on mitigating OT cyber risks. Without such guidance, DOD has not updated the sector-specific plan for its respective sector—the Defense Industrial Base—since 2010. In addition, DOE, DHS, and DOT have not updated their respective plans for the Energy and Transportation Systems sectors since 2015.

  In October 2022, CISA officials stated that they plan to provide guidance to SRMAs on how they should update their sector-specific plans. Specifically, CISA officials told us they expected to issue an updated sector-specific plan template 3 to 6 months after the release of the updated National Plan for SRMAs to use in collaboration with their sector partners.

  However, as of September 2023, CISA officials told us they did not have a timeline for issuing the updated National Plan and are waiting until the administration completes a review of PPD-21.[75] In addition, CISA officials could not provide an estimated time frame for when the administration will complete its review of PPD-21. Until CISA issues guidance on updating sector-specific plans regarding collaboration when agencies are mitigating cyber OT risks, CISA will not be optimally positioned to coordinate with SRMAs on mitigating cyber OT risks.

- **Lack of a CISA policy for developing agreements with SRMAs regarding collaboration.** CISA officials were not aware of any agency policies for developing agreements with SRMAs regarding

[75] In February 2023, we reported that CISA was working on guidance and more to help SRMAs implement their statutorily defined responsibilities, including guidance for updating sector-specific plans. We recommended that CISA set timelines for completing this work. As of December 2023, CISA has not addressed this recommendation. See, GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806 (Washington, D.C.: Feb. 7, 2023).

collaboration to mitigate cyber OT risks. CISA's Industrial Control Systems Expert noted that CISA needs to treat each SRMA differently based on that agency's resources. That official added that the thresholds for where an SRMA needs additional assistance is set by CISA's Stakeholder Engagement Division. However, CISA did not provide documentation of these thresholds. Until CISA develops and implements a policy on agreements with SRMAs regarding collaboration to mitigate cyber OT risks, CISA may continue to experience challenges in interagency collaboration.

Conclusions

As cyber threats to OT systems continue to grow, CISA plays a critical role in helping critical infrastructure owners and operators address these threats. To its credit, CISA developed and delivered 13 products and services intended to address this need. However, CISA and the selected nonfederal entities identified challenges to delivering and using these products and services. Although processes relating to measuring customer service and workforce planning can help agencies to address these challenges, CISA has not fully implemented such processes. Until CISA does so, critical infrastructure owners and operators will continue to experience challenges in using the products and services.

The need for CISA and the selected federal agencies to effectively collaborate to help critical infrastructure owners and operators address cyber threats to OT systems is equally important. Notably, all of the selected agencies cited several positive OT cybersecurity outcomes stemming from their collaboration with CISA. However, four of these agencies also identified challenges impeding this collaboration. Although implementing the five selected leading collaboration practices can help agencies to address coordination challenges, CISA has not fully addressed these practices. Key to this shortcoming is the lack of (1) guidance from CISA to the SRMAs on how to update their sector-specific plans with respect to collaboration and (2) a CISA policy for developing agreements with SRMAs regarding collaboration. Until CISA takes action to address these underlying weaknesses, it and the agencies will not be well-positioned to help critical infrastructure owners and operators address cyber risks to OT systems.

Recommendations for Executive Action

We are making four recommendations to CISA:

The Director of CISA should (1) measure customer service for all of its OT products and services and (2) use the results of such measures to make improvements to the products and services. (Recommendation 1)

The Director of CISA should (1) develop OT competency and staffing requirements, (2) assess OT competency and staffing gaps, and (3) develop strategies for filling any gaps. (Recommendation 2)

The Director of CISA should issue guidance on how SRMAs should update sector-specific plans that reflects the five selected leading collaboration practices when agencies are mitigating cyber OT risks. (Recommendation 3)

The Director of CISA should (1) develop an agency-wide policy on agreements with SRMAs regarding collaboration to mitigate OT risks and (2) implement that policy with the selected agencies. (Recommendation 4)

Agency Comments

We provided a draft of this report to the DOD, DOE, DHS, and DOT for review and comment. We received written comments from DHS on behalf of CISA, to which we made recommendations. In its written comments, DHS concurred with the four recommendations to CISA and described actions that CISA plans to take to implement them. For example, DHS stated that CISA intends to standardize and improve the quality of customer experience processes and rewrite technical competency descriptions to better capture the range of OT skillsets needed at the agency. DHS also stated that following updates to the National Plan and PPD-21, CISA will work closely with SRMAs to develop guidance on updates to sector-specific plans and identify additional approaches to risk mitigation that can be implemented across sectors. These comments are reprinted in appendix II.

In addition, DHS, DOE, and DOT provided technical comments, which we incorporated into the report as appropriate. DOD did not have any comments on the draft report.

We are sending copies of this report to the appropriate congressional committees and the heads of each agency in our review. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact Marisol Cruz Cain, at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VII.

Marisol Cruz Cain

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The National Defense Authorization Act of Fiscal Year 2022 includes a provision for us to review the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to mitigate cyber threats to industrial control systems.[1] We used National Institute of Standards and Technology (NIST) guidance to assess the current meaning of the term "industrial control systems" given that the term has been the focus of past publications that NIST issued.[2] Based on current NIST guidance, "industrial control systems" is a term that is encompassed by the broader designation of "operational technology" (OT).[3]

This report examines: (1) CISA's OT cybersecurity products and services and challenges in delivering them, and (2) how CISA and selected federal agencies work together to mitigate cyber OT risks and challenges to collaborating. For each area, we also evaluated CISA's efforts to address any challenges.

[1] Pub. L. No. 117-81, § 1541(c), 135 Stat. 1541, 2055 (Dec. 27, 2021).

[2] 15 U.S.C. § 278g-3. In 2015, NIST published *Guide to Industrial Control Systems (ICS) Security,* SP 800-82, Rev. 2 (Gaithersburg, MD: May 2015), which was the guidance that was current at the time the statute was enacted containing the questions we are addressing in this review. The 2015 guidance had replaced prior guidance of the same title, *Guide to Industrial Control Systems (ICS) Security,* SP 800-82, Rev. 1 (Gaithersburg, MD: May 2013).

[3] NIST, *Guide to Operational Technology (OT) Security*, SP 800-82, Rev. 3 (Gaithersburg, MD: September 2023). In April 2022, pursuant to a shift to broaden federal efforts to secure systems and devices, NIST proposed a draft to revise its 2015 version of SP 800-82, *Guide to Industrial Control Systems (ICS) Security,* SP 800-82, Rev. 2 (Gaithersburg, MD: May 2015). The 2022 NIST draft expanded the scope of its guidance on industrial control systems security to include OT security and changed how it characterizes industrial control systems. NIST, *Guide to Operational Technology (OT) Security,* SP-800-82, Rev. 3/Initial Public Draft (Gaithersburg, MD: April 2022). In September 2023, NIST finalized the proposed draft and issued revision 3. This superseded NIST's 2015 guidance that supports the reference to "industrial control systems" in the language of the statutory mandate that directs us to conduct this review. Given the expansion to OT security in the NIST draft that was incorporated into revision 3, we approached our review from the lens of NIST's most recent guidance on the topic. As stated in the NIST guidance, industrial control systems are an example of OT. Therefore, since the NIST guidance encompasses the term "industrial control systems" within "operational technology," we use the latter term throughout our report to incorporate the former term.

To address our first objective, we identified CISA's OT cybersecurity products and services that were offered to critical infrastructure owners and operators between October 2018 and October 2023. To do so, we reviewed CISA's *Industrial Control Systems Security Offerings*,[4] which lists 17 OT cybersecurity products and services. We then removed one product—the Automated Indicator Sharing System—that does not help critical infrastructure owners and operators to address cyber OT risks.[5] We also removed two services—the Industrial Control System Joint Working Group and technical analysis and one product—industrial control system alerts—that CISA had retired.

We validated that the remaining 13 OT products and services were offered to critical infrastructure owners and operators between October 2018 and October 2023 by obtaining documentation and written responses from CISA describing when these products and services were offered. Detailed information about the final 13 products and services, as well as the three retired products and services, are identified in appendices III, V, and VI.[6]

We then asked (1) CISA officials responsible for the 13 OT cybersecurity products and services and (2) officials from 13 selected nonfederal

[4] CISA's website describes this document as containing the "full catalog" of CISA's OT cybersecurity products and services. See https://www.cisa.gov/topics/industrial-control-systems.

[5] The Automated Indicator Sharing system is a tool that gathers, from critical infrastructure owners and operators, suspected malicious indicators of compromise (e.g., signatures of malicious files) relating to IT systems and networks. CISA also uses this system to disseminate, to critical infrastructure owners and operators, suspected indicators of compromise relating to IT systems and networks. However, while CISA's Industrial Control Systems Service Offerings Catalog identifies this system as a tool that stakeholders can use to share OT threat information, CISA officials told us that this system is not designed to gather OT-specific threat information. CISA officials further explained that critical infrastructure owners and operators could add OT threat data to the system, but the system does not have the capability to identify that threat data as relating to OT systems and networks.

[6] For each of these 13 products and services, we also asked CISA for the following information: (1) how many instances CISA has delivered the products and services and which sectors have leveraged them, (2) how many federal and contract staff CISA relies on to deliver the products and services, and (3) how much CISA has obligated or expended on the product and service since October 2018. We then summarized this information in appendices V and VI.

entities to describe any challenges with those products and services.[7] With respect to the 13 selected nonfederal entities, we interviewed or obtained written responses from:

- Three sector coordinating councils representing selected critical infrastructure sectors and subsectors:[8] the Defense Industrial Base, the Freight Rail, and the Oil and Natural Gas/Pipeline sector coordinating councils.[9] We selected the sector and subsectors because (1) OT is prevalent in the sector and subsectors and (2) the 2023 *Annual Threat Assessment of the U.S. Intelligence Community* highlighted their infrastructures as being at risk from malicious cyber actors.
- Seven OT vendors who joined CISA's Joint Cyber Defense Collaborative in April 2022 when CISA expanded this group to focus on OT cyber issues: (1) Bechtel Corporation, (2) General Electric, (3) Honeywell International Inc., (4) Nozomi Networks Inc., (5) Schneider Electric SE, (6) Siemens AG, and (7) Xylem.[10]
- Four cybersecurity researchers that contributed to the development of CISA's OT-related advisories.[11] We randomly selected researchers with a U.S. presence and who were highlighted in CISA's industrial

[7] We also asked the nonfederal entities to describe any positive experiences they had with the products and services. We describe these positive experiences in appendices V and VI.

[8] These councils are self-organized, self-governing councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. SRMAs and the councils coordinate and collaborate on issues pertaining to their respective critical infrastructure sectors.

[9] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023). According to the Pipeline sector Coordinating Council charter, the group serves as the subject matter expert advisory group to the Oil and Natural Gas Subsector Coordinating Council. As such, we considered the perspectives of the Oil and Natural Gas subsector to include the perspectives of the Pipeline Sector Coordinating Council.

[10] Cybersecurity and Infrastructure Security Agency, *CISA Expands the Joint Cyber Defense Collaborative to include Industrial Control Systems Industry Expertise,* accessed Sept. 14, 2023, https://www.cisa.gov/news-events/news/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems. Three other OT vendors also joined this collaborative in April 2022—Claroty, Dragos, and Schweitzer Engineering Laboratories. However, these vendors did not respond to our requests for information.

[11] One of the selected research organizations was also selected as an OT vendor that joined CISA's joint cyber defense collaborative in April 2022.

control system advisories published from January 2023 to June 2023 as having first identified the vulnerability discussed in the advisories.[12]

We then conducted a content analysis on the responses from CISA and the selected nonfederal entities to identify any frequently reported challenges. We totaled the number of times each challenge was identified and chose to report on the challenges that were identified by three or more entities.

In addition, we conducted interviews with or obtained written responses from CISA to identify efforts it has taken to address these challenges. We then compared CISA's efforts to address the challenges against leading practices in customer service[13] and workforce planning.[14]

To address our second objective, we described how CISA and the selected federal agencies work together to mitigate cyber OT risks and the extent to which they use leading interagency collaboration practices. In particular, we selected the following seven agencies: (1) Department of Defense's (DOD) Defense Cyber Crime Center (DC3); (2) DOD's National Security Agency (NSA); (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response; (4) Department of Homeland Security's (DHS) Transportation Security Administration; (5) DHS's U.S. Coast Guard; (6) Department of Transportation's (DOT) Federal Railroad Administration; and (7) DOT's Pipeline and Hazardous Materials Safety Administration. We did so because we each agency was (1) within sector risk management agencies for the sector and subsectors selected for our first objective[15] and (2) responsible for helping critical infrastructure owners and operators to mitigate cyber OT risks.

We then interviewed officials and reviewed documentation from CISA and the seven selected federal agencies to determine what mechanisms, if any, CISA used to collaborate with each of the agencies to mitigate cyber

[12] We randomly selected 10 cybersecurity researchers that met our criteria. Six of those researchers did not respond to our requests for information.

[13] GAO, *Taxpayer Service: IRS Could Improve the Taxpayer Experience by Using Better Service Performance Measures*, GAO-20-656 (Washington, D.C.: Sept. 23, 2020).

[14] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

[15] As previously mentioned, we selected the Defense Industrial Base sector as well as the Freight Rail, Oil and Natural Gas, and Pipeline subsectors.

OT risks. We also asked the seven agencies to identify any challenges they experienced when collaborating with CISA to mitigate cyber OT risks. Using this information, we conducted a content analysis to identify challenges frequently reported by the select federal agencies. We then totaled the number of times each challenge was identified and chose to report on all challenges.

We then compared CISA's efforts to address the challenges against selected leading practices for enhancing interagency collaboration when collaborating with the seven selected agencies to mitigate cyber OT risks. To do this, we selected (1) five of the eight leading practices that are most relevant for CISA's coordination with other SRMAs and (2) key considerations for each selected practice that were most relevant for this coordination. See table 5 below for the selected practices and considerations.[16]

Table 5: Selected Leading Interagency Collaborations Practices and Key Considerations

Leading collaboration practices	Selected key considerations
Define common outcomes	• Have the short- and long-term outcomes been clearly defined?
Ensure accountability	• What are the ways to assess progress toward the short- and long-term outcomes?
Bridge organizational cultures	• Have participating agencies established compatible policies, procedures, and other means to operate across agency boundaries?
Clarify roles and responsibilities	• Have the roles and responsibilities of the participants been clarified?
Develop and update written guidance and agreements	• If appropriate, have agreements regarding the collaboration been documented? • Have ways to continually update or monitor written agreements been developed?

Source: GAO-23-105520. | GAO-24-106576

We gathered and reviewed documentation describing CISA's and the agencies' collaborative efforts to mitigate cyber OT risks. We then evaluated these collaborative efforts against the selected interagency

[16] GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges,* GAO-23-105520 (Washington, D.C.: May 24, 2023).

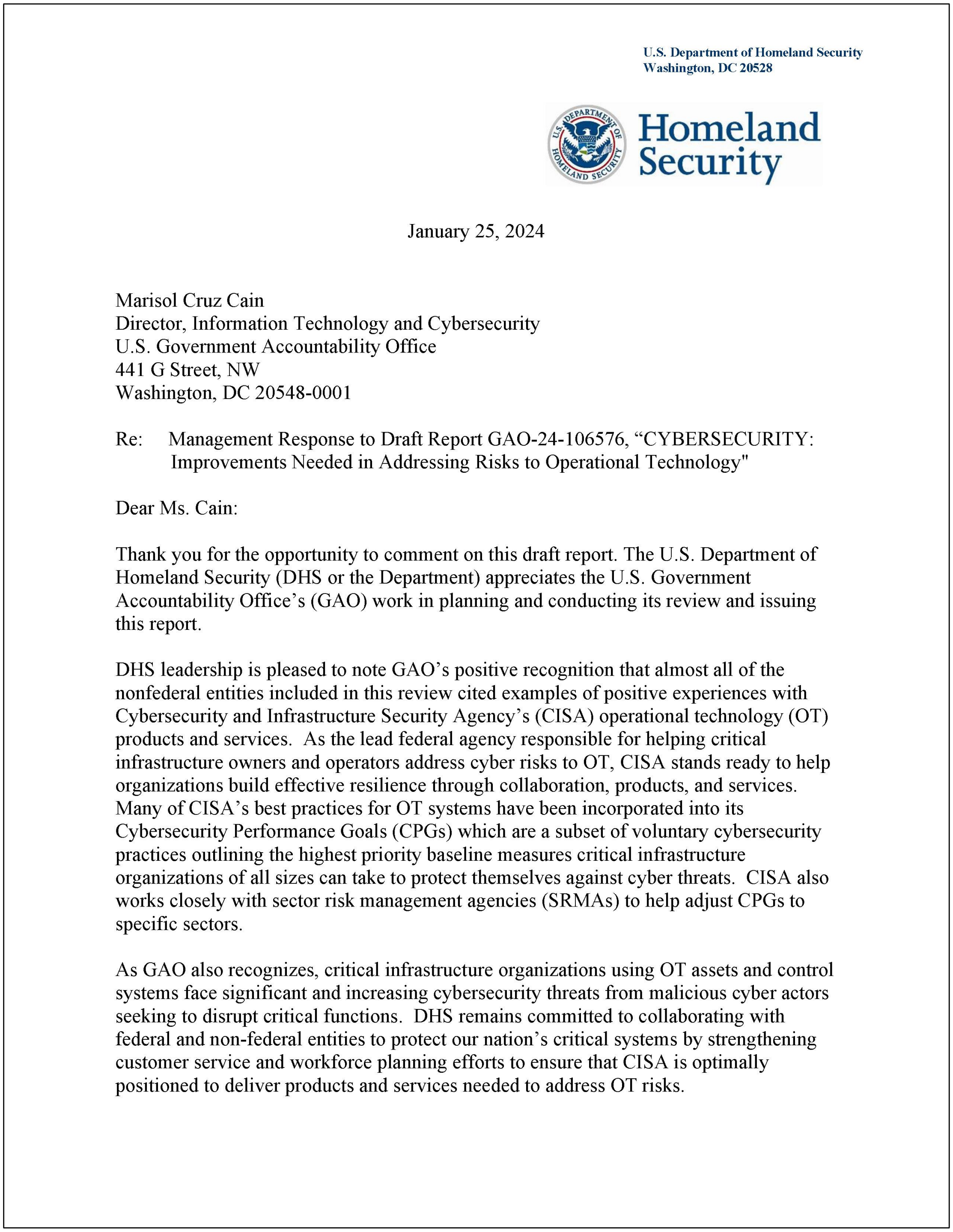
collaboration practices to determine the extent to which CISA and the agencies addressed these practices. We evaluated CISA and the agencies as having “generally addressed,” “partially addressed,” or “not addressed” the criterion for their collaborative efforts to mitigate cyber threats to OT, based on the following:

- Generally addressed—CISA and the selected federal entity provided complete evidence that addressed the key considerations associated with the selected practice.
- Partially addressed—CISA and the selected federal entity provided evidence that addressed some, but not all, of the key considerations associated with the selected practice.
- Not addressed—CISA and the selected federal entity did not provide evidence that addressed the key considerations associated with the selected practice.

We conducted this performance audit from January 2023 to March 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Homeland Security

Appendix II: Comments from the Department of Homeland Security



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

January 25, 2024

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

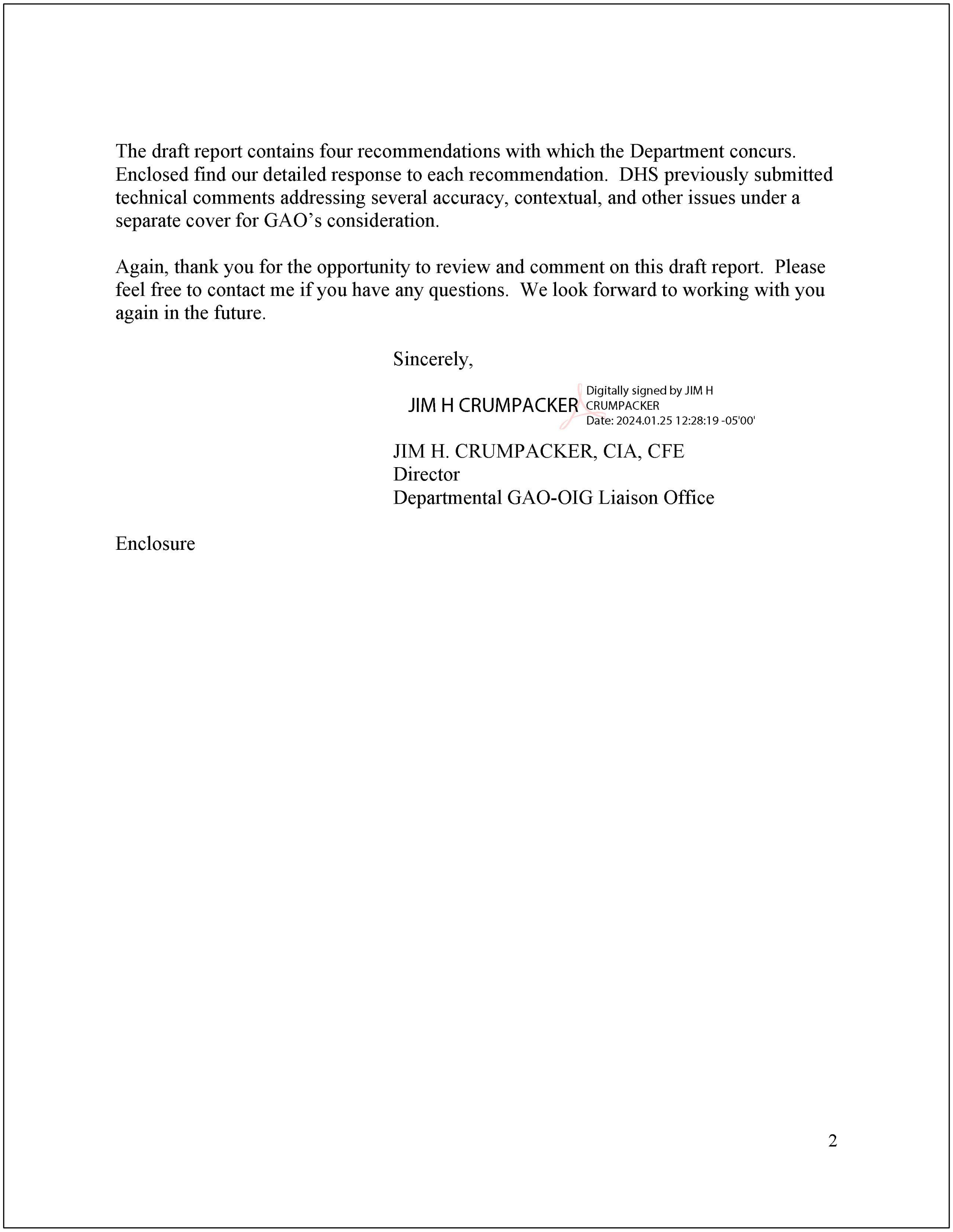
Re: Management Response to Draft Report GAO-24-106576, "CYBERSECURITY: Improvements Needed in Addressing Risks to Operational Technology"

Dear Ms. Cain:

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

DHS leadership is pleased to note GAO's positive recognition that almost all of the nonfederal entities included in this review cited examples of positive experiences with Cybersecurity and Infrastructure Security Agency's (CISA) operational technology (OT) products and services. As the lead federal agency responsible for helping critical infrastructure owners and operators address cyber risks to OT, CISA stands ready to help organizations build effective resilience through collaboration, products, and services. Many of CISA's best practices for OT systems have been incorporated into its Cybersecurity Performance Goals (CPGs) which are a subset of voluntary cybersecurity practices outlining the highest priority baseline measures critical infrastructure organizations of all sizes can take to protect themselves against cyber threats. CISA also works closely with sector risk management agencies (SRMAs) to help adjust CPGs to specific sectors.

As GAO also recognizes, critical infrastructure organizations using OT assets and control systems face significant and increasing cybersecurity threats from malicious cyber actors seeking to disrupt critical functions. DHS remains committed to collaborating with federal and non-federal entities to protect our nation's critical systems by strengthening customer service and workforce planning efforts to ensure that CISA is optimally positioned to deliver products and services needed to address OT risks.



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

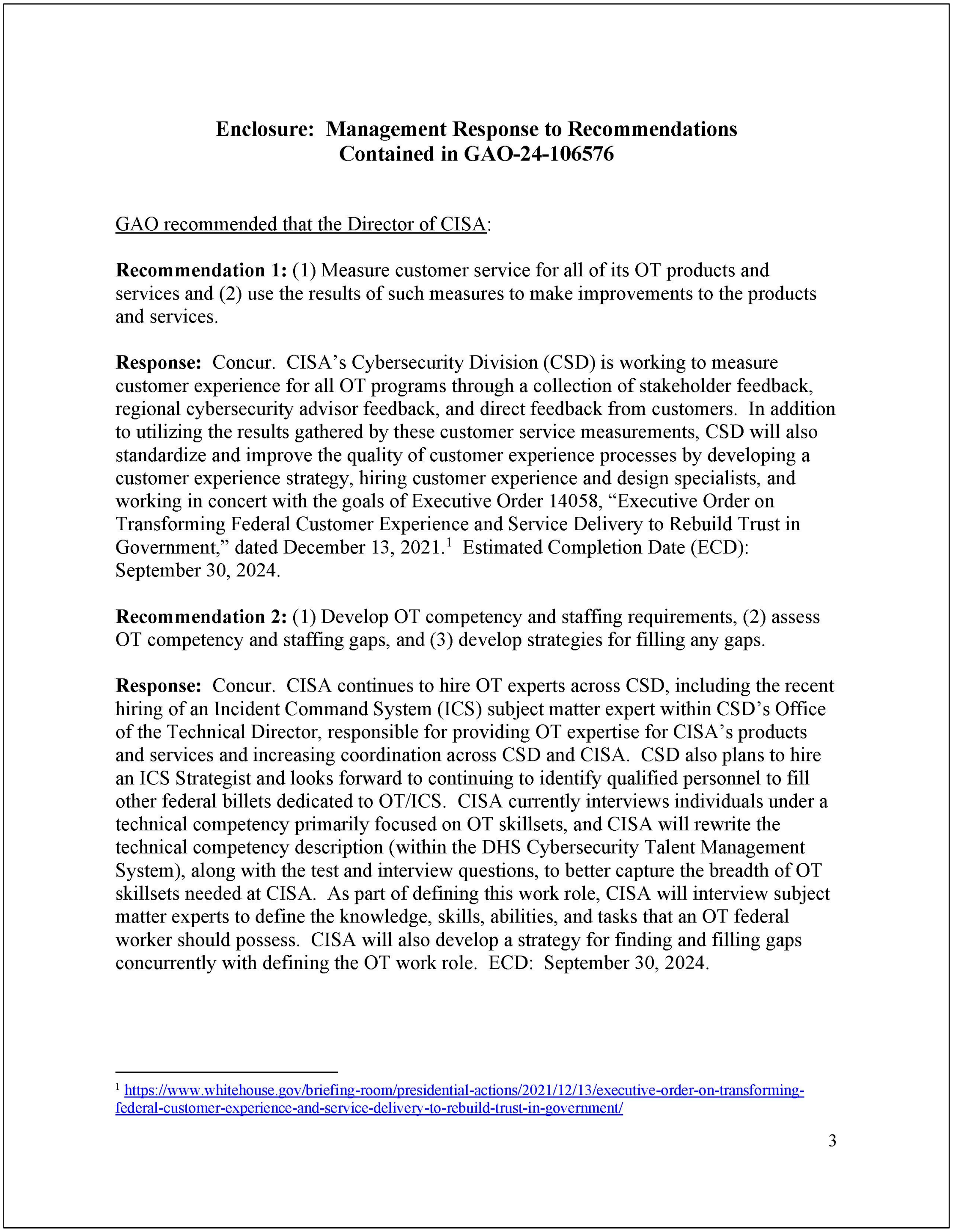
Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2024.01.25 12:28:19 -05'00'

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

Enclosure



Enclosure: Management Response to Recommendations Contained in GAO-24-106576

GAO recommended that the Director of CISA:

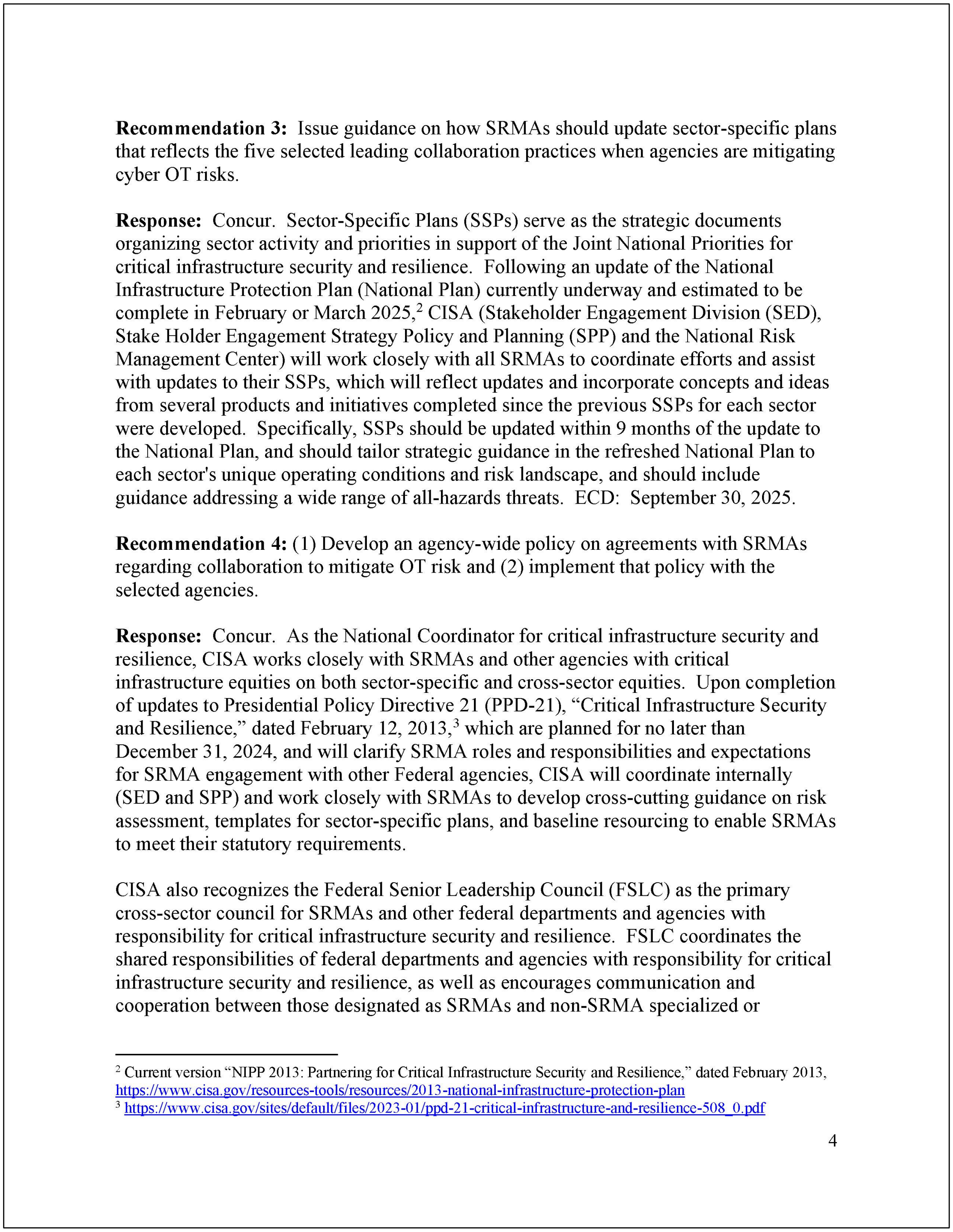
Recommendation 1: (1) Measure customer service for all of its OT products and services and (2) use the results of such measures to make improvements to the products and services.

Response: Concur. CISA's Cybersecurity Division (CSD) is working to measure customer experience for all OT programs through a collection of stakeholder feedback, regional cybersecurity advisor feedback, and direct feedback from customers. In addition to utilizing the results gathered by these customer service measurements, CSD will also standardize and improve the quality of customer experience processes by developing a customer experience strategy, hiring customer experience and design specialists, and working in concert with the goals of Executive Order 14058, "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government," dated December 13, 2021.[1] Estimated Completion Date (ECD): September 30, 2024.

Recommendation 2: (1) Develop OT competency and staffing requirements, (2) assess OT competency and staffing gaps, and (3) develop strategies for filling any gaps.

Response: Concur. CISA continues to hire OT experts across CSD, including the recent hiring of an Incident Command System (ICS) subject matter expert within CSD's Office of the Technical Director, responsible for providing OT expertise for CISA's products and services and increasing coordination across CSD and CISA. CSD also plans to hire an ICS Strategist and looks forward to continuing to identify qualified personnel to fill other federal billets dedicated to OT/ICS. CISA currently interviews individuals under a technical competency primarily focused on OT skillsets, and CISA will rewrite the technical competency description (within the DHS Cybersecurity Talent Management System), along with the test and interview questions, to better capture the breadth of OT skillsets needed at CISA. As part of defining this work role, CISA will interview subject matter experts to define the knowledge, skills, abilities, and tasks that an OT federal worker should possess. CISA will also develop a strategy for finding and filling gaps concurrently with defining the OT work role. ECD: September 30, 2024.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/



Recommendation 3: Issue guidance on how SRMAs should update sector-specific plans that reflects the five selected leading collaboration practices when agencies are mitigating cyber OT risks.

Response: Concur. Sector-Specific Plans (SSPs) serve as the strategic documents organizing sector activity and priorities in support of the Joint National Priorities for critical infrastructure security and resilience. Following an update of the National Infrastructure Protection Plan (National Plan) currently underway and estimated to be complete in February or March 2025,[2] CISA (Stakeholder Engagement Division (SED), Stake Holder Engagement Strategy Policy and Planning (SPP) and the National Risk Management Center) will work closely with all SRMAs to coordinate efforts and assist with updates to their SSPs, which will reflect updates and incorporate concepts and ideas from several products and initiatives completed since the previous SSPs for each sector were developed. Specifically, SSPs should be updated within 9 months of the update to the National Plan, and should tailor strategic guidance in the refreshed National Plan to each sector's unique operating conditions and risk landscape, and should include guidance addressing a wide range of all-hazards threats. ECD: September 30, 2025.

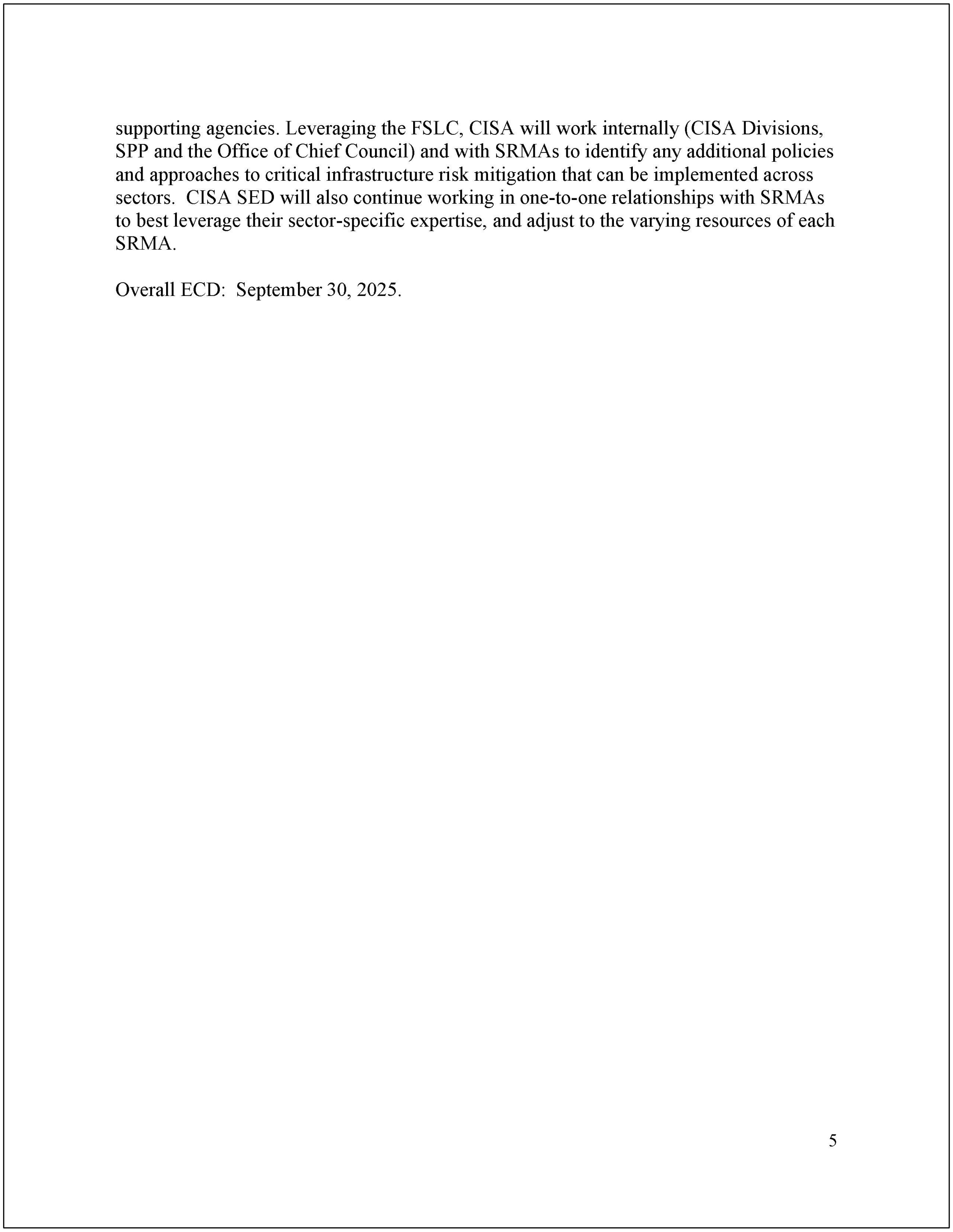
Recommendation 4: (1) Develop an agency-wide policy on agreements with SRMAs regarding collaboration to mitigate OT risk and (2) implement that policy with the selected agencies.

Response: Concur. As the National Coordinator for critical infrastructure security and resilience, CISA works closely with SRMAs and other agencies with critical infrastructure equities on both sector-specific and cross-sector equities. Upon completion of updates to Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," dated February 12, 2013,[3] which are planned for no later than December 31, 2024, and will clarify SRMA roles and responsibilities and expectations for SRMA engagement with other Federal agencies, CISA will coordinate internally (SED and SPP) and work closely with SRMAs to develop cross-cutting guidance on risk assessment, templates for sector-specific plans, and baseline resourcing to enable SRMAs to meet their statutory requirements.

CISA also recognizes the Federal Senior Leadership Council (FSLC) as the primary cross-sector council for SRMAs and other federal departments and agencies with responsibility for critical infrastructure security and resilience. FSLC coordinates the shared responsibilities of federal departments and agencies with responsibility for critical infrastructure security and resilience, as well as encourages communication and cooperation between those designated as SRMAs and non-SRMA specialized or

[2] Current version "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," dated February 2013, https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan

[3] https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf



supporting agencies. Leveraging the FSLC, CISA will work internally (CISA Divisions, SPP and the Office of Chief Council) and with SRMAs to identify any additional policies and approaches to critical infrastructure risk mitigation that can be implemented across sectors. CISA SED will also continue working in one-to-one relationships with SRMAs to best leverage their sector-specific expertise, and adjust to the varying resources of each SRMA.

Overall ECD: September 30, 2025.

Accessible Text for Appendix II: Comments from the Department of Homeland Security

January 25, 2024

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106576, “CYBERSECURITY: Improvements Needed in Addressing Risks to Operational Technology”

Dear Ms. Cain:

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

DHS leadership is pleased to note GAO's positive recognition that almost all of the nonfederal entities included in this review cited examples of positive experiences with Cybersecurity and Infrastructure Security Agency's (CISA) operational technology (OT) products and services. As the lead federal agency responsible for helping critical infrastructure owners and operators address cyber risks to OT, CISA stands ready to help organizations build effective resilience through collaboration, products, and services.Many of CTSA's best practices for OT systems have been incorporated into its Cybersecmity Perfotmance Goals (CPGs) which are a subset of voluntary cybersecurity practices outlining the highest priority baseline measures critical infrastructure organizations of all sizes can take to protect themselves against cyber threats. CISA also works closely with sector risk management agencies (SRMAs) to help adjust CPGs to specific sectors.

As GAO also recognizes, critical infrastrncture orgmtizations using OT assets and control systems face significant and increasing cybersecurity threats from malicious cyber actors seeking to disrupt critical functions. DHS remains committed to collaborating with federal and non-federal entities to protect our nation's critical systems by strengthening customer service and workforce planning efforts to ensure that CTSA is optimally positioned to deliver products and services needed to address OT risks.

The draft report contains four recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO'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.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2024.01.25 12:28:19 -05'00'

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

Enclosure

Enclosure: Management Response to Recommendations Contained in GA0-24-106576

<u>GAO recommended that the Director of CISA</u>:

Recommendation 1: (1) Measure customer service for all of its OT products and services and (2) use the results of such measures to make improvements to the products and services.

Response: Concur. CISA's Cybersecurity Division (CSD) is working to measure customer experience for all OT programs through a collection of stakeholder feedback, regional cybersecurity advisor feedback, and direct feedback from customers. In addition to utilizing the results gathered by these customer service measurements, CSD will also standardize and improve the quality of customer experience processes by developing a customer experience strategy, hiring customer experience and design specialists, and working in concert with the goals of Executive Order 14058, “Executive Order on Transforming Federal Customer

Experience and Service Delivery to Rebuild Trust in Govenunent," dated December 13, 2021.[1] Estimated Completion Date (ECD): September 30, 2024.

Recommendation 2: (1) Develop OT competency and staffing requirements, (2) assess OT competency and staffing gaps, and (3) develop strategies for filling any gaps.

Response: Concur. CISA continues to hire OT experts across CSD, including the recent hiring of an Incident Command System (ICS) subject matter expert within CSD's Office of the Technical Director, responsible for providing OT expertise for CISA's products and services and increasing coordination across CSD and CISA. CSD also plans to hire an ICS Strategist and looks forward to continuing to identify qualified personnel to fill other federal billets dedicated to OT/ICS. CISA currently interviews individuals under a teclmical competency primarily focused on OT skillsets, and CISA will rewrite the technical competency description (within the DHS Cybersecurity Talent Management System), along with the test and interview questions, to better capture the breadth of OT skillsets needed at CISA. As part of defining this work role, CISA will interview subject matter experts to define the knowledge, skills, abilities, and tasks that an OT federal worker should possess. CISA will also develop a strategy for finding and filling gaps concurrently with defining the OT work role. ECD: September 30, 2024.

Recommendation 3: Issue guidance on how SRMAs should update sector-specific plans that reflects the five selected leading collaboration practices when agencies are mitigating cyber OT risks.

Response: Concur. Sector-Specific Plans (SSPs) serve as the strategic documents organizing sector activity and priorities in support of the Joint National Priorities for critical infrastructure security and resilience. Following an update of the National Infrastructure Protection Plan (National Plan) currently underway and estimated to be complete in February or March 2025,[2] CISA (Stakeholder Engagement Division (SED), Stake Holder Engagement Strategy Policy and Planning (SPP) and the National Risk Management Center) will work closely with all SRMAs to coordinate efforts and assist with updates to their SSPs, which will reflect updates and incorporate concepts and ideas from several products and initiatives completed since the previous SSPs for each sector were developed. Specifically, SSPs should be

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

[2] Current version "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," dated February 2013, https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan

updated within 9 months of the update to the National Plan, and should tailor strategic guidance in the refreshed National Plan to each sector's unique operating conditions and risk landscape, and should include guidance addressing a wide range of all-hazards threats. ECO: September 30, 2025.

Recommendation 4: (1) Develop an agency-wide policy on agreements with SRMAs regarding collaboration to mitigate OT risk and (2) implement that policy with the selected agencies.

Response: Concur. As the National Coordinator for critical infrastructure security and resilience, CISA works closely with SRMAs and other agencies with critical infrastructure equities on both sector-specific and cross-sector equities. Upon completion of updates to Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," dated February 12, 2013,[3] which are planned for no later than December 31, 2024, and will clarify SRMA roles and responsibilities and expectations for SRMA engagement with other Federal agencies, CTSA will coordinate internally (SEO and SPP) and work closely with SRMAs to develop cross-cutting guidance on risk assessment, templates for sector-specific plans, and baseline resourcing to enable SRMAs to meet their statutory requirements.

CISA also recognizes the Federal Senior Leadership Council (FSLC) as the primary cross-sector council for SRMAs and other federal departments and agencies with responsibility for critical infrastructure security and resilience. FSLC coordinates the shared responsibilities of federal departments and agencies with responsibility for critical infrastructure security and resilience, as well as encourages communication and cooperation between those designated as SRMAs and non-SRMA specialized or supporting agencies. Leveraging the FSLC, CISA will work internally (CISA Divisions, SPP and the Office of Chief Council) and with SRMAs to identify any additional policies and approaches to critical infrastructure risk mitigation that can be implemented across sectors. CTSA SED will also continue working in one-to-one relationships with SRMAs to best leverage their sector-specific expertise, and adjust to the varying resources of each SRMA.

Overall ECD: September 30, 2025.

[3] https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastrtructure-and-resilience-508_0.pd[

Appendix III: Detailed Summary of CISA's Three Retired OT Cybersecurity Products and Services

The Cybersecurity and Infrastructure Security Agency (CISA) has retired three operational technology (OT) cybersecurity products and services since October 2018. Specifically:

- **Industrial control system alerts.** These alerts were intended to notify critical infrastructure owners and operators of cyber threats facing OT systems. CISA has issued six such alerts since becoming an agency in 2018. For example, in July 2019, CISA published an alert regarding the insecure implementation of certain networks impacting aircraft and how this vulnerability could be exploited.[1] In October 2023, a CISA official told us that the agency has retired its industrial control system-specific alerts product. This official explained that the agency plans to use its broader cybersecurity "alerts" product to describe any threats facing OT systems.
- **Industrial Control Systems Joint Working Group.** CISA used this group to facilitate information sharing and reduce the risk to the nation's OT. According to CISA, the working group was comprised of over 200 organizations representing all 16 critical infrastructure sectors, including all levels of government organizations, critical infrastructure owners and operators, vendors, and academic professionals. The working group's activities included in-person meetings, webinars, and newsletters.

CISA retired this group in August 2023 and intends to integrate aspects of its mission into the Joint Cyber Defense Collaborative Industrial Control Systems group. CISA added that it will continue to explore additional opportunities for former Industrial Control Systems Joint Working Group members to engage in Joint Cyber Defense Collaborative activities. For

[1] CISA, *ICS Alert: CAN Bus Network Implementation in Avionics*, ICS-ALERT-19-211-01 (July 30, 2019).

example, the collaborative is considering hosting an annual industrial control systems/OT conference in the second half of 2024.

- **Technical analysis.** CISA's industrial control systems advanced malware laboratory analyzed OT specific hardware and digital media to determine whether they have been compromised by malware. After identifying malware samples, CISA could analyze the malware to, among other things, learn more about the tactics, techniques, and procedures of cyber threat actors and identify associated mitigations. According to CISA, the advanced malware laboratory, which was hosted by Idaho National Laboratory, was retired and the contract for the dedicated industrial controls systems malware analysis capability was terminated.[2]

[2] According to CISA officials, the agency can continue to conduct limited industrial control systems malware analysis using an emulated OT environment and two employees with OT certifications.

Appendix IV: Detailed Summary of CISA's Joint Cyber Defense Collaborative Operational Technology Group

In April 2022, the Cybersecurity and Infrastructure Security Agency (CISA) expanded the Joint Cyber Defense Collaborative to include selected operational technology (OT) vendors, integrators, and distributors with the goal of leveraging their collective expertise to improve CISA's other products and services.[1] CISA explained that the group of partners helps the agency to build plans around the protection and defense of OT, inform U.S. government guidance on OT cybersecurity, and contribute to real time operational fusion across private and public partners in the OT space. For example, CISA officials told us that the collaborative's OT group provided input on a fact sheet from CISA, the Federal Bureau of Investigation, the National Security Agency, and the U.S. Department of the Treasury on improving the security of open source software in OT.

According to CISA officials, the collaborative does not have any staff permanently placed into its OT group. However, the officials added there are six federal employees and several contractor staff who support the collaborative's OT group.[2]

Five of the 13 selected nonfederal entities described positive experiences working with the Joint Cyber Defense Collaborative. For example, one nonfederal entity told us that the OT group focused on open source security in OT and it was a unique effort that brought stakeholders together to address this complex and highly impactful issue. Another

[1] CISA established the Joint Cyber Defense Collaborative as a joint cyber planning office pursuant to statutory requirement to establish an office to develop cyber defense operations for the public and private sectors. 6 U.S.C. §665b.

[2] CISA officials noted they are working to establish a contract vehicle that will be solely dedicated to this mission area in the future. They are also currently working to staff one full-time federal position that will be dedicated to the Joint Cyber Defense Collaborative's OT group. In addition, CISA could not provide obligation or expenditures information for the OT group because OT support is not identified as a separate budget item.

entity noted that it received actionable intelligence from the OT group in relation to Russia's invasion of Ukraine.

In addition, CISA and four nonfederal entities identified challenges with operating or working with the OT group:

- CISA officials identified two challenges pertaining to Joint Cyber Defense Collaborative.
    - CISA officials explained that some members of the OT community are hesitant about sharing concerns about OT issues in a forum such as a conference or meeting.
    - CISA officials told us that the collaborative's participants do not have expertise in all sectors that use OT. Those officials explained that not all members of the Joint Cyber Defense Collaborative's OT group are involved in every sector, and there are some that are only involved as specialists in specific sectors.
- Five selected nonfederal entities identified four challenges in working in the Joint Cyber Defense Collaborative's OT group.
    - Three nonfederal entities told us that industry participants do not always have the time or resources to participate in the collaborative's activities.
    - One nonfederal entity explained that some members stopped participating in the group because they thought the topics being discussed were too "high-level" and aimed at pleasing too many stakeholders.
    - One nonfederal entity explained that the group does not have any representation from critical infrastructure owners and operators.
    - One nonfederal entity stated that it was challenging to receive timely information from the group. That entity added that it would be beneficial if CISA could accelerate its process for reporting information to group participants.

Appendix V: Detailed Summary of CISA's Four OT Cybersecurity Products

The Cybersecurity and Infrastructure Security Agency (CISA) has provided four operational technology (OT) cybersecurity products to critical infrastructure owners and operators at no cost to those owners and operators. Two of these products are intended to share cyber threat information and best practices pertaining to OT:

- CISA's **industrial control system advisories** provide information about OT security issues, vulnerabilities, and exploits. As of November 2023, CISA has issued nearly 1,500 advisories since becoming an agency in 2018.[1] For example, in September 2023, CISA issued an advisory on a vulnerability that, if exploited, could allow a malicious actor to carry out a remote denial-of-service attack[2] on certain products without authentication (e.g., providing credentials for an authorized user).[3] CISA makes these advisories available on its public website.[4]
- CISA's **industrial control systems best practice guidance** describes practices that critical infrastructure owners and operators can use to address cyber risks facing their OT networks. CISA has published three guides on industrial control systems best practices since 2018.[5] For example, in September 2022 CISA and the National Security Administration published guidance describing tactics, techniques, and procedures that malicious actors use to compromise

[1] A CISA official estimated that approximately 99 percent of the advisories are OT-related.

[2] A denial-of-service attack prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

[3] CISA, *ICS Advisory*, Siemens SIMATIC, SIPLUS Products, ICSA-23-257-01 (Sept. 14, 2023).

[4] As discussed later in this report, the vulnerability coordination service culminates in these advisories. For more information on staffing and spending on this service and product, see the discussion of the coordinated vulnerability disclosure service in appendix V.

[5] A CISA official noted that best practice guidance for OT systems is also incorporated into the cross-sector cybersecurity performance goals. CISA, *Cross-Sector Cybersecurity Performance Goals* (March 2023).

OT systems, and mitigations that owners and operators can use to defend their systems.[6] CISA makes this best practice guidance available on its public website.[7]

The remaining two OT products are tools that critical infrastructure owners and operators can use to evaluate OT security practices and analyze OT network traffic and logs:

- The **Cyber Security Evaluation Tool (CSET®)** is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate OT and IT network security practices. CSET is available for download on CISA's GitHub repository.[8] According to CISA officials, CSET was downloaded 91,305 times between October 2018 and November 2023. The agency relied on one federal employee and roughly three and a half full-time equivalent contract employees from Idaho National Laboratory to maintain the product and help owners and operators to perform facilitated assessments using the tool.[9] In November 2023, CISA officials stated that the agency has expended between $12.6 and $13.9 million on CSET since 2018.
- **Malcolm** is a set of open source tools that enables the user to capture and analyze OT network traffic and logs. CISA makes Malcolm available for download on the agency's GitHub repository.[10] In November 2023, CISA officials told us that Malcolm was downloaded at least 48,000 times across several repositories since the product's initial release in June 2019.[11] CISA officials also told us that the

[6] NSA and CISA, *Control System Defense: Know the Opponent* (September 2022).

[7] As discussed earlier in this report, the Joint Cyber Defense Collaborative helps to develop guides like these. For more information on staffing and spending on this collaborative, see appendix IV.

[8] https://github.com/cisagov/cset. GitHub is a web-based software repository hosting service.

[9] In November 2023, CISA officials stated that CSET is fully staffed and does not have any vacancies.

[10] https://github.com/cisagov/Malcolm.

[11] CISA also explained that this number is based on incomplete data and should not be considered definitive. Those officials added that it is difficult to track "downloads" for a variety of reasons; for example, there are different ways to acquire the source code and download project files.

agency has obligated about $1.3 million for the product for fiscal years 2021 through 2023 and expended about $1 million.[12]

[12] Although the project began in fiscal year 2019, CISA officials explained that they were not able to provide funding data for fiscal years 2019 and 2020 because the project was in its early stages and the funding was included in other funding streams.

Appendix VI: Detailed Summary of CISA's Nine OT Cybersecurity Services

The Cybersecurity and Information Security Agency (CISA) has provided nine operational technology (OT) cybersecurity services to critical infrastructure owners and operators at no cost. Four of the services are aimed at helping owners and operators to identify cyber vulnerabilities in their OT networks and steps that can be taken to mitigate them:

- **Strategic risk analysis.** According to CISA, this service develops resources to manage risk facing OT systems, among others. CISA officials stated that the agency develops public resources as part of government initiative (e.g., an executive order or congressional direction).[1] For example, CISA published a resource in August 2022 that highlighted issues and strategies OT owners and operators should consider related to post-quantum cryptography.[2] CISA officials added that the amount of employees and contractor staff needed to deliver the service varies widely depending on the hazard being evaluated.[3]
- **Validated architecture design reviews.** These reviews are intended to evaluate an organization's systems, networks, and security services—including those related to OT—to determine if they are designed, built, and operated in a reliable and resilient manner. According to CISA, these reviews consist of three separate

[1] CISA officials stated that the primary focus of strategic risk analysis is across critical infrastructure sectors and is hazard driven, but the National Risk Management Center has conducted specific pipeline analyses and is planning on conducting sector-specific risk analyses in the future.

[2] CISA, *CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography* (available at https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf). Post-quantum cryptography refers to encryption methods that are intended to withstand attacks from future quantum computers that could break certain current encryption methods.

[3] CISA officials explained that they could not provide information on how much the agency expended to deliver this service because the amount cannot be disaggregated from the amounts used to fund other services that the same employees and contractor staff provide.

assessments: a network architecture review, a system configuration and log review, and a network traffic analysis.

Since the agency began tracking them in August 2019, CISA has completed 125 of the 572 OT-related requests for these reviews. CISA conducted these reviews for critical infrastructure owners and operators within the following 10 sectors: Chemical, Commercial Facilities, Critical Manufacturing, Dams, Energy, Government Facilities, Healthcare and Public Health, IT, Transportation Systems, Water and Wastewater Systems.

CISA reported that it expended nearly $7.9 million to conduct these reviews from February 2020 through June 2023.[4] In addition, as of July 2023, CISA utilized 10 federal staff and five contractor staff in support of this service.[5]

- **Vulnerability coordination.** According to CISA, the agency's Coordinated Vulnerability Disclosure program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services—including those relating to OT—with the affected vendor(s). The goal of the program is to ensure that the vulnerability reporter (e.g., security researcher that first identified a vulnerability) publicly discloses the existence of the vulnerability simultaneously with the affected vendor or service provider. When performed effectively, this simultaneous disclosure allows the vendor or service provider to give users clear and actionable information on how to address the vulnerability while reducing the ability of malicious actors to exploit the vulnerability.

  As discussed in more detail earlier in this report, this service culminates in CISA's publication of industrial control systems-related vulnerability advisories. As of November 2023, CISA has issued over 1,500 advisories since becoming an agency in 2018. According to CISA, as of October 2023 the agency relied on four federal staff and

[4] CISA officials explained that they were not able to provide expenditures for 2018 and 2019 because the current lead official for this service does not have access to financial reports for this period.

[5] As of November 2023, CISA officials told us that all but one of the 10 federal positions was filled.

10 contractor staff to provide this service.[6] As of November 2023, the agency did not have any vacancies for this service.

- **Administrative subpoena for vulnerability notification.** CISA seeks to warn critical infrastructure owners and operators of vulnerabilities in internet connected systems that may be exploited by threat actors using its administrative subpoena authority. To identify systems that may be vulnerable, CISA uses internal and open source tools, such as the search engine Shodan.[7] In cases where CISA does not know the owner of a vulnerable system, CISA uses its authority to issue administrative subpoenas to obtain information necessary to proactively identify and notify an entity at risk.[8] This authority applies when CISA identifies a system connected to the internet with a specific security vulnerability and has reason to believe the security vulnerability relates to critical infrastructure and affects a covered device or system but is unable to identify the entity at risk.

  CISA received administrative subpoena authority in January 2021 and did not issue its first subpoena until April 2021. According to CISA's Calendar Year 2021 *Administrative Subpoena for Vulnerability Notification Year in Review*, between April and December 2021, CISA issued 47 administrative subpoenas to identify owners or operators of a total of 221 vulnerable OT devices.[9] From the responses to the administrative subpoenas, CISA was able to identify 67 owners or operators for 155 out of the total 221 vulnerable OT devices. Of the 67 owners or operators that CISA notified, 22 entities did not respond to the notification, 40 entities acknowledged receipt of the notification but did not engage further with CISA, two entities acknowledged receipt of the notification and stated that they mitigated the vulnerability, and one entity denied ownership of the device.

[6] CISA officials explained that they could not provide information on how much CISA expended to deliver this service and advisories because the amount cannot be disaggregated from the amounts used to fund other services that the same employees and contractors provide.

[7] Shodan is a web-based search, accessible to both cyber defenders and threat actors, that can query for internet-connected assets.

[8] 6 U.S.C. § 659(p).

[9] CISA, *CY2021 Administrative Subpoena for Vulnerability Notification Year in Review* (available at *https://www.cisa.gov/sites/default/files/2023-01/CY2021_Admin_Subpoena_Summary_Factsheet_FINAL.pdf*). According to this document, these 221 devices span 13 unique types of vulnerable devices.

According to CISA's Calendar Year 2022 *Administrative Subpoena for Vulnerability Notification Year in Review*, between January 1, 2022, and December 31, 2022, CISA issued 122 administrative subpoenas to identify owners or operators of a total of 544 vulnerable OT devices in calendar year 2022.[10]

Three services are aimed at providing critical infrastructure owners and operators with training, exercises, and other information needed to prepare for cyberattacks on their OT networks:

- **Control Environment Laboratory Resource.** According to CISA, the goal of this resource is to allow stakeholders (including critical infrastructure owners and operators) to practice a variety of cybersecurity activities in an OT environment, such as incident response, threat hunting, and tool evaluation.[11] This resource can be provided either remotely or in-person.[12] CISA officials stated the agency used this resource to conduct exercises with two critical infrastructure entities between October 1, 2021, and September 30, 2023.[13] According to CISA, the agency utilizes four federal staff and seven contractor staff in support of this service. As of November 2023, the agency did not have any vacancies to support this service. CISA officials also told us that the agency has obligated about $19.1 million for the product for fiscal years 2021 through 2023 and expended about $19.6 million.[14]

[10] CISA, *CY2022 Administrative Subpoena for Vulnerability Notification Year in Review* (available at https://www.cisa.gov/sites/default/files/2023-12/CY2022-Administrative-Subpoena-for-Vulnerability-Notification-Year-in-Review-508c.pdf). CISA officials added that these 544 devices span 25 unique types of vulnerable devices.

[11] CISA officials stated that the agency partners with the following laboratories to deliver this resource: Idaho National Laboratory, Pacific Northwest National Laboratory, and John's Hopkins Applied Physics Laboratory.

[12] According to CISA, onsite simulated services enable teams to see the impact of a cyberattack on the physical equipment, as well as interact directly with the emulated adversary.

[13] CISA was unable to identify how many requests it has received since 2018 for this service. CISA officials explained that this is a new and emerging capability that has been solicited through leadership priorities or through collaboration with private sector partners.

[14] Although the project began in fiscal year 2019, CISA officials explained that they were not able to provide funding data for fiscal years 2019 and 2020 because the project was in its early stages and the funding was included in other funding streams. Additionally, CISA officials explained that they do not receive the level of dedicated funding they believe is necessary to increase the service offerings related to the Control Environment Laboratory Resource service and to grow the number of external participants.

- **Exercises.** CISA provides cyber exercise planning to support critical infrastructure partners—including those using OT—by delivering various types of cyber exercises. According to CISA, these can range from small discussion-based exercises that last 2 hours to internationally scoped exercises that can span multiple days.[15] These events can be used to assist organizations in the development and testing of their cybersecurity protection, mitigation, and response capabilities. In addition, CISA also provides Tabletop Exercise packages to assist partner organizations in developing their own tabletop exercises to assess information sharing processes and emergency plans.

  According to CISA, the agency conducted approximately 66 exercises involving OT from fiscal years 2019 through 2023 and the following sectors participated in these exercises: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Energy, Financial Services, Healthcare and Public Health, IT, Transportation Systems, and Water and Wastewater Systems.

  According to CISA, as of November 2023 the agency relied on 20 federal employees to deliver the National Cyber Exercise Program. CISA officials added that none of those staff are assigned full-time to delivering OT exercises or developing OT-focused exercises. The program is also supported with 30 full-time equivalent contractor staff. Further, CISA officials told us that, although they do not track costs for OT-specific exercises, the agency estimated that the average cost of a single tabletop exercise is approximately $80,000, depending on the scope and complexity of the exercise.

- **Training.** CISA provides OT cybersecurity training with online and in-person offerings. Specifically, CISA offers 13 web-based OT cybersecurity courses available on-demand.[16] In addition, CISA offers two courses that are taught by instructors virtually and that are made available each month. Lastly, CISA offers five instructor-led OT cybersecurity courses that are available in-person at either Idaho National Laboratory or various regions across the country. Two of these five courses include technical hands-on activities, such as day-

[15] For example, in March 2022 CISA conducted Cyber Storm VIII—a 3 day exercise involving over 2,000 participants from the cyber incident response community, aimed at encouraging the advancement of public-private partnerships within the critical infrastructure sectors; and strengthening the relationship between the federal government and its government partners at the state, local, and international levels.

[16] https://ics-training.inl.gov/learn.

long exercises where trainees are either attacking or defending IT and OT networks.

According to CISA data, as of September 2023, CISA's on-demand OT courses were completed 135,157 times and 6,121participants have completed CISA's instructor-led courses since fiscal year 2018. As of July 2023, CISA relied on between 12 and 14 contractor staff to deliver this.[17]

Two of CISA's services are aimed at helping to identify, analyze, or respond to malicious cyber activity on owner and operator OT networks:

- **CyberSentry** is a voluntary program that leverages hardware and software capabilities to identify malicious activity on critical infrastructure OT systems. After deploying these capabilities, CISA analyzes critical infrastructure partner networks for potential threats.[18] If CISA analysts find any cybersecurity concerns, the agency: (1) notifies the critical infrastructure partner; (2) works with them to help resolve the concern; and (3) if necessary, and if requested, can deploy resources to provide additional support. CISA makes this product available to a limited set of critical infrastructure participants who own and operate significant IT and OT systems that align with associated national critical functions.[19]

  A CISA official stated that as of November 2023, CyberSentry had been deployed to 29 partners representing various critical infrastructure sectors. Specifically, 28 of the CyberSentry partners represent seven of the 16 following critical infrastructure sectors: (1) Energy, (2) Healthcare and Public Health, (3) Water and Wastewater

[17] According to CISA, there is a functional lead stationed at Idaho National Laboratory. In addition, there are nine contracted instructors supported by three to five staff (including instructional designers and administrative personnel). We also asked CISA for information on how much CISA has obligated or expended on this service. We did not receive a response to this request in time for inclusion in our draft report. In addition, CISA officials explained that their funding is limited to the events defined in annual plans. The officials explained that this limits flexibility in the use of the funds and restricts their ability to address ad-hoc event requests.

[18] CyberSentry collects network traffic, including metadata and the full content of network communications, and compares that information against signatures and baseline network traffic in order identify malicious traffic. When a signature for a known or suspected cyber threat triggers an alert or the data flow significantly skews from the baseline, a predetermined amount of associated traffic that is analytically relevant to the potential threat is reviewed by a CyberSentry analyst.

[19] In 2019, CISA published its initial set of 55 National Critical Functions. https://www.cisa.gov/national-critical-functions-set.

Systems, (4) Nuclear Reactors, Materials, and Waste, (5) Communications, (6) Government Facilities, and (7) Transportation Systems. According to CISA, the remaining partner represented multiple sectors.

According to CISA, as of November 2023 the CyberSentry Program Management Office relied on 21 full-time equivalent positions and did not have any vacancies for the service. As of July 2023, CISA stated that it has obligated over $138 million and expended over $111 million on CyberSentry since October 2018.

- **Threat hunting and incident response.** CISA's Cyber Physical Forensics team is specifically focused on identifying sophisticated threats and adversary presence in OT and IT environments. Critical infrastructure owners and operators typically seek this team's assistance in threat hunting when they believe a threat actor may have gained initial access, but before that compromise has resulted in an adverse impact (e.g., incident). By contrast, owners and operators request incident response assistance from this team when they believe that a threat actor has caused an adverse impact on their network—such as a ransomware attack. In both cases, CISA's Cyber Physical Forensics team collects and analyzes data remotely or in-person and helps to identify possible steps that can be taken to remediate or mitigate cyber threats.

  CISA officials stated that the agency provided OT specific threat hunting and/or incident response services to eight entities since the agency started tracking OT-specific requests for this service in October 2021. Specifically, CISA has provided these services to three Transportation Systems sector entities, three Water and Wastewater Systems sector entities, one Communications sector entity, and one Government Facilities sector entity. According to CISA, as of July 2023, it relied on two federal staff and five contractor staff in support of this service. As of November 2023, there are two vacancies for this service.[20]

[20] We also asked CISA for information how much has CISA obligated or expended on this service. According to a CISA official, the agency is unable to provide OT-specific funding data because it did not separate funding for IT and OT threat hunting and incident response operations.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, (202) 512-5017 or CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Kaelin Kuhn (Assistant Director), David Matcham (Analyst-In-Charge), Bradley Becker, Christopher Businsky, Jillian Clouse, Rebecca Eyler, Anthony Gray, Franklin Jackson, Smith Julmisse, Ashley Mattson, and Andrew Stavisky made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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