



September 2023

CRITICAL INFRASTRUCTURE PROTECTION

National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods

Accessible Version

Why GAO Did This Study

Cyber threats to the nation’s critical infrastructure sectors are significant. As such, it is important that federal agencies and critical infrastructure owners and operators share cyber threat information. ONCD and CISA lead federal efforts to coordinate on national cyber policy and the security of critical infrastructure.

This report examines, among other things, (1) how federal agencies and critical infrastructure owners and operators share cyber threat information and (2) challenges to cyber threat information sharing and the extent to which federal agencies have taken action to address them.

To do so, GAO reviewed documentation from 14 federal agencies, including CISA, and seven nonfederal entities with responsibility for sharing cyber threat information. In addition, GAO interviewed relevant officials from these federal agencies and nonfederal entities regarding challenges to sharing cyber threat information.

Using information compiled from interviews, GAO then presented the cyber threat information challenges frequently identified by the relevant entities to the 14 federal agencies and ONCD. GAO also asked for and reviewed documentation on actions the 14 agencies and ONCD have taken or plan to take to address the challenges.

In addition, GAO compared the *National Cybersecurity Strategy* and accompanying implementation plan with its prior work on leading practices for national strategies and business process reengineering.

View [GAO-23-105468](#). For more information, contact Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov or Tina Won Sherman at (202) 512-8461 or ShermanT@gao.gov.

CRITICAL INFRASTRUCTURE PROTECTION

National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods

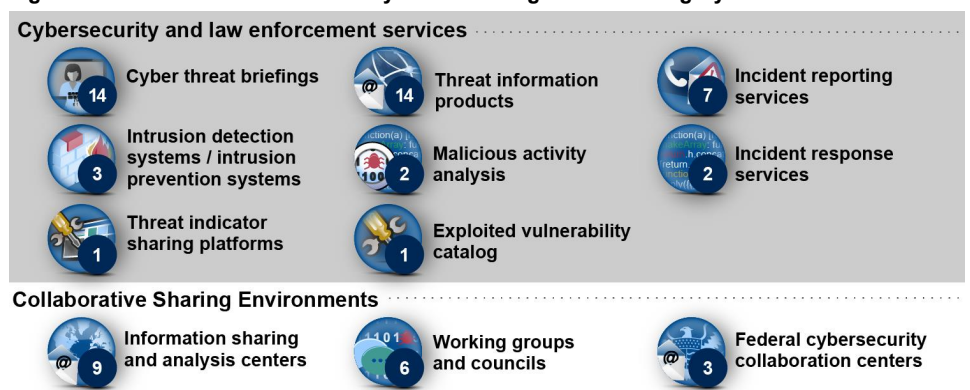
What GAO Found

The nation’s 16 critical infrastructure sectors rely on electronic systems to provide essential services such as electricity, communications, and financial services. Federal entities have key roles in helping to protect these sectors.

- The Office of the National Cyber Director (ONCD) is to advise the President on cybersecurity policy and strategy, and lead the coordination of implementation of the March 2023 *National Cybersecurity Strategy*.
- The Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is to coordinate the overall federal effort to promote the security of the nation’s critical infrastructure, including the sharing of threat information.
- The FBI is to lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors and share related cyber threat information.
- CISA and 12 other agencies are sector risk management agencies responsible for providing specialized expertise for protecting the cybersecurity of their assigned sectors (e.g., Department of Energy and the energy sector), to include the sharing of sector-specific threat information.

The 14 federal agencies in GAO’s review—CISA, FBI, and the other 12 sector risk management agencies—reported relying on 11 methods to facilitate sharing of cyber threat information with critical infrastructure owners and operators. As shown in figure 1, these agencies used each of the 11 methods to varying degrees (see the numbers next to each method).

Figure 1: Number of Methods Used by 14 Federal Agencies Sharing Cyber Threat Information



Sources: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-23-105468

Accessible Data for Figure 1: Number of Methods Used by 14 Federal Agencies Sharing Cyber Threat Information

Category	Subcategory	Subcategory total
Cybersecurity and law enforcement services	Cyber threat briefings	14
Cybersecurity and law enforcement services	Intrusion detection systems / intrusion prevention systems	3

CRITICAL INFRASTRUCTURE PROTECTION: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods

Category	Subcategory	Subcategory total
Cybersecurity and law enforcement services	Threat indicator sharing platforms	1
Cybersecurity and law enforcement services	Threat information products	14
Cybersecurity and law enforcement services	Malicious activity analysis	2
Cybersecurity and law enforcement services	Exploited vulnerability catalog	1
Cybersecurity and law enforcement services	Incident reporting services	7
Cybersecurity and law enforcement services	Incident response services	2
Collaborative sharing environments	Information sharing and analysis centers	9
Collaborative sharing environments	Working groups and councils	6
Collaborative sharing environments	Federal cybersecurity collaboration centers	3

Sources: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-23-105468

The 14 agencies varied in the number of information sharing methods that they each used. Specifically, four agencies—the Department of Defense, the Department of Energy, CISA, and FBI—used more than half of the 11 sharing methods and 10 agencies used fewer than half of the 11 sharing methods.

The agencies took two different approaches to using the 11 sharing methods. Specifically, two agencies—CISA and FBI—used a centralized approach to share information with each of the 16 critical infrastructure sectors. The other 12 remaining federal agencies shared sector-specific threat information.

What GAO Recommends

GAO is recommending that:

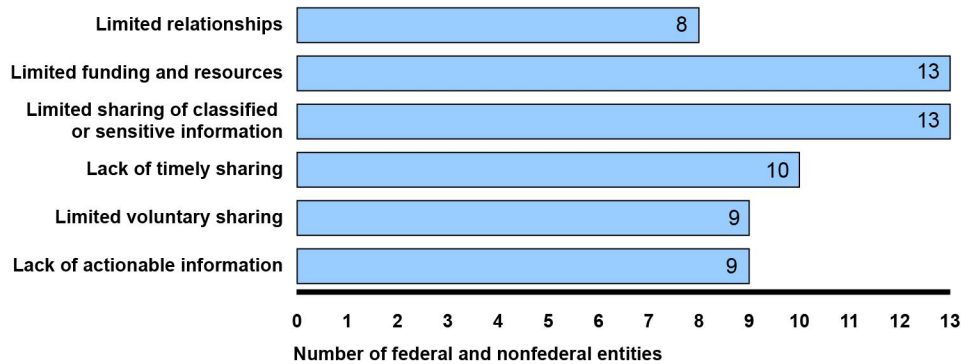
- (1) ONCD identify outcome-oriented performance measures for the cyber threat information sharing initiatives included in the *National Cybersecurity Strategy* implementation plan, and
- (2) CISA assess whether the current mix of centralized and sector-specific sharing methods used by agencies is the optimal approach to addressing cyber threat sharing challenges.

In commenting on a draft of this report, ONCD agreed with GAO’s finding on outcome-oriented measures but disagreed with the recommendation. As discussed in the report, GAO continues to believe that this recommendation is necessary to evaluate the effectiveness of planned efforts. Based on additional contextual information provided by ONCD, GAO withdrew from its report one recommendation on voluntary and timely information sharing.

DHS concurred with the recommendation to CISA.

Six challenges to effective sharing of cyber threat information were identified by at least a third of the 21 entities in GAO’s review (14 federal agencies and seven nonfederal entities) (see figure 2).

Figure 2: Six Challenges to Cyber Threat Information Sharing Identified by Federal Agencies and Nonfederal Entities



Source: GAO analysis of factors that challenged cyber threat information sharing. | GAO-23-105468

Accessible Data for Figure 2: Six Challenges to Cyber Threat Information Sharing Identified by Federal Agencies and Nonfederal Entities

Challenge	Number of federal and nonfederal entities
Limited relationships	8
Limited funding and resources	13
Limited sharing of classified or sensitive information	13
Lack of timely sharing	10
Limited voluntary sharing	9
Lack of actionable information	9

Source: GAO analysis of factors that challenged cyber threat information sharing. | GAO-23-105468

Although 13 of the 14 federal agencies reported that they have taken initial actions to address these threat sharing challenges, all 14 agencies also acknowledged that these challenges have not been fully resolved for their sectors. In March and July 2023, the White House issued its *National Cybersecurity Strategy* and accompanying implementation plan to articulate the administration’s plan for addressing the nation’s long-standing cybersecurity challenges—including those pertaining to information sharing. The implementation plan includes eight initiatives that, if effectively implemented, could help agencies make progress in addressing the cyber threat information sharing challenges. For example, the implementation plan includes an initiative focused on removing barriers to delivering cyber threat intelligence. This initiative could help agencies make progress in addressing the challenge of limited sharing of classified or sensitive information.

GAO's prior work emphasizes the importance of (1) identifying outcome-oriented performance measures and (2) assessing whether existing processes are optimal for addressing challenges.

- The implementation plan does not identify outcome-oriented performance measures to assess the effectiveness of the steps taken under the eight information sharing initiatives described in the plan.
- The long-standing nature of the cyber threat sharing challenges raises questions about whether the mix of centralized and sector-specific sharing approaches is optimal. Although the implementation plan calls for CISA to assess whether new or improved sharing methods are needed, it does not include an assessment of whether existing sharing methods should be retired in favor of centralized or sector-specific sharing approaches.

Until the ONCD and CISA take steps to resolve these weaknesses, the long-standing cyber threat sharing challenges will likely continue to persist.

Contents

GAO Highlights	2
Why GAO Did This Study	2
What GAO Found	2
What GAO Recommends	iv
Letter	1
Background	5
Federal Agencies Used Various Methods to Share Cyber Threat Information	16
Federal Agencies Identified Challenges That Have Not Been Fully Addressed	32
Conclusions	48
Recommendations for Executive Action	49
Agency Comments and Our Evaluation	51
Appendix I: Objectives, Scope, and Methodology	57
Appendix II: Comments from the Office of the National Cyber Director	62
Accessible Text for Appendix II: Comments from the Office of the National Cyber Director	68
Appendix III: Comments from the Department of Homeland Security	74
Accessible Text for Appendix III: Comments from the Department of Homeland Security	78
Appendix IV: GAO Contacts and Staff Acknowledgments	81
Table	
Table 1: Initiatives Related to Addressing Cyber Threat Information Sharing Challenges as Described in the National Cybersecurity Strategy Implementation Plan	42
Figures	
Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies	10
Accessible Data for Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies	11
Figure 2: Methods Used by Federal Agencies to Facilitate Sharing of Cyber Threat Information with Critical Infrastructure	

Owners and Operators, and the Number of Federal Agencies That Used Each Method	17
Accessible Data for Figure 2: Methods Used by Federal Agencies to Facilitate Sharing of Cyber Threat Information with Critical Infrastructure Owners and Operators, and the Number of Federal Agencies That Used Each Method	18
Figure 3: Number of Federal Agencies and Nonfederal Entities That Identified Factors That Facilitate and Challenge Cyber Threat Information Sharing	33
Accessible Data for Figure 3: Number of Federal Agencies and Nonfederal Entities That Identified Factors That Facilitate and Challenge Cyber Threat Information Sharing	33

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FPS	Federal Protective Service
GSA	General Services Administration
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
IT	information technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ONCD	Office of the National Cyber Director
SRMA	sector risk management agency
TSA	Transportation Security Administration
Treasury	Department of the Treasury
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 26, 2023

Congressional Addressees

The nation’s 16 critical infrastructure sectors provide the essential services—such as electricity, oil and gas distribution, transportation, and water—that underpin American society.¹ These sectors rely on electronic networks, systems, and data to support their missions. However, cyber threats to these critical infrastructure sectors are significant, varied, and constantly changing.

In particular, cyber-based threats can come from a wide variety of sources, including nation states, corrupt employees, and transnational criminal groups. These threat actors vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain, or seeking an economic, political, or military advantage. In addition, cyber threat actors make use of various and ever-changing tactics, techniques, and procedures to adversely affect an organization’s electronic networks and systems.

Due to the variety and changing nature of the threats, critical infrastructure owners and operators must receive timely cyber threat information to adequately defend their networks and systems.² Using this information, critical infrastructure entities are better positioned to make

¹The 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).

²According to the National Institute of Standards and Technology, cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Examples of cyber threat information include indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures, security alerts, threat intelligence reports, and recommended security tool configurations. National Institute of Standards and Technology, Special Publication 800-150, *Guide to Cyber Threat Information Sharing* (October 2016).

informed decisions regarding threat detection and mitigation strategies. In addition, these entities can use cyber threat information to determine whether a malicious actor may have compromised their networks and systems.

Several federal entities play critical roles in gathering and disseminating cyber threat information across the 16 critical infrastructure sectors. For example:

- The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) provide information sharing methods that can be used by all 16 critical infrastructure sectors, including incident reporting methods and cyber threat alerts.
- Sector risk management agencies (SRMA) designated as the lead agencies for particular sectors (e.g., Department of Energy and the energy sector) often use methods to share sector-specific cyber threat information (e.g., cyber threat alerts with indicators of malicious cyber activity).³

We conducted this work under the authority of the Comptroller General to assist Congress with its oversight responsibilities. This report examines: (1) how federal agencies and critical infrastructure owners and operators share cyber threat information with each other, and (2) the factors that facilitate and challenge cyber threat information sharing and the extent to which federal agencies have taken action to address the challenging factors.

To address the first objective, we reviewed documentation on cyber threat information sharing methods.⁴ To do this, we reviewed documentation

³The nine SRMAs are: the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; the General Services Administration; and the Environmental Protection Agency.

⁴For the purposes of our review, we define the word “share” and “sharing” to mean bi-directional information sharing—that is (1) critical infrastructure owners and operators share with federal agencies and (2) federal agencies share with critical infrastructure owners and operators. In addition, we use the term “methods” to broadly refer to various systems, processes, and programs used to share information.

from and interviewed 14 primary federal agencies responsible for sharing cyber threat information with critical infrastructure owners and operators.⁵

Specifically, we reviewed documentation and interviewed officials from the selected federal agencies regarding the methods they use to share cyber threat information (e.g., descriptions of the methods, types of information shared). We then aligned each method to one of 11 categories: one existing category that was identified and summarized by federal cybersecurity guidance⁶ and the remaining 10 categories based on a content analysis of descriptions of the methods we received from the agencies.

To address the second objective, we interviewed officials and representatives from the 14 federal agencies selected for the first objective (e.g., CISA, FBI, and the other 12 agencies) and seven nonfederal entities to identify factors that facilitated and challenged their abilities to share cyber threat information. We selected these seven nonfederal entities based on sectors and entities that (1) have information sharing agreements with federal agencies, (2) operate threat information sharing services, and (3) have SRMAs that do not regularly develop cyber threat information sharing reports:

⁵More specifically, we selected the FBI, seven of the nine SRMAs, and six components from the remaining two SRMAs. The seven SRMAs we selected were the Departments of Agriculture, Defense, Energy, Transportation, and the Treasury; the Environmental Protection Agency; and the General Services Administration. The six components we chose from the remaining two SRMAs were the Department of Health and Human Services' Food and Drug Administration and Administration for Strategic Preparedness and Response; and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Federal Protective Service, Transportation Security Administration, and U.S. Coast Guard. Of note, we obtained information from the Department of Health and Human Services' Administration for Strategic Preparedness and Response and Food and Drug Administration on cyber threat information sharing in the healthcare and public health sector. For purposes of describing the department's collective efforts to share cyber threat information in the healthcare and public health sector, we aggregated the responses of the Administration for Strategic Preparedness and Response and the Food and Drug Administration and referred to those efforts as being performed by "HHS." By contrast, we only received information from one Department of Health and Human Services' agency—the Food and Drug Administration—on cyber threat information sharing efforts in the food and agriculture sector. As such, we referred to those efforts as being performed by the Department of Health and Human Services' Food and Drug Administration or "FDA."

⁶National Institute for Standards and Technology, *Guide to Cyber Threat Information Sharing*, Special Publication 800-150 (October 2016).

- two private sector Information Sharing and Analysis Centers (ISAC)⁷ that receive federal funding and serve as a mechanism for gathering and analyzing cyber threat information and sharing it among the stakeholders in respective infrastructure sectors and between the federal government—the Electricity ISAC and the Multi-State ISAC;
- four sector coordinating councils⁸ comprised of critical infrastructure owners and operators and industry representatives, among others, and partner with federal agencies on cyber threat sharing methods;⁹ and
- the State, Local, Tribal, and Territorial Government Coordinating Council, which is a national cross-sector council that leverages the expertise of its members to bring the governments’ perspectives into the national critical infrastructure protection planning process.

Specifically, we conducted structured interviews with officials and representatives from the selected federal agencies and nonfederal entities. During these interviews, we asked the officials and representatives open-ended questions to identify any factors that facilitated and challenged their abilities to share cyber threat information. Using this information, we conducted a content analysis in order to identify and categorize factors that were frequently identified as facilitating and challenging. We then totaled the number of times each factor was mentioned by department and agency officials, choosing to report on the top six factors that were identified by seven or more organizations (i.e., a third or more of the organizations in our review).

We then presented the factors that challenged cyber threat information sharing to the selected 14 federal agencies and asked them to provide

⁷ISACs are sector-based organizations that facilitate the sharing of cyber and physical threat information between government and the private sector.

⁸Sector coordinating councils are formed as 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 sector coordinating councils coordinate and collaborate on issues pertaining to their respective critical infrastructure sectors.

⁹Specifically, we met with two sector-wide sector coordinating councils (the Food and Agriculture Sector Coordinating Council and the Water Sector Coordinating Council), for which their respective SRMAs do not regularly develop cyber threat information products. In addition, we met with two subsector coordinating councils (the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council), for which their SRMAs regularly develop cyber threat information products.

documentation on actions the agencies have taken or plans they have developed to address those challenges.

In addition, we presented the factors that challenged cyber threat information sharing with the Office of the National Cyber Director (ONCD)—a component of the Executive Office of the President that is responsible for developing a national cyber strategy—and interviewed ONCD officials on their plans for addressing the challenges. We also compared the White House’s *National Cybersecurity Strategy* and accompanying implementation plan¹⁰ with the following practices highlighted in our prior work on national strategies and business process reengineering: (1) developing planned actions that address relevant challenges, (2) identifying outcome-oriented performance measures, and (3) reassessing whether existing processes are optimal for addressing challenges.¹¹

We conducted this performance audit from October 2021 to September 2023 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

Systems and networks supporting critical infrastructure are composed of, and connected to, enterprise IT systems and operational technology

¹⁰The White House, *National Cybersecurity Strategy*, (Washington, D.C.: March 2023) and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

¹¹GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, [GAO-17-300](#) (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, [GAO-15-602](#) (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, [GAO-05-372](#) (Washington, D.C.: Sept. 8, 2005); *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); and *Business Process Reengineering Assessment Guide*, Version 3, [GAO/AIMD-10.1.15](#) (Washington, D.C.: May 1997).

systems.¹² These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems and networks used by federal agencies and our nation's critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet.

With this greater connectivity, threat actors (e.g., nation-states, transnational criminal groups, activists, and disgruntled employees) are increasingly interested in and capable of conducting a cyberattack on our nation's critical infrastructure that could be disruptive and destructive. To facilitate their efforts, cyber adversaries use a variety of tactics (e.g., perform reconnaissance, gain network access, evade network defenders, and steal data) and techniques (e.g., reconnaissance scans, social engineer users, and disable security software). These tactics and techniques often exploit vulnerabilities in electronic systems.

Furthermore, threat actors use these tactics and techniques to facilitate cybersecurity incidents that have a range of consequences. These consequences may include the disruption of critical operations and inappropriate access to and disclosure, modification, or destruction of sensitive information. As a result, these cybersecurity incidents can threaten national security, economic well-being, and public health and safety. We have previously reported that, although federal agencies do not have a comprehensive inventory of cybersecurity incidents, several key federal and industry sources show (1) an increase in most types of cyberattacks across the United States, including those affecting critical infrastructure, and (2) significant and increasing costs for cybersecurity incidents.¹³

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of cybersecurity vulnerabilities, and the associated risks, we first designated federal information security as a

¹²Enterprise IT systems encompass traditional IT computing and communications hardware and software components that may be connected to the internet. Operational technology systems are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

¹³GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, [GAO-22-10456](#) (Washington, D.C.: June 21, 2022).

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 April 2023 high-risk update on major cybersecurity challenges.¹⁴

Cyber Threat Information Sharing

According to the National Institute of Standards and Technology (NIST), cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information can include:

- indicators of compromise;¹⁵
- tactics and techniques used by cyber threat actors;
- vulnerabilities that threat actors exploit;
- types of organizations targeted by threat actors;
- suggested actions to detect, contain, or prevent attacks; and
- findings from the analyses of incidents.

Sharing cyber threat information increases awareness about potential threats that might otherwise be undiscovered by an organization or a community. To enable access to this information, organizations that have been targeted by cyber threat actors must first share information with others about the malicious activity observed on their networks. Other organizations can then analyze this information to identify trends (e.g., seemingly unrelated attacks may be part of a larger threat actor campaign) and then widely disseminate specific strategies to enable other organizations to detect and prevent the malicious activity. If done effectively, cyber threat information sharing can create economies of

¹⁴GAO, *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. 19, 2023).

¹⁵Indicators of compromise refer to identification of forensic evidence from an organization's systems at the host or network level. Indicators of compromise are comprised of threat indicators, signatures, and techniques that IT professionals can use to identify unusual or irregular network activity.

scale for network defenders while also increasing costs for threat actors by forcing them to develop new tactics and techniques.

Roles and Responsibilities for Critical Infrastructure Threat Information Sharing

Because the private sector owns the majority of the nation's critical infrastructure, public and private sectors must work together to protect these assets and systems. Toward this end, a presidential directive, public-private policy, and federal law assign roles and responsibilities for federal agencies to assist the private sector in protecting critical infrastructure, including enhancing cybersecurity.

Presidential Policy Directive 21, issued in February 2013, categorized the nation's critical infrastructure into 16 sectors and outlined federal agency roles and responsibilities for protecting them. For example:

- The directive calls for the Department of Homeland Security (DHS) to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. For example, the directive calls for DHS to provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and share information and intelligence. Since the issuance of the directive, the White House has designated CISA to be the lead for cyber and physical infrastructure security within DHS.¹⁶
- The directive also called for the Department of Justice, including the FBI, to lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. In addition, the FBI is to conduct domestic collection, analysis, and dissemination of cyber threat information, according to the directive.
- The directive established sector-specific agencies as the federal entities responsible for providing institutional knowledge and specialized expertise for enhancing and protecting the cybersecurity of critical infrastructure. 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

¹⁶White House, *National Cybersecurity Strategy* (March 1, 2023).

“sector-specific agency.”¹⁷ The act also outlines responsibilities for SRMAs, including those related to supporting information sharing.¹⁸

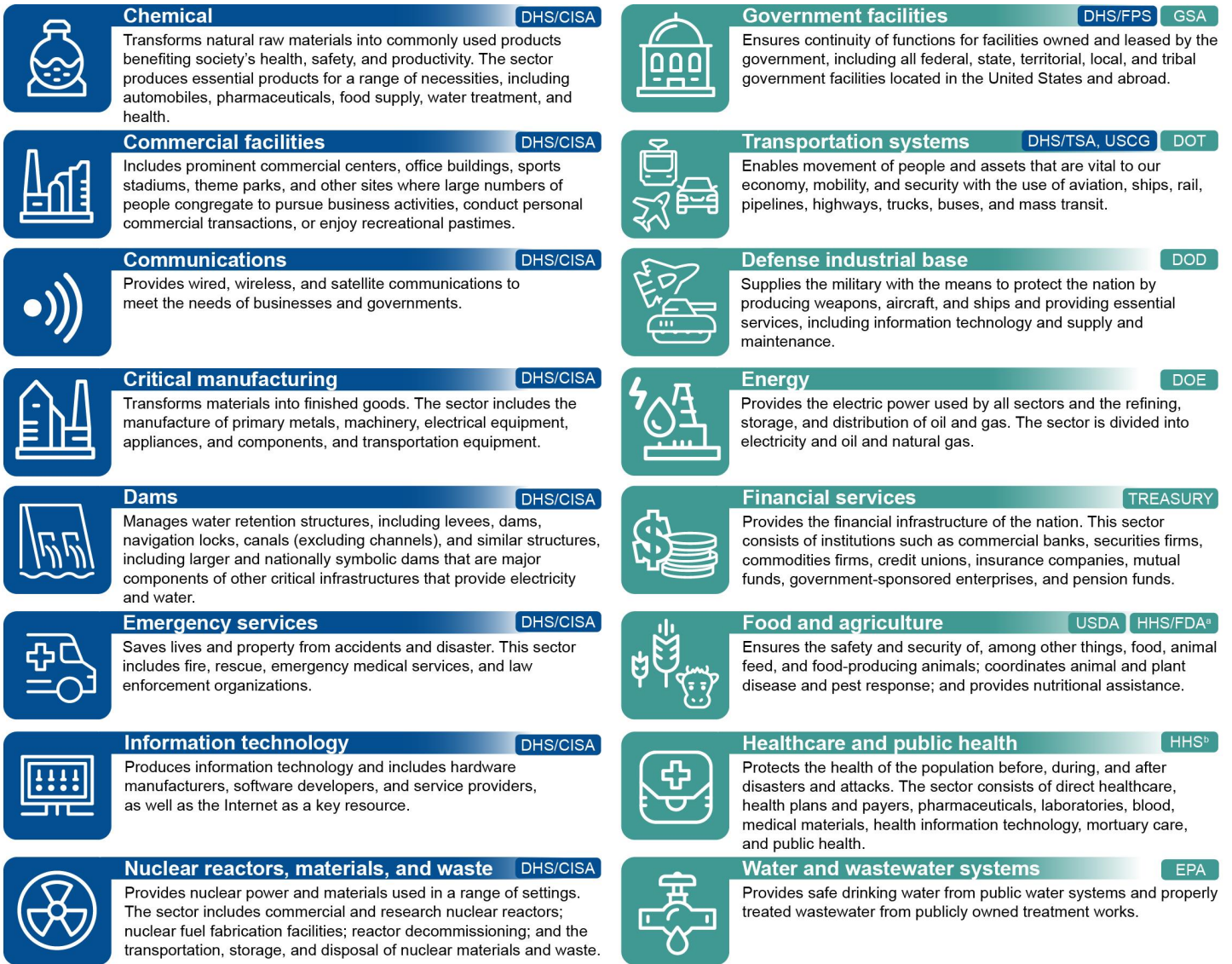
As shown in figure 1, each of the 16 critical infrastructure sectors has at least one federal agency designated as the lead for the sector based on authorities and capabilities specific to that sector.¹⁹ Some sectors have co-lead agencies where more than one agency shares SRMA responsibilities. DHS is unique among the SRMAs in that it has lead responsibility for eight of the 16 sectors, and co-leads two other sectors.

¹⁷6 U.S.C. § 652a.

¹⁸6 U.S.C. § 665d.

¹⁹The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 required the Secretary of Homeland Security to review the current framework for securing critical infrastructure and submit a report to appropriate congressional committees and the President that included recommendations related to sector risk management. 6 U.S.C. § 652a(b). According to CISA, in January 2023, the President initiated the process to rewrite Presidential Policy Directive 21. As part of ongoing efforts to revise this directive, officials noted that revisions are likely to include updates to, among other things, the specific agencies responsible for mitigating and responding to risk in each critical infrastructure sector and how agencies serving as the SRMA will interact with CISA in its effort to coordinate the broader national SRMA partnership framework.

Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies



Sectors solely managed by DHS
 Sectors managed by DHS and/or another federal agency

Sources: GAO analysis of Presidential Policy Directive 21 and DHS's National Infrastructure Protection Plan 2013; motorama/stock.adobe.com (icons). | GAO-23-105468

Accessible Data for Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies

Category	Category member	Category member information	Agencies
Sectors solely managed by DHS	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.	DHS/CISA
Sectors solely managed by DHS	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.	DHS/CISA
Sectors solely managed by DHS	Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS/CISA
Sectors solely managed by DHS	Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.;	DHS/CISA
Sectors solely managed by DHS	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.	DHS/CISA
Sectors solely managed by DHS	Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS/CISA
Sectors solely managed by DHS	Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS/CISA
Sectors solely managed by DHS	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.;	DHS/CISA
Sectors managed by DHS and/or another federal agency	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.	DHS/FPS, GSA

Letter

Category	Category member	Category member information	Agencies
Sectors managed by DHS and/or another federal agency	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.	DHS/TSA, USCG, DOT
Sectors managed by DHS and/or another federal agency	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.	DOD
Sectors managed by DHS and/or another federal agency	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.	DOE
Sectors managed by DHS and/or another federal agency	Financial services	Provides the financial infrastructure of the nation. This sector consists of institutions such as commercial banks, securities firms, commodities firms, credit unions, insurance companies, mutual funds, government-sponsored enterprises, and pension funds.	TREASURY
Sectors managed by DHS and/or another federal agency	Food and agriculture	Ensures the safety and security of, among other things, food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	USDA, HHS/FDA
Sectors managed by DHS and/or another federal agency	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.	HHS
Sectors managed by DHS and/or another federal agency	Water and wastewater systems	Provides safe drinking water from public water systems and properly treated wastewater from publicly owned treatment works.	EPA

Sources: GAO analysis of Presidential Policy Directive 21 and DHS's National Infrastructure Protection Plan 2013; motorama/stock.adobe.com (icons). | GAO-23-105468

Note: DHS (Department of Homeland Security), CISA (Cybersecurity and Infrastructure Security Agency), FPS (Federal Protective Service), GSA (General Services Administration), TSA (Transportation Security Administration), USCG (United States Coast Guard), DOT (Department of Transportation), DOD (Department of Defense), DOE (Department of Energy), Treasury (Department of the Treasury), USDA (Department of Agriculture), FDA (Food and Drug Administration), ASPR (Administration for Strategic Preparedness and Response), HHS (Department of Health and Human Services), EPA (Environmental Protection Agency). Five of the nine SRMAs—DHS, DOT, GSA, HHS/FDA, and USDA—also function as co-SRMAs, in which they work collaboratively to support a particular sector. Specifically, as co-SRMAs, HHS/FDA and USDA lead the food and agriculture sector; GSA and DHS lead the government facilities sector; and DHS and DOT lead the transportation systems sector.

^aIn contrast to the healthcare and public health sector, only one HHS agency—FDA—has responsibilities in the food and agriculture sector.

^bSeveral HHS agencies and operating divisions have responsibilities for the healthcare and public health sector. For purposes of this review, we referred to those agencies' and operating divisions' responsibilities collectively as "HHS."

Presidential Policy Directive 21 also highlights efficient information exchange, including threat information, as a strategic imperative. In doing so, the directive emphasizes the need for federal agencies to (1) gather threat information from critical infrastructure owners and operators and (2) disseminate threat information to critical infrastructure owners and operators. In particular, the directive emphasizes the importance of agencies gathering quality and timely threat information from critical infrastructure owners and operators.²⁰ With this information, federal agencies can analyze and disseminate integrated and actionable information to the broader critical infrastructure communities.

To address the implementation of Presidential Policy Directive 21, DHS updated *the National Infrastructure Protection Plan in 2013*.²¹ The plan describes a voluntary partnership model for coordinating federal agency and critical infrastructure owner and operator efforts, including information sharing. To facilitate threat information sharing, the plan encourages owners and operators to form several groups:

- **Information Sharing and Analysis Centers (ISAC)** are entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and share intelligence and information related to critical infrastructure. Specifically, ISACs serve as operational and dissemination arms for many sectors and subsectors to facilitate sharing of information between government and the private sector, and work closely with sector coordinating councils (see below) in the sectors where they are recognized. They are designed to provide in-depth sector analysis and help coordinate sector response during incidents, including information sharing within sectors, between sectors, and among public and private sector critical infrastructure stakeholders. Government agencies also may rely on

²⁰The directive also emphasizes the importance of inter-agency sharing. Agency Inspectors General have issued a series of reports analyzing procedures for sharing threat information between agencies. See, e.g., Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2021-002-U (Washington, D.C.: Dec. 9, 2021); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2019-005-U (Washington, D.C.: Dec. 19, 2019); and *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Audit Report No. AUD-2017-005 (Washington, D.C.: Dec. 19, 2017).

²¹Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

ISACs for situational awareness and to enhance their ability to provide timely, actionable data to targeted entities. Most sectors have established one or more ISACs or ISAC-like capabilities.²²

- **Sector coordinating councils** are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, and activities. Membership on the councils can vary from sector to sector but is meant to represent a broad base of stakeholders, including owners, operators, associations, and other entities—both large and small—within the sector. All of the sectors have at least one sector coordinating council.

In addition, the National Infrastructure Protection Plan called for SRMAs to develop plans that identified actions needed to address sector-specific risks and challenges.²³ Most SRMAs completed their respective plans for their sectors by 2015. Several plans call for the use of methods for sharing threat information tailored to the needs of the specific sectors.²⁴

Prior Federal Efforts to Address Cyber Threat Information Sharing Challenges

We and others have previously identified a number of long-standing challenges that agencies face in effectively facilitating cyber threat information sharing between federal agencies and critical infrastructure stakeholders. For example, in July 2004, we reported on challenges that public-private threat information sharing centers face, such as building trusted relationships, obtaining necessary funding, and overcoming

²²Of note, although some ISACs receive government funding (e.g., the Multi-State ISAC and Communications ISAC), many require a paid membership to receive ISAC services.

²³Of note, at the time the National Infrastructure Protection 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.

²⁴We 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).

sharing barriers.²⁵ In addition, agency Inspectors General have issued a series of reports since 2017 highlighting barriers to sharing cyber threat information between federal agencies and private organizations.²⁶ The *Cyberspace Solarium Commission's U.S. Cyberspace Solarium Commission Final Report* also identified a number of challenges to addressing the nation's cyber threats, including those relating to federal agencies' efforts to facilitate cyber threat information sharing.²⁷

Federal agencies and Congress have recognized these challenges and taken steps aimed at addressing them. For example, pursuant to the *Cybersecurity Information Sharing Act of 2015*, DHS established the Automated Information Sharing system to facilitate the sharing of cyber threat indicators.²⁸ More recently, Congress and the President enacted legislation calling for CISA to engage in rulemaking to require certain

²⁵GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, [GAO-04-780](#) (Washington, D.C.: Jul. 9, 2004).

²⁶See, e.g., Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2021-002-U (Washington, D.C.: Dec. 9, 2021); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2019-005-U (Washington D.C.: Dec. 19, 2019); and *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Audit Report No. AUD-2017-005 (Washington, D.C.: Dec. 19, 2017).

²⁷The John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (Aug. 13, 2018) established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees, as well as officials from the Office of the Director of National Intelligence, DHS, the Department of Defense, and the Federal Bureau of Investigation. In March 2020, the commission released a final report containing recommendations to Congress and federal agencies aimed at addressing the strategic approach needed to defend the nation against cyberattacks and the policies and legislation needed to implement that strategy. U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

²⁸6 U.S.C. §659(h). Threat indicators are system artifacts or observables associated with an attack, such as an attempt to log into an account from a known malicious internet protocol address.

critical infrastructure owners and operators to report information to CISA on select cybersecurity incidents.²⁹

In addition, Congress has recognized the need to clearly define a leadership role to coordinate the federal government's efforts that would address cyber challenges, such as those pertaining to threat information sharing. Specifically, in January 2021 Congress enacted legislation to establish the position of National Cyber Director within the Executive Office of the President.³⁰ The director is to lead the coordination and implementation of national cyber policy and strategy, including the *National Cybersecurity Strategy*.

Federal Agencies Used Various Methods to Share Cyber Threat Information

The 14 federal agencies in our review reported relying on a range of methods to facilitate sharing of cyber threat information with critical infrastructure owners and operators. In particular, federal agencies relied on 11 methods that fall into two broad categories:

- **Cybersecurity and law enforcement services.** Eight methods represent cybersecurity and law enforcement services that federal agencies use to, among other things, share threat information with critical infrastructure owners and operators.
- **Collaborative sharing environments.** Three methods represent collaborative sharing environments (e.g., ISACs and working groups and councils) that federal agencies and owners and operators use to share threat information with each other.

²⁹The Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted on March 15, 2022, as part 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 act was signed into law to issue the proposed rule, and an additional 18 months to issue a final rule. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y (Cyber Incident Reporting for Critical Infrastructure Act of 2022), 136 Stat. 49, 1043 (March 15, 2022) codified at 6 U.S.C. § 681b.

³⁰The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, div. A, title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021) codified at 6 U.S.C. §1500. The Act was vetoed by the President but overridden by Congress.

See figure 2 for a summary of the 11 methods—and their associated categories—that federal agencies used to facilitate threat information sharing.

Figure 2: Methods Used by Federal Agencies to Facilitate Sharing of Cyber Threat Information with Critical Infrastructure Owners and Operators, and the Number of Federal Agencies That Used Each Method



Sources: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-23-105468

Accessible Data for Figure 2: Methods Used by Federal Agencies to Facilitate Sharing of Cyber Threat Information with Critical Infrastructure Owners and Operators, and the Number of Federal Agencies That Used Each Method

Category	Subcategory	Subcategory information	Subcategory total
Cybersecurity and law enforcement services	Cyber threat briefings	A collection of purposeful briefings and meetings including calls, conferences, and webinars that are used to share cyber threat information.	14
Cybersecurity and law enforcement services	Threat information products	Threat information products include structured and unstructured cyber threat information that are shared as alerts, advisories, and various assessments.	14
Cybersecurity and law enforcement services	Incident reporting services	Web, telephone, or other systems that are used to facilitate the reporting and tracking of cyber incidents.	7
Cybersecurity and law enforcement services	Intrusion detection systems / intrusion prevention systems	Intrusion detection systems analyze events on systems or networks and use indicators that help detect incidents to share with others. Intrusion prevention systems attempt to stop incidents from occurring.	3
Cybersecurity and law enforcement services	Malicious activity analysis	Malicious activity analysis allows for the examination of suspicious files that may be present on systems and networks to determine what they do and how to remove them.	2
Cybersecurity and law enforcement services	Incident response services	Incident response services can assist in mitigating and determining the impact of cybersecurity incidents and investigating those responsible.	2
Cybersecurity and law enforcement services	Threat indicator sharing platforms	Threat indicator sharing platforms automate the exchange of structured data in real time to allow the comparison of network activity with previously discovered malicious activity to detect and prevent cyber incidents.	1
Cybersecurity and law enforcement services	Exploited vulnerability catalog	An exploited vulnerability catalog is an inventory of vulnerabilities in software and networks that are known to have been exploited by cyber threat actors.	1

Category	Subcategory	Subcategory information	Subcategory total
Collaborative sharing environments	Information sharing and analysis centers	Information Sharing and Analysis Centers are sector-based organizations that facilitate cyber threat information sharing with critical infrastructure owners and operators.	9
Collaborative sharing environments	Working groups and councils	Working groups and councils are dedicated collaboration environments to engage on cyber threat information sharing efforts.	6
Collaborative sharing environments	Federal cybersecurity collaboration centers	Federal cybersecurity collaboration centers are operational collaborative environments that are focused on enabling the timely, actionable, and relevant sharing of cyber threat information with, among others, critical infrastructure owners and operators.	3

Sources: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-23-105468

Note: Numbers in circles represent the number of federal agencies that use each method to share cyber threat information with critical infrastructure owners and operators. In addition, for the purposes of this report, we defined each method based on examples that federal agencies provided to reflect their information sharing efforts.

Agencies took two different approaches to using the 11 methods. Specifically, two agencies—CISA and FBI—used the methods share information in a centralized approach with each of the 16 critical infrastructure sectors. The other 12 remaining federal agencies used the 11 methods in a federated approach, to varying extents, to share sector-specific threat information. As discussed in more detail later in this report, the long-standing challenges to sharing cyber threat information raises questions about whether the existing mix of sharing methods is optimal for addressing those challenges.

In addition, each of the 11 information sharing methods were used to varying degrees. Specifically:

- Three methods—cyber threat briefings, threat information products, and ISACs—were used by both CISA and FBI and by more than half of the remaining 12 federal agencies to share sector-specific threat information.
- Eight methods—incident reporting services, working groups and councils, federal cybersecurity collaboration centers, intrusion

detection and/or prevention systems, malicious activity analysis, incident response services, threat indicator sharing platforms, and exploited vulnerability catalog—were also used by CISA or FBI and by half or less of the remaining 12 federal agencies to share sector-specific information.

Further, the 14 agencies in our review varied in the number of information sharing methods that they each used. Specifically,

- one agency—CISA—used all 11 methods to share cyber threat information;
- three agencies—the Department of Defense (DOD), the Department of Energy (DOE), and FBI—used more than half of the 11 methods to share threat information; and
- 10 agencies used fewer than half of the 11 information sharing methods.

Federal Agencies Used Eight Cybersecurity and Law Enforcement Services

Threat Information Product Example

In February 2023, the Cybersecurity and Infrastructure Security Agency, FBI, the National Security Agency, and other authoring agencies released a joint cybersecurity advisory describing observed threat activities associated with North Korean state-sponsored cyber threat actors. The agencies highlighted observed tactics, techniques, and procedures as well as indicators of compromise used by malicious actors to target critical infrastructure with ransomware. For example,

- **Acquire infrastructure.** The agencies explained that the threat actors first acquired the resources needed to carry out the ransomware attacks, including malicious website domain names and their associated Internet Protocol addresses. For example, the advisory highlighted two malicious domain names ending in .com and .kr extensions that malicious actors used in their attacks.
- **Gain access.** The agencies highlighted that the threat actors then gained access to critical infrastructure systems and networks by exploiting common vulnerabilities in commercial software libraries and devices and identified specific vulnerabilities that the actors have used.
- **Employ malicious tools.** After gaining access, the agencies noted that threat actors employed various tools including malicious ransomware and encryption software to further their malicious activity. To help remove these tools, the advisory identified specific signatures to identify the tools in an organization's environment.
- **Demand ransom.** After employing their malicious tools, the agencies noted that threat actors demanded a ransom to be paid in cryptocurrency to remove their presence from an organization's environment. In addition, the advisory identified signatures associated with the actor's ability to collect cryptocurrency from organizations.

Source: GAO analysis of agency documentation. | GAO-23-105468

Fourteen federal agencies used eight cybersecurity and law enforcement services to share cyber threat information with critical infrastructure owners and operators. These eight services include gathering and/or disseminating such information via:

- **Cyber threat briefings.** All 14 federal agencies relied on cyber threat briefings and other meetings to facilitate the gathering or dissemination of cyber threat information with critical infrastructure owners and operators. In particular, FBI and CISA generally relied on in-person or virtual discussions, webinars, or briefings to facilitate centralized cyber threat information sharing with critical infrastructure owners and operators in all 16 sectors. For example, in March 2022, CISA and FBI officials held a conference call with critical infrastructure owners and operators to, among other things, share information on potential cyber threats as a result of the Russia-Ukraine conflict. As part of the call, federal officials highlighted the potential for Russian cyber threat actors to target critical infrastructure owners and operators and steps they can take to mitigate the threat.

In addition, within their respective sectors, the other 12 federal agencies primarily relied on in-person or virtual discussions, webinars, or briefings with specific critical infrastructure sector groups. For example, in November 2022, DOE made publicly available a briefing on cyber threats to renewable and distributed energy sector systems, including an overview of threat actor capabilities and recent incidents.

Mandatory Cyber Incident Reporting

Five federal agencies—the Department of Defense (DOD), Department of Energy (DOE), Department of Health and Human Services (HHS), Transportation Security Administration (TSA), and U.S. Coast Guard (USCG)—relied on incident reporting services to help gather incident reports that owners and operators are required to submit. In particular:

- DOD gathered mandatory cyber incident reports from certain owners and operators in the defense industrial base, as required by DOD regulation.
- DOE gathered mandatory cyber incident reports from certain owners and operators in the energy sector on electric emergency incidents and disturbances, including cyber incidents, as required by federal law and policy.
- HHS gathered mandatory cyber incident reports from certain owners and operators (covered entities) in the healthcare and public health sector as required by federal regulation.
- TSA facilitated the gathering of mandatory cyber incident reports from owners and operators in the transportation sector (i.e., freight rail and pipelines, and regulated airports and aircraft operators) to CISA, as required by security directives.
- The U.S. Coast Guard gathered mandatory transportation security incidents, including cyber incidents, reports through its National Response Center, from owners and operators of certain vessels or facilities, as required by federal regulation.

Source: GAO analysis of mandatory cyber in

- **Threat information products.** All 14 agencies in our review have disseminated cyber threat information products (e.g., alerts, advisories, and assessments) to critical infrastructure owners and operators. (See the sidebar for a summary of a threat product relating to North Korean actors.)
- Two of the agencies—FBI and CISA—developed various products to disseminate information in a centralized manner to all 16 critical

infrastructure sectors. Specifically, the FBI developed several unclassified products on an as-needed basis on cyberattacks and associated mitigations. The FBI then shared these products by way of its InfraGard system³¹ or its public website. The FBI also developed several classified products on an ad hoc basis and made them available to users of a classified system. In addition, CISA developed various unclassified alerts, assessments, and advisories on an ad hoc and periodic basis to highlight threats to enterprise IT systems and operational technology systems. CISA disseminated products with sensitive information by way of the Homeland Security Information Network or email, and disseminated non-sensitive information through its public website.

- Seven of the 12 remaining agencies—DOD, DOE, the Department of Health and Human Services (HHS), Transportation Security Administration (TSA), the Department of Transportation (DOT), Treasury, and U.S. Coast Guard (USCG)—developed cyber products to disseminate information to their respective sectors in a federated manner. Specifically, all seven of these agencies developed unclassified cyber products that they shared by way of the Homeland Security Information Network, email, or their websites. In addition, three of these agencies—DOD, TSA, and USCG—established classified cyber threat products that they shared by way of classified systems.

The remaining five agencies—Environmental Protection Agency (EPA), General Services Administration (GSA), Food and Drug Administration (FDA), Federal Protective Service (FPS), and U.S. Department of Agriculture (USDA)—did not regularly develop their own cyber threat products. However, all of these agencies primarily shared cyber threat information developed by CISA or the FBI with their sectors. In addition, three of these agencies—EPA, FDA, and USDA—co-authored a product with other agencies such as CISA or FBI.

³¹InfraGard is a nonprofit organization associated with the FBI. The program consists of regional chapters with representatives from the public and private sectors. The program focuses on activities related to critical infrastructure protection and cybercrime. For example, FBI uses a system operated by the association to securely share information with private industry, other government agencies, state and local law enforcement, and the academic community.

Intrusion Detection and Prevention System Information Sharing

To participate in these intrusion detection and prevention systems, critical infrastructure owners and operators voluntarily choose to deploy sensors to their networks. These sensors then monitor network traffic for malicious activity (e.g., indicators of compromise). When malicious activity is identified, the systems prevent the malicious activity or alert the owner or operator of the activity.

In addition, the systems gather threat information for federal agencies by sending the agencies certain information on observed malicious activity (e.g., associated indicators of compromise). Federal agencies can in turn add relevant indicators of compromise to these systems, thereby increasing protection for other owners and operators.

Source: GAO analysis of agency documentation. | GAO-23-105468

- **Incident reporting services.** Seven federal agencies—CISA, FBI, DOD, DOE, HHS, TSA, and USCG—reported using incident reporting services to gather information on cybersecurity incidents that have impacted critical infrastructure owners and operators. In particular, CISA and the FBI used separate web-based incident reporting services that allow victims of cyberattacks across all 16 sectors to voluntarily report information on cyber incidents, such as a description of the incident and type of organization impacted.³² The other five federal agencies used incident reporting services to gather incident reports that owners and operators are required to submit.³³ (See the sidebar for more information on these mandatory incident reporting requirements.)

Agencies analyzed and compiled information received from these incident reports and then disseminated cyber threat information to relevant critical infrastructure owners and operators. For example, the FBI received multiple reports of cyber criminals increasingly targeting

health care payment processors to redirect victim payments. The FBI used information received from these reports to develop and

³²See <https://www.cisa.gov/forms/report> and <https://www.ic3.gov/Home/FileComplaint>.

³³Several of the incident reporting services also allow owners and operators to voluntarily report incident information.

disseminate a Private Industry Notification that highlighted this threat and recommendations for addressing it.³⁴

- **Intrusion detection and/or prevention systems.** Three federal agencies in our review—CISA, DOD, and DOE—relied on intrusion detection and/or prevention systems to facilitate the gathering or dissemination of cyber threat information to critical infrastructure owners and operators. (See the sidebar for more information on these systems, including how they gather and disseminate information.)

In particular, CISA relied on two intrusion detection and/or prevention systems to facilitate centralized cyber threat information sharing from all 16 critical infrastructure sectors. Specifically, CISA operates CyberSentry, a voluntary program that leverages hardware and software to identify malicious activity on operational technology systems. Further, CISA operates its Enhanced Cybersecurity Services program to compare cyber activity on owner and operator networks with classified and unclassified indicators of compromise (e.g., malicious internet protocol address).³⁵

The other two federal agencies—DOE and DOD—used intrusion prevention systems in a federated manner to facilitate the gathering or dissemination of cyber threat information within their respective sectors. For example, DOE leverages the Cybersecurity Risk Information Sharing Program,³⁶ which identifies malicious cyber activity on systems used by critical infrastructure owners and operators in the electricity and oil, and natural gas subsector. In addition, DOD uses the Protective Domain Name System, which prevents certain malicious cyber activity on IT systems used by critical

³⁴FBI, Private Industry Notification, *Cyber Criminals Targeting Healthcare Payment Processors, Costing Victims Millions in Losses*, PIN Number 20220914-001 (Sept. 14, 2022).

³⁵CISA's Enhanced Cybersecurity Services program previously relied on both classified and unclassified cyber threat indicators. According to CISA officials, the agency stopped providing new classified indicators to the program during the COVID-19 pandemic. These officials stated that the agency plans to retire the system in fiscal year 2024 and there are no plans to replace the system.

³⁶The Cyber Risk Information Sharing Program is managed by the E-ISAC, advised by DOE's Office of Cybersecurity, Energy Security, and Emergency Response, and is supported with DOE cyber threat intelligence and DOE analytics through the Pacific Northwest National Laboratory.

infrastructure owners and operators in the defense industrial base sector.³⁷

- **Malicious activity analysis.** Two federal agencies—CISA and DOD—operated web-based systems that received samples of malicious activity (e.g., malware) from critical infrastructure owners and operators. Specifically, CISA’s Malware Analysis submission site allowed critical infrastructure owners and operators from all 16 sectors to voluntarily submit malware samples.³⁸ In addition, DOD’s Electronic Malware Submission portal allowed defense industrial base owners and operators to submit malware, phishing emails, email attachments, and other suspicious files for automated analysis.³⁹

After receiving the malware samples, CISA and DOD (and other federal agencies they share the information with) can analyze the malware to, among other things, learn more about the tactics, techniques, and procedures of cyber threat actors and identify associated mitigations. For example, in July 2022 CISA published a technical malware analysis report on a file submitted to the agency that contained malicious code used to facilitate communication with the threat actor’s infrastructure and provide remote access to a victim’s system. The report included indicators of compromise associated with the malware (e.g., the Internet Protocol address of the threat actor’s infrastructure) and recommendations for mitigating the threat of the malware.⁴⁰

- **Incident response services.** Two federal agencies—CISA and FBI—reported that their incident response services enabled them to gather cyber threat information. Specifically, CISA often identifies

³⁷The system focuses on malicious domains and Internet Protocol addresses. Users access information online through domain names (e.g., federalagency.gov), while web browsers access information through Internet Protocol addresses (e.g., 192.168.0.1). The Domain Name System translates domain names to Internet Protocol addresses so that browsers can load internet resources. Cyber threat actors often attempt to trick users into visiting malicious domains and Internet Protocol addresses by manipulating these requests to translate names to Internet Protocol addresses. DOD’s system helps protect against these tricks by analyzing Domain Name System requests that owners and operators may make to prevent them from visiting malicious websites.

³⁸<https://www.cisa.gov/resources-tools/services/malware-analysis>.

³⁹According to DOD, results are ready in less than 15 minutes. Also of note, certain Defense contractors are required by federal regulation to provide malicious software that has been discovered and isolated by the contractor to DOD. 32 CFR § 236.4

⁴⁰CISA, Analysis Report, *MAR-10382580-r2.v1 –RAT*, Alert Code AR22-197A (July 18, 2022).

threat information when helping critical infrastructure owners and operators recover from an incident. Similarly, FBI identifies threat information when performing a law enforcement investigation. For example, from November 2021 through January 2022, CISA responded to an incident involving a defense industrial base sector organization's network and identified malicious activity associated with an advanced persistent threat actor.⁴¹ Using information gathered as part of this effort, in October 2022 CISA published a cybersecurity advisory that highlighted tactics and techniques used by the actor and identified steps owners and operators can use to detect and prevent those tactics and techniques.⁴² As another example, the FBI infiltrated the "Hive" ransomware group in July 2022, captured the ransomware's decryption keys, and offered them to victims, according to a Department of Justice press release.⁴³

- **Threat indicator sharing platforms.** One agency—CISA—relied on a threat indicator sharing platform to gather and disseminate cyber threat information with critical infrastructure owners and operators in a centralized manner from all 16 critical infrastructure sectors. Specifically, CISA operates the Automated Indicator Sharing system which, among other things, gathered suspected malicious indicators of compromise (e.g., signatures of malicious files) from critical infrastructure owners and operators. These owners and operators voluntarily shared information with the Automated Indicator Sharing system when malicious activity was detected on their networks and systems. CISA, through its Automated Indicator Sharing system, also disseminated suspected indicators of compromise (e.g., malicious Internet Protocol addresses) that were used to detect and prevent

⁴¹According to NIST, an advanced persistent threat is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.

⁴²CISA, Cybersecurity Advisory, *Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization*, Alert Code AA22-277A (Oct. 4, 2022).

⁴³<https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>. According to the Department of Justice, the Hive ransomware group has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and other critical infrastructure.

malicious activity on critical infrastructure owner and operator networks and systems.

- **Exploited vulnerability catalog.** One agency—CISA—maintained and updated a list of vulnerabilities that have been exploited by cyber threat actors. Specifically, CISA developed the Known Exploited Vulnerability Catalog to identify specific vulnerabilities in certain software and hardware solutions that malicious actors have successfully exploited. CISA made this list publicly available on its website.⁴⁴

Federal Agencies Used Three Collaborative Sharing Environments

Nine of the 14 federal agencies we reviewed used three collaborative sharing environments to share cyber threat information with critical infrastructure owners and operators. The remaining five federal agencies generally did not use collaborative sharing environments to share such information.

Specifically, the three collaborative sharing environments that the nine agencies used to share cyber threat information include gathering and/or disseminating such information via:

- **Information Sharing and Analysis Centers (ISAC).** Nine federal agencies—CISA, DOD, DOE, EPA, FBI, HHS,⁴⁵ Treasury, TSA, and USCG—reported leveraging ISACs to facilitate the gathering or dissemination of information from owners and operators. In addition, five of those nine agencies—CISA, DOD, DOE, HHS, and Treasury—reported establishing formal agreements with their respective ISACs that enabled sharing between the organizations.

For example, DOD officials stated they established a cooperative research and development agreement with the National Defense ISAC that enables DOD to collaborate with critical infrastructure owners and operators in the defense industrial base through a communications platform developed by the ISAC. The remaining four agencies relied on informal relationships with the ISACs to facilitate

⁴⁴<https://www.cisa.gov/known-exploited-vulnerabilities>.

⁴⁵According to HHS officials, the Center for Devices and Radiological Health within HHS holds an agreement with the Health ISAC to protect medical devices against cybersecurity threats.

the exchange of cyber threat information. For example, USCG officials explained that the agency participates in meetings with the Maritime Transportation System ISAC every other month to collaborate on cybersecurity threats to maritime transportation system assets.

- **Working groups and councils.** Six federal agencies—CISA, FBI, DOD, DOE, HHS, and TSA—reported leveraging more than a dozen sector- and technology-specific working groups and councils to facilitate the gathering or dissemination of cyber threat information with critical infrastructure owners and operators. For example, HHS officials explained that they gather information from owners and operators through their collaboration with the Cyber Health Working Group. According to the group’s website, the working group is a collection of IT professionals in the health sector that use a web-based platform to share cyber threat information and resources.⁴⁶

As another example, CISA relied on the Industrial Control Systems Joint Working Group. CISA established this group to facilitate information sharing, including information relating to cyber threats to operational technology.

- **Federal cybersecurity collaboration centers.** Three federal agencies—CISA, DOD, DOE—operated four cybersecurity collaboration centers that served as operational collaborative environments to facilitate the gathering or dissemination of cyber threat information with critical infrastructure owners and operators.
 - In August 2021, CISA announced the launch of the Joint Cyber Defense Collaborative pursuant to authority provided by Congress to establish a joint cyber planning office.⁴⁷ According to CISA, the center provides a central collaborative environment for cyber defense planning and operations with participants from the federal government and private sector, including critical infrastructure owners and operators. For example, in December 2021, federal Joint Cyber Defense Collaborative members gathered and disseminated indicators of compromise from critical infrastructure

⁴⁶According to the working group’s website, the group was originally created by the National Capital Region chapter of InfraGard and the Cyber Task Force at the FBI’s Washington Field Office. <https://www.intelligence.healthcare/>.

⁴⁷6 U.S.C. §665b. CISA established a joint cyber planning office pursuant to authority provided by Congress to establish an office to develop cyber defense operations for the public and private sectors.

owners and operators on an emerging and actively exploited vulnerability known as Log4Shell.⁴⁸

- Under DOD's Defense Industrial Base Cybersecurity Program, the *DOD Cyber Crime Center* operates the Defense Industrial Base Collaborative Information Sharing Environment Directorate to share cyber threat information at both classified and unclassified levels. For example, the center made software publicly available that owners and operators could use to extract information (e.g., filenames and passwords) from malware in a consistent format—thus making it easier to share this information.⁴⁹ According to DOD, more than 1,000 companies share information using the environment.
- DOD's National Security Agency established the *Cybersecurity Collaboration Center* with the aim of scaling intelligence-driven cybersecurity through open and collaborative partnerships. The center works with industry, agency, and international partners to harden networks and operationalize the National Security Agency's insights on nation-state cyber threats. For example, the agency works with these partners to jointly create mitigations guidance for emerging activity, chronic cybersecurity challenges, and secure emerging technologies.
- DOE's *Energy Threat Analysis Center* is a pilot collaborative environment for experts from federal agencies and private industry from the energy sector to work together to analyze and address cyber threats to the energy sector. According to DOE officials, the pilot environment allows analysts from the federal government and

⁴⁸Log4Shell is a vulnerability in a software library that provides functionality to a wide range of applications and services. The vulnerability enables malicious cyber threat actors to submit a specially crafted request to a vulnerable system that uses the library, causing the system to execute arbitrary code and allowing threat actors to take full control of the affected system.

⁴⁹The software enables critical infrastructure owners and operators to extract information from malware in a consistent open standard that is used to share cyber threat information called the Structured Threat Information Expression format. The software is publicly available on a web-based software repository hosting service known as GitHub. See <https://github.com/dod-cyber-crime-center>.

private sector to collaborate on, among other things, cyber threat intelligence, and relevant mitigations to cyber threats.⁵⁰

Federal Agencies Identified Challenges That Have Not Been Fully Addressed

The 21 entities in our review—14 federal agencies and seven nonfederal entities—identified factors that facilitate or challenge cyber threat information sharing between federal agencies and critical infrastructure owners and operators. Although 13 federal agencies reported that they have taken initial actions to address the six most frequently identified challenges, all 14 agencies acknowledged that one or more of these challenges still existed for each of the 16 sectors. The *National Cybersecurity Strategy* and accompanying implementation plan outline eight initiatives related to improving cyber threat information sharing. While the eight initiatives should address the six cyber threat information sharing challenges, if implemented effectively, neither the strategy or plan (1) identify measures to assess the effectiveness of each initiative or (2) assess if the current mix of sharing methods are optimal.

Factors Facilitating and Challenging Information Sharing

Six factors that facilitate or challenge effective sharing of cyber threat information were identified by at least a third (seven or more) of the 21 entities in our review.⁵¹ Specifically, seven or more of the agencies and entities in our review identified two of these factors as facilitating cyber threat information sharing. In addition, seven or more of the entities identified all six factors as challenging threat information sharing. Of note, each of the 14 federal agencies and seven nonfederal entities identified at

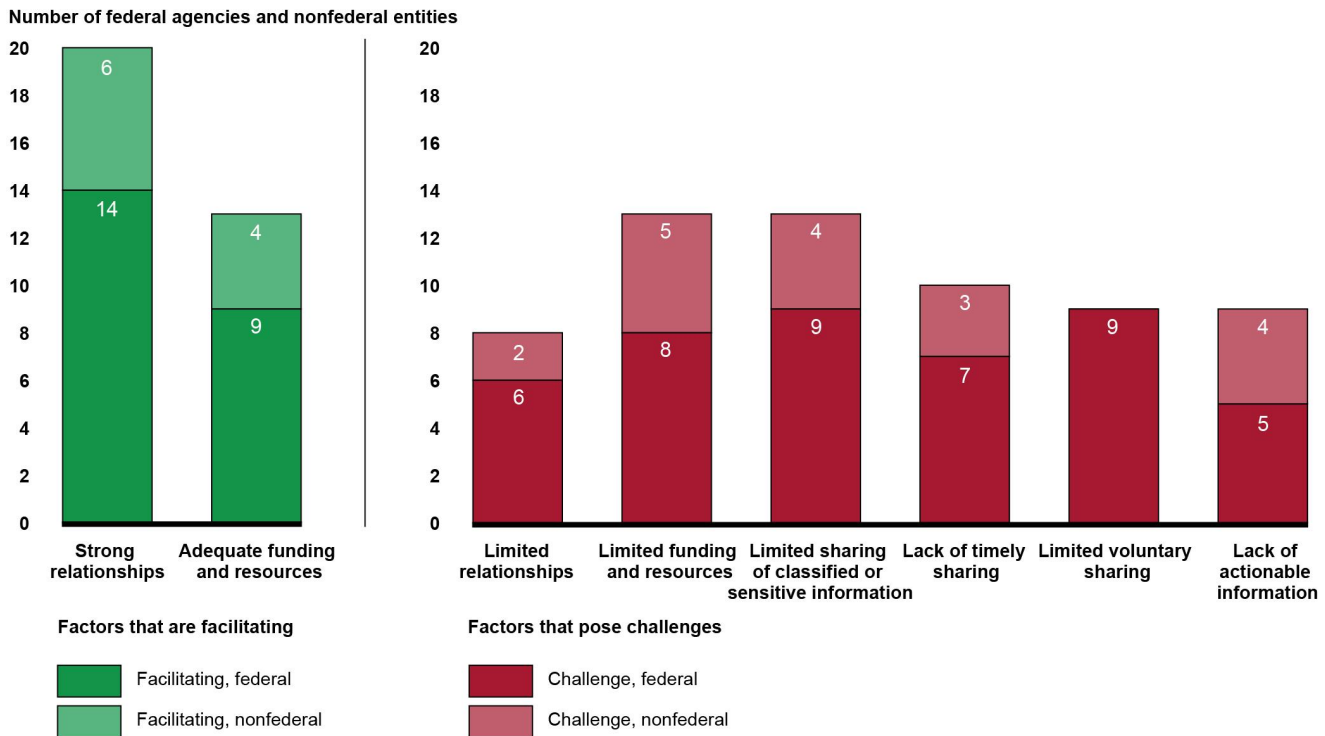
⁵⁰According to DOE's fiscal year 2023 congressional budget justification, the agency will establish the Energy Threat Analysis Center, in partnership with CISA's Joint Cyber Defense Collaborative, to advance industry-government threat situational awareness, mitigation, and response. The center's goals will be to, among other things, (1) establish a government and industry operational collaborative environment to develop actionable operational intelligence; (2) enable an information exchange among government and industry to address a shared problem; and (3) achieve a deeper understanding of threat actor tactics, capabilities, and activities with potential to impact systemic risks to the energy sector.

⁵¹Entities identified certain factors as both facilitating and challenging cyber threat information sharing.

least one of the six most frequently cited factors as challenging to threat information sharing.

Figure 3 shows the numbers of federal agencies and nonfederal entities that identified the six factors as enabling and challenging their abilities to share cyber threat information.

Figure 3: Number of Federal Agencies and Nonfederal Entities That Identified Factors That Facilitate and Challenge Cyber Threat Information Sharing



Source: GAO analysis of factors that challenged or facilitated cyber threat information sharing. | GAO-23-105468

Accessible Data for Figure 3: Number of Federal Agencies and Nonfederal Entities That Identified Factors That Facilitate and Challenge Cyber Threat Information Sharing

Factors that are facilitation	Facilitating, federal	Facilitating, nonfederal
Strong relationships	14	6
Adequate funding and resources	9	4

Factors that pose challenges	Challenge, federal	Challenge, nonfederal
Limited relationships	6	2
Limited funding and resources	8	5
Limited sharing of classified or sensitive information	9	4
Lack of timely sharing	7	3
Limited voluntary sharing	9	0
Lack of actionable information	5	4

Source: GAO analysis of factors that challenged or facilitated cyber threat information sharing. | GAO-23-105468

Note: Among the 21 total entities we spoke to in our review—including 14 federal agencies and seven nonfederal entities—some federal agencies and nonfederal entities identified certain factors as both facilitating and challenging cyber threat information sharing. Additionally, some federal agencies and nonfederal entities did not identify certain factors as facilitating or challenging. As a result, the numbers for each factor above do not add up to the total of 21 agencies and entities included in this review.

The six most frequently identified factors that facilitated or challenged cyber threat information sharing are as follows:

- **Relationships.** Agencies and nonfederal entities identified relationships as a factor that both facilitated and challenged cyber threat information sharing. Specifically,
 - *Facilitated.* Twenty organizations—all 14 federal agencies and six nonfederal entities—reported that having strong relationships between various federal agencies and nonfederal entities facilitated more effective cyber threat information sharing. For example, Treasury officials explained that their strong relationships with the sector coordinating council and ISAC in the financial sector has enabled them to more effectively collaborate on cyber threat information with critical infrastructure owners and operators. Similarly, officials from a sector coordinating council highlighted their strong and long term relationship with the FBI, noting that the agency regularly provides cyber threat briefings to critical infrastructure owners and operators in that specific sector.
 - *Challenged.* Although most organizations cited relationships as a facilitating factor, eight organizations—six federal agencies and two nonfederal entities—also noted that limited relationships between critical infrastructure owners and operators and federal agencies challenged cyber threat information sharing. For example, although Treasury officials highlighted strong relationships with certain sector organizations, they also

highlighted challenges in developing in-depth relationships with all owners and operators in their sector.

As another example, officials at USDA stated that, given the large and diverse scope of entities in the food and agriculture sector (e.g., family farmers, small businesses, and large conglomerates), critical infrastructure owners and operators may not have a direct relationship with the agency to share cyber threat information, thus challenging the sharing of such information.

- **Funding and resources.** Agencies and nonfederal entities identified funding and resources as a factor that both facilitated and challenged cyber threat information sharing. Specifically,
 - *Facilitated.* Thirteen organizations—nine federal agencies and four nonfederal entities—reported that having adequate funding and resources facilitated cyber threat information sharing efforts. For example, representatives from a nonfederal entity in the energy sector explained that DOE funding (in addition to funding from industry) has enabled the development of the Cybersecurity Risk Information Sharing Program.⁵²
 - *Challenged.* Although many organizations cited funding and resources as a facilitating factor, 13 organizations—eight federal agencies and five nonfederal entities—also told us that critical infrastructure owners and operators often have limited funding and resources; as such, they were not always able to effectively share cyber threat information with federal agencies. For example, representatives from a nonfederal entity in the energy sector stated that smaller critical infrastructure owners and operators in the sector do not have adequate funding to effectively use cyber threat information sharing methods—highlighting the importance of programs such as the Cybersecurity Risk Information Sharing Program in helping to address these concerns.

As another example, officials from CISA explained that a resource-limited critical infrastructure owner or operator may prioritize addressing other critical cybersecurity issues (e.g., replacing outdated and vulnerable equipment) over sharing cyber threat information. Further, representatives from a nonfederal entity noted that critical infrastructure owners and operators in their sector often have a small number of employees (e.g., 10 to

⁵²As previously discussed, the program detects malicious cyber activity on certain systems used by critical infrastructure owners and operators in the electricity, oil, and natural gas subsector.

15 employees) with few to no cybersecurity personnel—thereby limiting the amount of information that is shared with federal agencies.

- **Sharing of classified or sensitive information.** Thirteen organizations—nine federal agencies and four nonfederal entities—identified limited sharing of classified or sensitive information as a challenge to effective cyber threat information sharing.⁵³ In particular, because of these restrictive classifications or designations, federal agencies do not always widely share cyber threat information with critical infrastructure owners and operators. For example, DOT officials stated that when certain federal agencies provide classified briefings on select cybersecurity threats, only certain critical infrastructure owners and operators that have staff with the necessary security clearances may participate.

In addition, TSA officials explained that it has been difficult to “unmask” (i.e., make viewable) the identity of owners and operators in the transportation systems sector that are described in classified threat intelligence products as having been targeted by cyber threat actors.⁵⁴ Without this information, TSA is not able to inform those owners and operators of the relevant threat. As another example, officials at a sector coordinating council noted that U.S. critical

⁵³Classified information means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Executive Order 13526, *Classified National Security Information*, states that an individual may be authorized to access classified information provided that (1) a favorable determination of eligibility has been made by an agency head or designee, (2) the person has signed an approved nondisclosure agreement, and (3) the person has a need-to-know the information. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009). Sensitive information, also known as controlled unclassified information, is any information (other than classified) that requires special handling and controls to prevent the unauthorized disclosure to the public or other individuals without an official need-to-know. Examples of sensitive information include For Official Use Only, Law Enforcement Sensitive, and designations under DHS’s traffic light protocol.

⁵⁴Intelligence Community elements may acquire intelligence that identifies the name of a “U.S. person”—which includes U.S. citizens, unincorporated associations composed of U.S. citizens, and corporations incorporated in the United States. In certain circumstances, it may be necessary for those elements to disseminate the identity of a U.S. person so that recipients can fully understand the intelligence. Office of the Director of National Intelligence policy provides that the identity of a U.S. person can be “unmasked” (i.e., made viewable) and disseminated to other agencies under specified procedures. See Director of National Intelligence, *Intelligence Community Policy Guidance 107.1, Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*, (Jan. 11, 2018).

infrastructure owners and operators that have an international presence are not always able to access restricted cyber threat information (e.g., For Official Use Only) from federal agencies that would otherwise be relevant to the sector.

- **Timely sharing.** Ten organizations—seven federal agencies and three nonfederal entities—identified a lack of timely sharing of cyber threat information as a challenge to effective sharing of this information. Specifically, these organizations stated that federal agencies do not always share such information with critical infrastructure owners and operators in a timely manner.

For example, officials at a sector coordinating council pointed out that in March 2022 the FBI shared information about the October 2021 cyberattacks targeting election officials. These officials explained that it would have been more valuable to share this information near the time of the attack.⁵⁵ Similarly, officials at FDA and HHS noted that CISA and FBI may take weeks to alert the agency of a cyber incident in their sector.

- **Voluntary sharing.** Nine of the 14 selected federal agencies identified limited voluntary sharing as a challenge to effective cyber threat information sharing.⁵⁶ Specifically, critical infrastructure owners and operators are not always required to share information on cyber incidents and may have other reasons for not voluntarily sharing information on cyber incidents.⁵⁷ For example, CISA officials stated

⁵⁵FBI, Private Industry Notification, *Cyber Actors Target US Election Officials with Invoice-Themed Phishing Campaign to Harvest Credentials*, PIN Number 20220329-001 (March 29, 2022).

⁵⁶As discussed in more detail later in this report, recently enacted legislation may help to address this challenge. Signed in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 specifies that covered entities must report covered cyber incidents no later than 72 hours after the entity reasonably believes an incident has occurred. To support this requirement, CISA, in consultation with SRMAs and others, are required to publish a final rule within 42 months after enactment of the Act (September 2025).

⁵⁷For example, according to the work of several Inspectors General, some private sector companies and industries are reluctant to share cyber threat information with federal law enforcement agencies based on the perception that cooperation with such agencies may lead to negative business and regulatory consequences. The Inspectors General also reported that private sector entities are reluctant to share information with federal entities because they do not understand how federal entities use and protect the information being shared. See Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, AUD-2021-002-U, Dec. 9, 2021.

that, although the agency operates a system that allows critical infrastructure owners and operators to provide cyber incident reports to the agency, it receives very few reports.⁵⁸

CISA officials also stated that its voluntary intrusion detection and prevention system—the Enhanced Cybersecurity Services—had very few entities (about 15 as of October 2022) that participated in the program, which limited the amount of information that CISA could gather and disseminate.⁵⁹ Due in part to this low enrollment, CISA plans to retire the system in fiscal year 2024. Similarly, DOE’s Cybersecurity Risk Information Sharing Program is made available to over 3,000 electricity, oil, and natural gas owners and operators, but agency officials told us that only 68 sector entities participate in this program, as of June 2022.

- **Actionable information.** Nine organizations—five federal agencies and four nonfederal entities—identified a lack of actionable information as a challenge to effective sharing of cyber threat information. For example, officials at an ISAC noted that CISA’s Automated Indicator Sharing system lacked customized threat information tailored to specific sectors or subsectors. As a result, critical infrastructure owners and operators were not always aware of actions they needed to take to address sector-specific threats, according to officials from that ISAC.

As another example, officials from a sector coordinating council stated that cyber threat information that federal agencies share can be vague. These officials explained that critical infrastructure owners and operators would benefit from having specific and detailed cyber threat information (e.g., malicious indicators) included in bulletins and briefings. The officials further noted that critical infrastructure owners and operators not only want to receive cyber threat information, but also want to know how best to utilize and operationalize it.

⁵⁸HHS officials added that DHS’s and the Department of Justice’s interpretation of federal law incentivizes owners and operators to report cyber threat information to DHS and not to applicable SRMAs. Specifically, HHS officials noted that critical infrastructure owners and operators receive additional liability protections under the *Cybersecurity Information Sharing Act of 2015* when owners and operators provide cyber threat information to DHS. DHS and Department of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (Oct. 2020).

⁵⁹CISA operates its Enhanced Cybersecurity Services program to compare cyber activity on owner and operator networks with classified and unclassified indicators of compromise (e.g., malicious Internet Protocol address).

All six of the factors identified by seven or more of the federal agencies and nonfederal entities are consistent with previous findings from the Inspectors General community regarding challenges that federal agencies face in sharing cyber threat information. For example, in March 2023, DHS's Inspector General noted a number of cyber threat information sharing challenges that CISA faced, including funding and resources, restrictive classifications that impacted critical infrastructure owners' and operators' ability to obtain cyber threat information, and the timely sharing of information.⁶⁰ In addition, the Inspectors General community identified the remaining factors—strong relationships, voluntary information sharing, and actionable information—as challenges to effective cyber threat information sharing over the course of three joint reviews on the implementation of the Cybersecurity Information Sharing Act of 2015.⁶¹

⁶⁰Office of the Inspector General of the Department of Homeland Security, *CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation*, Report No. OIG-23-19 (Washington, D.C.: Mar. 3, 2023).

⁶¹See, e.g., Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2021-002-U (Washington, D.C.: Dec. 9, 2021); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2019-005-U (Washington, D.C.: Dec. 19, 2019); and *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Audit Report No. AUD-2017-005 (Washington, D.C.: Dec. 19, 2017).

Federal Agencies Have Taken Initial Actions to Address Challenges

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Division Y of Public Law 117-103)

Signed in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 specifies that covered entities must report covered cyber incidents no later than 72 hours after the entity reasonably believes an incident has occurred.

To support this requirement, the Cybersecurity and Infrastructure Security Agency, in consultation with sector risk management agencies and others, are required to publish a final rule 42 months after enactment (September 2025). The rule should address, among other things, (1) what constitutes a covered cyber entity and incident as well as (2) the contents of cyber incident reports. Further, CISA is required to conduct outreach to provide entities with information on methods to submit reports, protections entities have when sharing information, consequences of noncompliance, and any third parties that could help entities with creating reports.

The act also requires CISA to analyze all reports submitted and provide critical infrastructure related stakeholders with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including contextual information, cyber threat indicators, and defensive measures. In addition, CISA is to publish quarterly, unclassified public reports that describe aggregate, anonymized observations, findings, and recommendations based on covered cyber incident reports.

Source: GAO. | GAO-23-105468

Most of the federal agencies in our review reported taking initial actions to address the six most frequently identified factors that challenge cyber threat information sharing. Specifically, 13 of the 14 federal agencies that share information—all except DOT—reported taking initial actions to address the six most frequently identified factors. For example:

- **Limited voluntary sharing:** CISA has taken steps towards implementing incident reporting requirements called for in the recently passed Cyber Incident Reporting for Critical Infrastructure Act of 2022. (See the sidebar for more information on this legislation.) For example, the agency released a formal request for information and hosted 10 listening sessions through which stakeholders will be able to provide CISA with their perspectives on various aspects of the act's

future regulations. As another example, after years of relying on voluntary reporting, between May and December 2021, TSA established mandatory cyber incident reporting requirements in the transportation systems sector that extend to critical infrastructure owners and operators for pipelines, surface transportation, and aviation.

- **Limited sharing of classified or sensitive information:** EPA officials stated that they have worked closely with critical infrastructure owners and operators in the water and wastewater systems sector to obtain clearances for key personnel that need to obtain classified information.
- **Lack of actionable information:** HHS stated that it was developing new guidance to ensure actionable information is provided to members in the healthcare and public health sector.⁶² These resources are expected to include internal guidance aimed at better tailoring cyber alerts to the healthcare and public health sector.

Nevertheless, each of the 14 agencies acknowledged that one or more of the six most frequently identified challenges have not yet been resolved for their sector. In addition, ONCD officials recognized that these challenges are still present to varying degrees across the critical infrastructure sectors.

National Cybersecurity Strategy and Accompanying Implementation Plan Recognize Information Sharing Challenges, but Do Not Address Measures and Methods

In March and July 2023, the White House issued its *National Cybersecurity Strategy* and accompanying implementation plan to articulate the administration's plan for addressing the nation's long-standing cybersecurity challenges—including those pertaining to

⁶²As previously mentioned, several HHS agencies and operating divisions have responsibilities for the healthcare and public health sector. For purposes of this review, we aggregated the information we received from those agencies and operating divisions regarding their efforts to address cyber threat information sharing challenges for the healthcare and public health sector. We collectively referred to those aggregated efforts as being performed by "HHS." By contrast, only one HHS agency—the Food and Drug Administration—has responsibilities in the food and agriculture sector. As such, we referred to efforts in the food and agriculture sector as being performed by the Food and Drug Administration.

information sharing.⁶³ The implementation plan for the *National Cybersecurity Strategy* includes eight initiatives that, if effectively implemented, could help agencies make progress in addressing the frequently identified cyber threat information sharing challenges discussed earlier in this report. Table 1 below provides details on the eight initiatives as described in the implementation plan, the agency that is responsible for leading each initiative, and the target completion date.

Table 1: Initiatives Related to Addressing Cyber Threat Information Sharing Challenges as Described in the National Cybersecurity Strategy Implementation Plan

Initiative title	Initiative description	Responsible agency	Target completion date
Assess and improve Federal Cybersecurity Centers' and related cyber centers' capabilities and plans necessary for collaboration at speed and scale	The Office of the National Cyber Director (ONCD) will conduct a review of federal cybersecurity centers and related cyber centers to identify gaps in capabilities and other key findings.	ONCD	September 2023
Evaluate how the Cybersecurity and Infrastructure Security Agency (CISA) can leverage existing reporting mechanisms or the potential creation of a single portal to integrate and operationalize sector risk management agencies' (SRMA) sector-specific systems and processes.	CISA will work with SRMAs to understand where gaps exist in information sharing and understand requirements for an interoperable system for information exchange among SRMAs and other federal partners. Where SRMAs do not have robust information sharing capabilities already in place, CISA will work with them to develop a process to mature their capabilities.	CISA	June 2024
Remove barriers to delivering cyber threat intelligence and data to critical infrastructure owners and operators	The Office of the Director of National Intelligence (ODNI) will, in coordination with the Departments of Justice and Homeland Security, review policies and procedures for sharing cyber threat intelligence with critical infrastructure owners and operators and evaluate the need for expanding clearances and intelligence access to enable this sharing.	ODNI	June 2024
Establish an SRMA support capability	CISA will establish an SRMA Support Office Capability to serve as the single point of contact for supporting all SRMAs. The office will coordinate the provision of CISA services for each SRMA, depending on its capabilities. CISA will work with each SRMA to define its needs and priorities for support from the office, to include evaluating options and opportunities for shared services, and use this information to update CISA's services catalog, as necessary.	CISA	March 2025

⁶³The White House, *National Cybersecurity Strategy* (Washington, D.C.: March 2023); and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

Letter

Initiative title	Initiative description	Responsible agency	Target completion date
Issue final Cyber Incident Reporting for Critical Infrastructure Act rule	CISA will consult with SRMAs, the Department of Justice, and other federal agencies to implement the Cyber Incident Reporting for Critical Infrastructure Act. CISA will publish a Notice of Proposed Rulemaking and Final Rule per statutory requirements, and develop the processes to advance effective actioning of incident reports (e.g., sharing of incident reports with appropriate agencies).	CISA	September 2025
Identify and operationalize sector-specific intelligence needs and priorities	The National Security Council will lead a policymaking process to establish an agreed-upon approach for SRMAs to identify sector-specific intelligence needs and priorities.	National Security Council	December 2025
Update the National Cyber Incident Response Plan	CISA, in coordination with ONCD, will lead a process to update the National Cyber Incident Response Plan to strengthen processes, procedures, and systems to more fully realize the policy that “a call to one is a call to all.” This update will also include clear guidance to external partners on the roles and capabilities of federal agencies in incident response and recovery.	CISA	December 2025
Investigate opportunities for new and improved information sharing and collaboration platforms, processes, and mechanisms	CISA will lead a cross-sector effort to review public-private collaboration mechanisms. SRMAs, in coordination with CISA as appropriate, will represent the activities in their sectors to deliver to CISA for the development of a maturity model for public-private collaboration.	CISA	December 2026

Source: The National Cybersecurity Strategy Implementation Plan. | GAO-23-105468

In addition, in June 2023, the Office of Management and Budget and ONCD issued a memorandum directing federal agencies to formulate and prioritize cybersecurity investments in their fiscal year 2025 budget submissions using the *National Cybersecurity Strategy*.⁶⁴ For example, federal agencies are directed to demonstrate how their budget submissions prioritize building the capacity and mechanisms to collaborate with critical infrastructure owners and operators to, among other things, mitigate threats to their respective sectors.

Our prior work on national strategies and business process reengineering emphasizes the importance of (1) developing planned actions that address relevant challenges, (2) identifying outcome-oriented performance measures, and (3) reassessing whether existing processes

⁶⁴Office of Management and Budget and ONCD, *Administration Cybersecurity Priorities for the FY 2025 Budget*, Memorandum M-23-18 (Washington, D.C.: June 27, 2023).

are optimal for addressing challenges.⁶⁵ While the strategy and implementation plan have initiatives that, if implemented effectively, should address each of the six cyber threat sharing challenges, they do not (1) identify outcome-oriented performance measures for the initiatives related to cyber threat information sharing, or (2) comprehensively assess whether the mix of centralized and federated sharing approaches is optimal.

The Strategy and Implementation Plan Acknowledge Cyber Threat Information Sharing Challenges

Our prior work on national strategies emphasizes the importance of identifying and documenting planned actions in national strategies to address long-standing challenges that cut across levels of government and industry sectors.⁶⁶ Doing so can help to focus needed attention and resources on resolving the challenges.

The *National Cybersecurity Strategy*, accompanying implementation plan, and related budget memo discuss efforts that, if implemented effectively, should address all six cyber threat information sharing challenges identified in our review. For example,

⁶⁵GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, [GAO-17-300](#) (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, [GAO-15-602](#) (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, [GAO-05-372](#) (Washington, D.C.: Sept. 8, 2005); *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); and *Business Process Reengineering Assessment Guide*, Version 3, [GAO/AIMD-10.1.15](#) (Washington, D.C.: May 1997).

⁶⁶GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, [GAO-17-300](#) (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, [GAO-15-602](#) (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, [GAO-05-372](#) (Washington, D.C.: Sept. 8, 2005); and *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

- **Limited relationships.** The strategy calls for the federal government to build on decades of experience working with ISACs and others to work with them to develop a shared vision of how the public-private sharing model should evolve. The implementation plan aligns this call to action by identifying an initiative for investigating opportunities for new and improved information sharing. If agencies effectively implement this initiative, they can be better positioned to address the challenge of limited relationships.
- **Limited funding and resources.** The joint Office of Management and Budget and ONCD fiscal year 2025 budget memo call for agencies to align their budget submissions with the *National Cybersecurity Strategy*. For example, the memo calls for agency budget submissions to demonstrate how they prioritize building the capacity and mechanisms to collaborate with critical infrastructure owners and operators. If agencies effectively carry out this guidance, they can be better positioned to address the challenge of limited funding and resources.
- **Limited sharing of classified or sensitive information.** The implementation plan includes an initiative focused on removing barriers to delivering cyber threat intelligence to critical infrastructure owners and operators. This threat intelligence is often classified or sensitive. Accordingly, if agencies effectively implement this initiative, they will likely make progress in addressing the challenge of limited sharing of classified or sensitive information.
- **Lack of actionable information.** The strategy calls for the federal government to review declassification policies and processes to determine the conditions under which extending additional classified access and expanding clearances is necessary to provide actionable intelligence. The implementation plan aligns this call to action with an initiative to review policies and procedures for sharing cyber threat intelligence and to evaluate the need for expanding clearances and intelligence access. If agencies effectively carry out this initiative, they can be better positioned to address the challenge of lack of actionable information.
- **Limited voluntary sharing.** The implementation plan includes an initiative focused on the issuance of the final Cyber Incident Reporting for Critical Infrastructure Act rule that relates to the challenge of limited voluntary sharing.⁶⁷ As previously mentioned, the act specifies that covered entities must report covered cyber incidents to CISA no

⁶⁷See Division Y of the Consolidated Appropriations Act, 2022, Cyber Incident Report for Critical Infrastructure Act, Pub. L. No. 117-103, 136 Stat. 1038 (March 14, 2022).

later than 72 hours after the entity reasonably believes an incident has occurred. To support this requirement, CISA, in consultation with sector risk management agencies and others, are required to publish a final rule 42 months after enactment (September 2025). The rule should address, among other things, (1) what constitutes a covered cyber entity and incident as well as (2) the contents of cyber incident reports. The implementation of this final rule will likely result in more agencies being required to share information relating to cyber incidents that have a negative impact on organizations' systems.⁶⁸

- **Lack of timely sharing.** The *National Cybersecurity Strategy* and accompanying implementation address the remaining challenge of timely sharing. The strategy includes a strategic objective calling for agencies to increase the speed of intelligence sharing and victim notification and includes two related initiatives that address delivering threat information more rapidly.⁶⁹ If effectively carried out, agencies will be better positioned to address the challenge of timely cyber threat information sharing.

The Strategy and Implementation Plan Do Not Identify Outcome-Oriented Performance Measures

Our prior work on national strategies emphasizes the importance of developing outcome-oriented performance measures to assess the

⁶⁸As stated in ONCD's written comments on a draft of this report, the implementation plan's initiative on removing barriers to delivering cyber threat intelligence may incentivize critical infrastructure owners and operators to voluntarily share more information. ONCD officials explained that owners and operators often seek to "enrich" information about malicious cyber activity observed on their networks (e.g., obtain information on what threat actor was responsible). ONCD officials added that federal agency sharing of threat intelligence is a valuable method for enriching such malicious cyber activity. ONCD further explained that, if barriers to delivering threat intelligence are removed, owners and operators seeking to enrich information about malicious cyber activities observed on their network may be more likely to voluntarily share those activities with federal agencies. Accordingly, if the initiative is effectively carried out, agencies will likely make progress towards addressing the challenge of limited voluntary information.

⁶⁹The titles of the two related initiatives are (1) identify and operationalize sector-specific intelligence needs and priorities, and (2) remove barriers to delivering cyber threat intelligence and data to critical infrastructure owners and operators.

effectiveness of actions taken to help address long-standing challenges.⁷⁰ Establishing such measures can help organizations demonstrate the degree to which desired results were achieved.

Although the implementation plan tasks ONCD with assessing the effectiveness of the strategy, the plan does not identify any outcome-oriented performance measures to assess the effectiveness of the steps taken under the eight information sharing initiatives described in the plan. In a written response, ONCD officials stated that performance measures will be developed, as appropriate, for the assessment of cyber threat information sharing activities. However, ONCD did not identify a time frame for when it plans to develop performance measures. Until ONCD identifies outcome-oriented performance measures to assess progress made in implementing the eight information sharing initiatives, ONCD will not have a clear definition of what it wants to accomplish—including the extent to which the information sharing challenges are to be addressed.

The Strategy and Implementation Plan Do Not Assess the Current Mix of Cyber Threat Information Sharing Approaches

We have previously reported that many of the largest federal agencies find themselves encumbered with structures and processes rooted in the past. To address this issue, our prior work on business process reengineering emphasizes the need for organizations to reassess whether existing processes need improvement when existing processes are not meeting customer or stakeholder needs.⁷¹ Doing so can provide organizations with a complete picture of the benefits, costs, and risks involved in moving to new processes, redesigning them, or eliminating processes altogether.

⁷⁰GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, [GAO-17-300](#) (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, [GAO-15-602](#) (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, [GAO-05-372](#) (Washington, D.C.: Sept. 8, 2005); and *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

⁷¹GAO, *Business Process Reengineering Assessment Guide*, Version 3, [GAO/AIMD-10.1.15](#) (Washington, D.C.: May 1997).

However, the strategy and implementation plan do not comprehensively assess whether the mix of centralized and federated sharing approaches is optimal for addressing the frequently identified cyber threat information sharing challenges. To its credit, the implementation plan calls for CISA to lead SRMAs in investigating opportunities for new and improved information sharing and collaboration platforms, processes, and mechanisms. Although this initiative could help agencies to make progress in addressing sharing challenges through new or improved sharing methods, it does not include an assessment of whether existing sharing methods should be retired in favor of centralized or federated sharing approaches.

In addition, the implementation plan does not call for CISA to work with FBI as part of the initiative to investigate opportunities for new and improved information sharing. As previously discussed, FBI operates more than half of the 11 cyber threat information sharing methods. In addition, FBI is one of two agencies that uses a centralized approach to share information with all 16 sectors.

As previously mentioned, the long-standing cyber threat information sharing challenges raises questions about whether the current mix of centralized and federated sharing approaches is optimal for addressing the challenges. For example, agencies may be able to better address the challenge of lack of timely sharing if federal agency resources that are spread across centralized and federated approaches were aligned under a single approach.

In a written response, CISA officials stated that the agency could not comment on why this initiative does not include an assessment of whether certain sharing methods should be retired because the initiative is within a White House document and not a CISA-owned document. Nevertheless, until CISA, in coordination with the 14 agencies, assesses whether the current mix of sharing methods is optimal for addressing the sharing challenges—including whether existing sharing methods should be retired—agencies will likely struggle to address the long-standing sharing challenges.

Conclusions

As cyber threats continue to grow in size and sophistication, federal agencies and critical infrastructure owners and operators face an urgent need to cooperate on cyber threat information sharing efforts that will help

address these threats. Although most federal agencies and nonfederal entities frequently cited factors that helped facilitate cyber threat information sharing, long-standing challenges inhibit information sharing between federal agencies and critical infrastructure owners and operators. In addition, the long-standing challenges to sharing cyber threat information raises questions about whether the existing mix of centralized and federated sharing methods is optimal for addressing those challenges.

Recognition of these challenges in the White House's *National Cybersecurity Strategy* and accompanying implementation plan is a positive development. In particular, the strategy and accompanying implementation plan include eight initiatives that, if effectively implemented, could help federal agencies make progress towards addressing the frequently identified challenges. However, the implementation plan does not include outcome-oriented performance measures needed to define what the initiatives are to accomplish. Further, although the implementation plan includes an initiative that calls for CISA to assess whether new or improved sharing methods are needed, it does not include an assessment of whether existing sharing methods should be retired in favor of centralized or federated sharing approaches. Until CISA and ONCD take action to resolve these weaknesses, the long-standing cyber threat information sharing challenges will likely continue to persist.

Recommendations for Executive Action

We are making two recommendations—one to ONCD and one to CISA. Specifically:

The National Cyber Director should identify outcome-oriented performance measures for the eight cyber threat information sharing initiatives that are included in the *National Cybersecurity Strategy Implementation Plan*. (Recommendation 1)

The Director of CISA, in coordination with the 14 agencies, should conduct a comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the cyber threat sharing challenges—including whether existing sharing methods should be retired in favor of centralized or federated approaches. (Recommendation 2)

Letter

Agency Comments and Our Evaluation

We provided a draft of this report to 11 federal agencies.⁷² In response, we received written comments from the agencies to which we made recommendations, ONCD and DHS.

In written comments, ONCD disagreed with one recommendation originally included in our draft report and the one current recommendation.

- ONCD disagreed with our recommendation included in the draft of this report on updating the *National Cybersecurity Strategy Implementation Plan* to fully address the two challenges relating to a lack of voluntary and timely sharing. The agency provided additional information and context that the plan had addressed the two challenges identified in our report. Upon our review of the information, we agreed that the agency had sufficiently addressed these challenges in the plan. Accordingly, we removed this finding and withdrew the recommendation from the final report.
- ONCD agreed with our finding on outcome-oriented measures and stated it intends to develop performance measures. However, ONCD disagreed with the associated recommendation that it identify outcome-oriented performance measures for the eight cyber threat information sharing initiatives included in the plan (Recommendation 1). It explained that a lack of validated outcome based performance measures exist in the cybersecurity field to measure cybersecurity information sharing. It further noted that developing such measures would likely require years of work and research. As a result, the agency stated that it is premature to have the plan include outcome-oriented measures and that without additional research, ONCD would be severely limited in its ability to identify and develop effective metrics for the plan.

However, we believe that it is feasible for ONCD to develop outcome-oriented measures to help ensure that ongoing implementation of the eight information sharing-related initiatives are achieving results in addressing and resolving the information sharing challenges

⁷²Specifically, we provided the report to 11 federal entities that provided comments representing the views of the 14 selected federal agencies—USDA, DOD, DOE, DHS, HHS, DOT, the Treasury, EPA, FBI, and GSA—and ONCD. DHS provided comments representing the views of the following four component agencies included in our review: CISA, FPS, TSA, and U.S. Coast Guard. In addition, HHS provided comments representing the views of the following two operating divisions included in our review: the Food and Drug Administration and Administration for Strategic Preparedness and Response.

highlighted in this report. For example, with respect to the initiative of issuing the final Cyber Incident Reporting for Critical Infrastructure Act rule, ONCD may be able to measure the number of threat information products (e.g., alerts) that are developed based on incident reporting under this rule. In doing so, ONCD could survey users of these threat information products to determine what specific impacts these products had on the security of their networks.

In addition, existing critical infrastructure protection policy emphasizes the importance and feasibility of measuring outcomes to evaluate the effectiveness of planned efforts. For example, DHS's *2013 National Infrastructure Protection Plan* calls for the critical infrastructure community to evaluate its progress in accomplishing the plan's goals and priorities, such as identifying high-level outputs or outcomes and evaluating progress toward achieving the national goals and priorities.⁷³

Further, specific sectors have already included outcome data in assessing the performance of their information sharing efforts. For example, DHS's and HHS's *2015 Healthcare and Public Health Sector Specific-Plan* includes "outcome data" for assessing the effectiveness of sector information sharing, such as feedback on the quality of sector information sharing systems, tools, and collaborative efforts. Similarly, in 2015, we reported that DOD established performance metrics to monitor cybersecurity-related activities, including the number of cyber threat products disseminated by DOD to cleared companies and the timeliness of shared threat information.⁷⁴ Accordingly, we believe that our recommendation is warranted and that ONCD should identify outcome-oriented performance measures for the eight cyber threat information sharing initiatives that are included in the *National Cybersecurity Strategy Implementation Plan*.

ONCD's comments are reprinted in appendix II. The agency also provided technical comments, which we incorporated into the report, as appropriate.

In its written comments, DHS concurred with our recommendation that CISA, in coordination with the 14 agencies, should conduct a

⁷³Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

⁷⁴GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, [GAO-16-79](#) (Washington, D.C.: Nov. 19, 2015).

comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the cyber threat sharing challenges (Recommendation 2). The department stated that CISA would coordinate with ONCD to evaluate the feasibility of conducting a comprehensive assessment of existing information sharing methods and determine a path forward, as appropriate. DHS's comments are reprinted in appendix III. DHS also provided technical comments, which we incorporated into the report as appropriate.

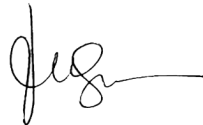
In addition, five agencies—DOE, DOT, FBI, GSA, and USDA—responded that they did not have any comments on the draft report. The remaining four agencies—DOD, EPA, HHS, and Treasury—provided technical comments, which we incorporated into the report as appropriate.

We are sending copies of this report to the appropriate congressional addressees 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 or Tina Won Sherman at (202) 512-8461 or ShermanT@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 IV.



Marisol Cruz Cain
Director, Information Technology and Cybersecurity



Tina Won Sherman
Director, Homeland Security and Justice

List of Addressees

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 Margaret Wood Hassan
Chairwoman
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Frank Lucas
Chairman
Committee on Science, Space, and Technology
House of Representatives

The Honorable Andrew Garbarino
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security
House of Representatives

The Honorable Nancy Mace
Chairwoman
The Honorable Gerald E. Connolly

Ranking Member
Subcommittee on Cybersecurity, Information Technology, and
Government Innovation
Committee on Oversight and Accountability
House of Representatives

The Honorable Jay Obernolte
Chairman
Subcommittee on Investigation and Oversight
Committee on Science, Space and Technology
House of Representatives

The Honorable Angus S. King, Jr.
United States Senate

The Honorable Thom Tillis
United States Senate

The Honorable Mike Gallagher
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The specific objectives for this report were to examine (1) how federal agencies and critical infrastructure owners and operators share cyber threat information with each other, and (2) the factors that facilitate and challenge cyber threat information sharing and the extent to which federal agencies have taken action to address the challenging factors.¹

To address the first objective, we selected the 14 primary federal agencies responsible for sharing cyber threat information with critical infrastructure owners and operators. In particular, we selected

- Thirteen federal departments or agencies (including components within some agencies), designated by presidential directive as a sector risk management agency (SRMA) or co-SRMA.² Specifically, we selected the (1) Department of Agriculture, (2) Department of Defense, (3) Department of Energy, (4) Department of Transportation, (5) Department of the Treasury, (6) Department of Health and Human Services' (HHS) Food and Drug Administration, (7) HHS's Administration for Strategic Preparedness and Response,³ (8)

¹For the purposes of our review, we define the word “share” and “sharing” to mean information that (1) critical infrastructure owners and operators share with federal agencies and (2) federal agencies share with critical infrastructure owners and operators.

²Presidential Policy Directive-21 (PPD-21) previously called these agencies Sector-Specific Agencies. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified Sector-Specific Agencies as SRMAs. See 6 U.S.C. § 652a(c)(3). In 2013, PPD-21 categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as SRMA for the sector, although the number of sectors and SRMA assignments are subject to review and modification. Those designations are still in effect.

³We obtained responses from HHS's Administration for Strategic Preparedness and Response and Food and Drug Administration on methods to share threat information in the healthcare and public health sector. For purposes of describing the department's collective efforts to share cyber threat information in the healthcare and public health sector, we aggregated the responses of the Administration for Strategic Preparedness and Response and the Food and Drug Administration and referred to those efforts as being performed by “HHS.” By contrast, only HHS agency—the Food and Drug Administration—has responsibilities in the food and agriculture sector. As such, we referred to efforts in the food and agriculture sector as being performed by the Food and Drug Administration or “FDA”.

Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, (9) Department of Homeland Security's Federal Protective Service, (10) Department of Homeland Security's Transportation Security Administration, (11) Department of Homeland Security's U.S. Coast Guard, (12) Environmental Protection Agency, and (13) General Services Administration. We selected the departments, EPA, and GSA because (1) they are designated by presidential directive as SRMAs as authorized by statute and (2) the statute assigns designated agencies responsibility for assisting critical infrastructure owners and operators with identifying threats. We also selected the components of HHS and the Department of Homeland Security because we identified their threat information sharing responsibilities in our prior reports.

- The Federal Bureau of Investigation (FBI). We selected the FBI because we identified the agency's threat information sharing responsibilities in federal policy.⁴

We asked the 14 selected federal agencies to provide documentation on methods they use to share cyber threat information with critical infrastructure owners and operators (e.g., descriptions of the methods, types of information shared). We then aligned each method to one of 11 categories. To develop the 11 categories, we first aligned the methods to an existing threat information category that was identified and summarized by the National Institute of Standards and Technology's *Guide to Cyber Threat Information Sharing*: threat information products.⁵

For those methods that did not align to the existing categories, we performed a content analysis on each of the method descriptions to identify and summarize 10 additional categories. We then aligned those remaining methods to these new categories. To further organize and describe these 11 categories for this report, we assigned each of the 11 categories into either one of two larger groups—cybersecurity and law enforcement services and collaborative sharing environments—based on the category description.

⁴Specifically, PPD-21, issued in February 2013, called for the Department of Justice, including the FBI, to lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. In addition, the FBI is to conduct domestic collection, analysis, and dissemination of cyber threat information, according to the directive.

⁵National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing*, Special Publication 800-150 (October 2016).

To address the second objective, we conducted structured interviews with officials and representatives from the 14 federal agencies selected for the first objective and seven nonfederal entities. During these interviews, we asked the officials and representatives open-ended questions to identify any factors that facilitated and challenged their abilities to share cyber threat information. The seven nonfederal entities we interviewed were:

- two private sector Information Sharing and Analysis Centers (ISAC)—specifically, the Electricity ISAC and Multi-State ISAC. We selected these organizations because, based on our review of ISAC websites and our prior reports, they are the ISACs that (1) have an agreement with federal agencies to regularly provide agencies with information or disseminate information received from agencies (Multi-State ISAC), (2) operate a threat information sharing service in partnership with a federal agency (Electricity ISAC), or (3) receive federal funding (both ISACs).
- four sector coordinating councils—specifically, the Food and Agriculture Sector Coordinating Council, the Water Sector Coordinating Council, the Electricity Subsector Coordinating Council, and the Oil and Natural Gas Subsector Coordinating Council. We selected these four organizations because, based on our review of ISAC websites and our prior reports, they represent sectors with (1) ISACs that have established a partnership with federal agencies (the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council), or (2) with SRMAs that do not regularly develop cyber threat information sharing reports (Food and Agriculture Sector Coordinating Council and the Water Sector Coordinating Council).
- the State, Local, Tribal, and Territorial Government Coordinating Council. We selected this organization because it represents a sector with an ISAC that has established a partnership with federal agencies (the government facilities sector).

Additionally, we conducted a content analysis of the interview transcripts to identify and categorize factors that were frequently identified as facilitating and challenging. Specifically, two analysts independently reviewed and coded the data with their initial factors. They then compared their coding results and discussed any discrepancies to reach a consensus on the final coding scheme and factors.

Subsequently, we totaled the number of times each factor was identified by federal agencies and nonfederal entities, choosing to report on the factors that were identified by seven or more organizations (i.e., a third or

more of the organizations in our review). We also compared our factors to the most frequently identified challenges highlighted in prior Inspectors General reports.⁶

We then presented the factors that challenged cyber threat information sharing to the selected 14 federal agencies and asked them to provide documentation on actions the agencies have taken or plans they have developed to address those challenges. In addition, we presented the factors that challenged cyber threat information sharing with Office of the National Cyber Director (ONCD)—the office within the White House that is responsible for developing a national cyber strategy—and interviewed ONCD officials on their plans for addressing the challenges. We also compared the White House’s *National Cybersecurity Strategy* and accompanying implementation plan⁷ with the following practices highlighted in our prior work on national strategies and business process reengineering: (1) developing planned actions that address relevant challenges, (2) identifying outcome-oriented performance measures, and (3) reassessing whether existing processes are optimal for addressing challenges.⁸

We conducted this performance audit from October 2021 to September 2023 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

⁶See, e.g., Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2021-002-U (Washington, D.C.: Dec. 9, 2021); *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Report No. AUD-2019-005-U (Washington, D.C.: Dec. 19, 2019); and *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, Audit Report No. AUD-2017-005 (Washington, D.C.: Dec. 19, 2017).

⁷The White House, *National Cybersecurity Strategy*, (Washington, D.C.: March 2023) and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

⁸GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, [GAO-17-300](#) (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, [GAO-15-602](#) (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, [GAO-05-372](#) (Washington, D.C.: Sept. 8, 2005); *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); and *Business Process Reengineering Assessment Guide*, Version 3, [GAO/AIMD-10.1.15](#) (Washington, D.C.: May 1997).

**Appendix I: Objectives, Scope, and
Methodology**

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 Office of the National Cyber Director

**Appendix II: Comments from the Office of the
National Cyber Director**



**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF THE NATIONAL CYBER DIRECTOR**
WASHINGTON, D.C. 20503

August 28, 2023

Dear General Dodaro,

Thank you for the opportunity to respond in writing to GAO's report entitled "National Cybersecurity Strategy Needs to Address Information Sharing Challenges, Performance Measures, and Methods." We appreciate GAO's longstanding interest in cybersecurity challenges facing the U.S. government and our nation and the work that went into preparing this report.

The report has two findings and corresponding recommendations that pertain to the Office of the National Cyber Director (ONCD). In addition to our response to those findings, we share our views on the third recommendation, which is directed toward the Cybersecurity and Infrastructure Security Agency (CISA), as it implicates the National Cybersecurity Strategy as well.

As discussed below, our response reflects the fact that the National Cybersecurity Strategy Implementation Plan (NCSIP) is a "living document that will be updated annually. Initiatives will be added as the evolving cyber landscape demands and removed after completion."¹

Finding 1 – The Strategy and Implementation Plan Do Not Fully Address Cyber Threat Information Sharing Challenges

ONCD does not concur with this finding or its corresponding recommendation. The finding notes that the NCSIP addresses four of the six cyber threat information challenges identified by GAO during its review. ONCD agrees that those four challenges ("limited relationships," "limited funding and resources," "limited sharing of classified or sensitive information," and "lack of actionable information") are addressed by the eight NCSIP initiatives GAO highlights in its report. However, the NCSIP also addresses the two other challenges identified in the report. These are discussed below.

Limited Voluntary Sharing

GAO states that the NCSIP only partially addresses the challenge of "limited voluntary sharing" of information. It acknowledges that the issuance of the final Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) rule, as required in NCSIP Initiative 1.4.2, will likely result in more sharing of incident-related information but raises concerns that implementation of CIRCA will "likely not increase voluntary sharing related to unsuccessful attempts" at breaches.² This interpretation of CIRCA

¹ National Cybersecurity Strategy Implementation Plan, at p.4.

² In the draft report provided to ONCD for comment, GAO did not include any evidence that the fourteen agencies interviewed for this report identified limited sharing of unsuccessful attempts as a distinct challenge. In the summary of survey results, GAO mentions a statement from CISA that it receives very few voluntary reports of cyber incidents, but that is distinct from unsuccessful attempts. In any event, GAO acknowledges that reports of cyber incidents will increase with the implementation of the CIRCA mandatory reporting rule, and as discussed in ONCD's comments, the CIRCA rule is expected to increase voluntary sharing of cyber incident information,

**Appendix II: Comments from the Office of the
National Cyber Director**

implementation focuses on the mandatory reporting of incidents while ignoring incentives in the law to share information voluntarily, including information about unsuccessful hacking attempts.

Initiative 1.4.2 in the NCSIP requires CISA to issue the final rule implementing CIRCIA by the fourth quarter of Fiscal Year 2025. CIRCIA contains provisions³ that extend protections for voluntary sharing of incident information similar to those that exist for the sharing of cyber threat indicators and defensive measures under the Cybersecurity Information Sharing Act of 2015.⁴ The protections associated with voluntary sharing extend broadly to incidents that would not meet the threshold for mandatory sharing (because they are not “substantial”) and apply to all entities, not just those defined during the CIRCIA rulemaking process as being “covered entities.”⁵ Accordingly, implementation of CIRCIA is expected to increase the willingness of all entities to share incident-related information with the government voluntarily, including information about unsuccessful attempts.

GAO’s draft report also fails to account for other NCSIP initiatives that will improve voluntary sharing of information, including unsuccessful attempts to compromise systems. The draft report acknowledges that one barrier to voluntary sharing has been the perception of private sector entities that they do not receive actionable or enriched information from the government in response to their sharing indicators like malware signatures. However, while the draft report appropriately acknowledges that the NCSIP has eight initiatives that address challenges in information sharing, it fails to recognize that improvements in the Federal government’s sharing of sensitive information through implementation of Initiatives 1.3.1, 1.2.3, 1.2.5, 2.3.1, 2.3.2, 1.4.1, and 1.2.4 will incentivize additional voluntary information sharing by the private sector.

While ONCD agrees with the finding that limited voluntary sharing is a challenge, eight initiatives in the NCSIP directly or indirectly address it. ONCD does not concur with this portion of the finding.⁶

Lack of Timely Sharing

GAO’s draft report states that the NCSIP does not address the “lack of timely sharing” of information. This is incorrect. Two of the initiatives in the NCSIP fall under the Strategic Objective entitled “Increase the Speed and Scale of Intelligence Sharing and Victim Notification.” In addition, other initiatives in the NCSIP identified by GAO as being responsive to other identified information sharing challenges will also improve timely sharing of information.

including unsuccessful hacking attempts. Note that GAO’s observation of low private sector participation in Department of Energy and CISA sensor programs is not the type of “voluntary sharing” discussed in Finding One, and in any event, the Federal government has improved the integration of cyber threat intelligence feeds and this will enable increased identification of unsuccessful attempts to compromise a network.

³ See 6 U.S.C. § 681c(c).

⁴ See 6 U.S.C. § 1504.

⁵ See 6 U.S.C. § 681c.

⁶ It is worth noting that, for the specific concerns GAO identifies related to unsuccessful attempts that are blocked in some way, the U.S. Government is taking several steps to encourage collection of relevant artifacts. Implementation of EO 14028 and the Zero Trust Architecture Strategy, both of which call for increased endpoint detection and response (EDR) capabilities (guidance that has also been repeated to critical infrastructure owners and operators), will enhance automated collection of exactly these kinds of indicators. Many next generation EDR capabilities are also connected to the cloud, allowing for near real-time sharing of “near misses.” This is not directly related to voluntary sharing, but it would likely be effective at addressing the underlying concern about unsuccessful attempts to compromise systems.

**Appendix II: Comments from the Office of the
National Cyber Director**

NCSIP Initiative 2.3.2 requires ODNI to leverage the deliverables and lessons learned from implementation of Section 4 of Executive Order 13636,⁷ and review policies and procedures for sharing cyber threat intelligence with critical infrastructure owners and operators. This initiative advances the purpose of EO 13636, which is “to increase the volume, timeliness, and quality of cyber threat information shared with the U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.”⁸ Reviewing those policies and processes in light of the current cyber threat landscape and technological ecosystem, and taking action to address any identified gaps will not only increase the sharing of actionable information, it will also improve the timeliness of sharing. Delays in the sharing of information can result from concerns that sharing might reveal the sources and methods used to collect it. By working to improve sanitization processes and clear appropriate private sector personnel, the timeliness of sharing could be significantly improved. By addressing upstream issues like more robust sanitization processes, key impediments to timely sharing would be removed.

The GAO draft report also does not account for NCSIP initiatives aimed at improving machine-to-machine sharing and at strengthening integration among Federal Cybersecurity Centers (and emerging cybersecurity collaboration centers), both of which address a separate challenge related to timely sharing: the technology underpinning the information exchange.

NCSIP Initiative 1.2.3 requires CISA to work with sector risk management agencies to explore how to use common platforms for information sharing across government agencies charged with protecting critical infrastructure. Machine-to-machine sharing of information across these agencies would be significantly faster than manual processes such as email, and would therefore help increase the timely sharing of information, as well as increase the amount of data that can be shared.

Initiative 1.3.1, which focuses on integrating the Federal Cybersecurity Centers and emerging Federal cybersecurity collaboration centers could similarly improve timely sharing among a subset of operational agencies. Some of those agencies interface directly with private sector entities. For sectors that do not have a specific collaboration center, speedier information sharing by other agencies with CISA could be leveraged using existing channels or those contemplated in Initiative 1.2.3 to get relevant indicators out to private sector owners and operators more quickly.

While ONCD does agree with GAO that the timely sharing of information is a challenge, several initiatives in the NCSIP specifically address it. Therefore, ONCD does not concur with this portion of the finding.

Conclusion

Because existing initiatives in the NCSIP address all six of the information sharing challenges identified by GAO, ONCD does not concur with the first finding in the report. ONCD therefore also does not concur with GAO’s recommendation to update the NCSIP with new initiatives to address “limited voluntary sharing” and “lack of timely sharing.” ONCD will continue to update the NCSIP on an annual basis to reflect progress made and the changing ecosystem.

⁷ Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013).

⁸ *Id.* (emphasis added).

Finding 2 – The Strategy and Implementation Plan Do Not Identify Outcome-Oriented Performance Measures

ONCD concurs with this finding. ONCD agrees with GAO that the NCSIP does not identify specific outcome-oriented performance measures to assess the effectiveness of the eight information sharing-related initiatives identified by GAO. While ONCD intends to develop performance measures for the Implementation Plan, in the cybersecurity field in general there remains a lack of validated, outcome-based performance measures for this kind of cybersecurity information sharing. Thus, ONCD believes it is premature for a recommendation to update the NCSIP to include them.

ONCD is tracking programmatic performance measures associated with each initiative related to information sharing in the NCSIP. While it would be beneficial to tie the initiatives to measurable outcomes, as GAO suggests, developing outcome-based performance measures for cybersecurity effectiveness is a challenging topic that will likely require years of work and research to address, especially given the lack of validated cybersecurity metrics across a range of desired outcomes.⁹

ONCD accepts this finding. However, the associated recommendation – that the NCD identify performance measures for the cyber threat initiatives in the NCSIP – is problematic. Without research to develop such performance metrics, the NCD will be severely limited in their ability to identify and develop effective metrics. While ONCD notes that the challenges GAO identifies in the report are themselves not based on outcome-oriented performance measures, ONCD would welcome insights from GAO as to what outcome-based performance measures they have used in other studies of information sharing that could be applicable to future versions of the NCSIP.

Finding 3 - Strategy and Implementation Plan Do Not Assess the Current Mix of Cyber Threat Information Sharing Approaches

ONCD concurs in part with this finding. ONCD takes no position on the recommendation to CISA associated with it. GAO is correct that the 2023 NCSIP does not require an assessment of the current mix of information sharing approaches across the government, but ONCD notes that the NCSIP sets the stage for such an assessment in the future.

GAO acknowledges that NCSIP Initiative 1.2.4 requires CISA and SRMAs to investigate new and improved information sharing and collaboration mechanisms.¹⁰ GAO also recognizes that Initiative 1.2.4 calls for the development of a maturity model for collaboration based on emerging collaboration methods. Such a maturity model is expected to form the basis of the very type of assessment GAO is requesting.

ONCD would welcome a GAO recommendation that the maturity model be used to conduct such an assessment in a future National Cybersecurity Strategy Implementation Plan; however, because of the

⁹ There may be output-based (rather than outcome-based) measures that could be put into place; however, without demonstrated correlation to outcomes, their use could result in programs that optimize measures in a way that, at best, does not actually improve cybersecurity – and, at worst, exacerbates challenges.

¹⁰ GAO also notes that the initiative in question (1.2.4) does not require CISA to collaborate with the FBI, despite the fact that the FBI operates more than half of the cyber threat information sharing methods identified in the report. However, GAO ignores initiative 1.2.3, which requires CISA collaborate with the FBI and specifically addresses sharing of information across government to ensure that all agencies that collect and analyze relevant information are able to distribute it, regardless of whether a centralized or federated model is deemed most effective going forward. ONCD suggests GAO update the finding to reflect this fact.

**Appendix II: Comments from the Office of the
National Cyber Director**

timelines associated with the initiatives in the 2023 NCSIP,¹¹ it did not make sense to require an assessment that would not begin until 2026. ONCD does not take a position on GAO's existing recommendation, which is directed to CISA.

Conclusion

Thank you again for the opportunity to comment on this product and on your collaborative approach throughout this review. ONCD would welcome further conversations on how to update the report to reflect our concerns.

Sincerely,

James Halpert
General Counsel

¹¹ The NCSIP is a living document that will be updated on an annual basis.

Accessible Text for Appendix II: Comments from the Office of the National Cyber Director

August 28, 2023

Dear General Dodaro,

Thank you for the opportunity to respond in writing to GAO's report entitled "National Cybersecurity Strategy Needs to Address Information Sharing Challenges, Performance Measures, and Methods." We appreciate GAO's longstanding interest in cybersecurity challenges facing the U.S. government and our nation and the work that went into preparing this report.

The report has two findings and corresponding recommendations that pertain to the Office of the National Cyber Director (ONCD). In addition to our response to those findings, we share our views on the third recommendation, which is directed toward the Cybersecurity and Infrastructure Security Agency (CISA), as it implicates the National Cybersecurity Strategy as well.

As discussed below, our response reflects the fact that the National Cybersecurity Strategy Implementation Plan (NCSIP) is a "living document that will be updated annually. Initiatives will be added as the evolving cyber landscape demands and removed after completion."¹

Finding 1 – The Strategy and Implementation Plan Do Not Fully Address Cyber Threat Information Sharing Challenges

ONCD does not concur with this finding or its corresponding recommendation. The finding notes that the NCSIP addresses four of the six cyber threat information challenges identified by GAO during its review. ONCD agrees that those four challenges ("limited relationships," "limited funding and resources," "limited sharing of classified or sensitive information," and "lack of actionable information") are addressed by the eight NCSIP initiatives GAO highlights in its report. However, the NCSIP also addresses the two other challenges identified in the report. These are discussed below.

¹ National Cybersecurity Strategy Implementation Plan, at p.4.

Limited Voluntary Sharing

GAO states that the NCSIP only partially addresses the challenge of “limited voluntary sharing” of information. It acknowledges that the issuance of the final Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule, as required in NCSIP Initiative 1.4.2, will likely result in more sharing of incident-related information but raises concerns that implementation of CIRCIA will “likely not increase voluntary sharing related to unsuccessful attempts” at breaches.² This interpretation of CIRCIA implementation focuses on the mandatory reporting of incidents while ignoring incentives in the law to share information voluntarily, including information about unsuccessful hacking attempts.

Initiative 1.4.2 in the NCSIP requires CISA to issue the final rule implementing CIRCIA by the fourth quarter of Fiscal Year 2025. CIRCIA contains provisions³ that extend protections for voluntary sharing of incident information similar to those that exist for the sharing of cyber threat indicators and defensive measures under the Cybersecurity Information Sharing Act of 2015.⁴ The protections associated with voluntary sharing extend broadly to incidents that would not meet the threshold for mandatory sharing (because they are not “substantial”) and apply to all entities, not just those defined during the CIRCIA rulemaking process as being “covered entities.”⁵ Accordingly, implementation of CIRCIA is expected to increase the willingness of all entities to share incident-related information with the government voluntarily, including information about unsuccessful attempts.

GAO’s draft report also fails to account for other NCSIP initiatives that will improve voluntary sharing of information, including unsuccessful attempts to compromise systems. The draft report acknowledges that one barrier to voluntary sharing has

² In the draft report provided to ONCD for comment, GAO did not include any evidence that the fourteen agencies interviewed for this report identified limited sharing of unsuccessful attempts as a distinct challenge. In the summary of survey results, GAO mentions a statement from CISA that it receives very few voluntary reports of cyber incidents, but that is distinct from unsuccessful attempts. In any event, GAO acknowledges that reports of cyber incidents will increase with the implementation of the CIRCIA mandatory reporting rule, and as discussed in ONCD’s comments, the CIRCIA rule is expected to increase voluntary sharing of cyber incident information, including unsuccessful hacking attempts. Note that GAO’s observation of low private sector participation in Department of Energy and CISA sensor programs is not the type of “voluntary sharing” discussed in Finding One, and in any event, the Federal government has improved the integration of cyber threat intelligence feeds and this will enable increased identification of unsuccessful attempts to compromise a network.

³ See 6 U.S.C. § 681c(c).

⁴ See 6 U.S.C § 1504.

⁵ See 6 U.S.C. § 681c.

been the perception of private sector entities that they do not receive actionable or enriched information from the government in response to their sharing indicators like malware signatures. However, while the draft report appropriately acknowledges that the NCSIP has eight initiatives that address challenges in information sharing, it fails to recognize that improvements in the Federal government's sharing of sensitive information through implementation of Initiatives 1.3.1, 1.2.3, 1.2.5, 2.3.1, 2.3.2, 1.4.1, and 1.2.4 will incentivize additional voluntary information sharing by the private sector.

While ONCD agrees with the finding that limited voluntary sharing is a challenge, eight initiatives in the NCSIP directly or indirectly address it. ONCD does not concur with this portion of the finding.⁶

Lack of Timely Sharing

GAO's draft report states that the NCSIP does not address the "lack of timely sharing" of information. This is incorrect. Two of the initiatives in the NCSIP fall under the Strategic Objective entitled "Increase the Speed and Scale of Intelligence Sharing and Victim Notification." In addition, other initiatives in the NCSIP identified by GAO as being responsive to other identified information sharing challenges will also improve timely sharing of information.

NCSIP Initiative 2.3.2 requires ODNI to leverage the deliverables and lessons learned from implementation of Section 4 of Executive Order 13636,⁷ and review policies and procedures for sharing cyber threat intelligence with critical infrastructure owners and operators. This initiative advances the purpose of EO 13636, which is "to increase the volume, timeliness, and quality of cyber threat information shared with the U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."⁸ Reviewing those policies and processes in light of the current cyber threat landscape and technological ecosystem, and taking action to address any identified gaps will not

⁶ It is worth noting that, for the specific concerns GAO identifies related to unsuccessful attempts that are blocked in some way, the U.S. Government is taking several steps to encourage collection of relevant artifacts. Implementation of EO 14028 and the Zero Trust Architecture Strategy, both of which call for increased endpoint detection and response (EDR) capabilities (guidance that has also been repeated to critical infrastructure owners and operators), will enhance automated collection of exactly these kinds of indicators. Many next generation EDR capabilities are also connected to the cloud, allowing for near real-time sharing of "near misses." This is not directly related to voluntary sharing, but it would likely be effective at addressing the underlying concern about unsuccessful attempts to compromise systems.

⁷ Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013).

⁸ *Id.* (emphasis added).

only increase the sharing of actionable information, it will also improve the timeliness of sharing. Delays in the sharing of information can result from concerns that sharing might reveal the sources and methods used to collect it. By working to improve sanitization processes and clear appropriate private sector personnel, the timeliness of sharing could be significantly improved. By addressing upstream issues like more robust sanitization processes, key impediments to timely sharing would be removed.

The GAO draft report also does not account for NCSIP initiatives aimed at improving machine-to-machine sharing and at strengthening integration among Federal Cybersecurity Centers (and emerging cybersecurity collaboration centers), both of which address a separate challenge related to timely sharing: the technology underpinning the information exchange.

NCSIP Initiative 1.2.3 requires CISA to work with sector risk management agencies to explore how to use common platforms for information sharing across government agencies charged with protecting critical infrastructure. Machine-to-machine sharing of information across these agencies would be significantly faster than manual processes such as email, and would therefore help increase the timely sharing of information, as well as increase the amount of data that can be shared.

Initiative 1.3.1, which focuses on integrating the Federal Cybersecurity Centers and emerging Federal cybersecurity collaboration centers could similarly improve timely sharing among a subset of operational agencies. Some of those agencies interface directly with private sector entities. For sectors that do not have a specific collaboration center, speedier information sharing by other agencies with CISA could be leveraged using existing channels or those contemplated in Initiative 1.2.3 to get relevant indicators out to private sector owners and operators more quickly.

While ONCD does agree with GAO that the timely sharing of information is a challenge, several initiatives in the NCSIP specifically address it. Therefore, ONCD does not concur with this portion of the finding.

Conclusion

Because existing initiatives in the NCSIP address all six of the information sharing challenges identified by GAO, ONCD does not concur with the first finding in the report. ONCD therefore also does not concur with GAO's recommendation to update the NCSIP with new initiatives to address "limited voluntary sharing" and "lack of timely sharing." ONCD will continue to update the NCSIP on an annual basis to reflect progress made and the changing ecosystem.

Finding 2 – The Strategy and Implementation Plan Do Not Identify Outcome-Oriented Performance Measures

ONCD concurs with this finding. ONCD agrees with GAO that the NCSIP does not identify specific outcome-oriented performance measures to assess the effectiveness of the eight information sharing-related initiatives identified by GAO. While ONCD intends to develop performance measures for the Implementation Plan, in the cybersecurity field in general there remains a lack of validated, outcome-based performance measures for this kind of cybersecurity information sharing. Thus, ONCD believes it is premature for a recommendation to update the NCSIP to include them.

ONCD is tracking programmatic performance measures associated with each initiative related to information sharing in the NCSIP. While it would be beneficial to tie the initiatives to measurable outcomes, as GAO suggests, developing outcome-based performance measures for cybersecurity effectiveness is a challenging topic that will likely require years of work and research to address, especially given the lack of validated cybersecurity metrics across a range of desired outcomes.⁹

ONCD accepts this finding. However, the associated recommendation – that the NCD identify performance measures for the cyber threat initiatives in the NCSIP – is problematic. Without research to develop such performance metrics, the NCD will be severely limited in their ability to identify and develop effective metrics. While ONCD notes that the challenges GAO identifies in the report are themselves not based on outcome-oriented performance measures, ONCD would welcome insights from GAO as to what outcome-based performance measures they have used in other studies of information sharing that could be applicable to future versions of the NCSIP.

Finding 3 - Strategy and Implementation Plan Do Not Assess the Current Mix of Cyber Threat Information Sharing Approaches

ONCD concurs in part with this finding. ONCD takes no position on the recommendation to CISA associated with it. GAO is correct that the 2023 NCSIP does not require an assessment of the current mix of information sharing approaches across the government, but ONCD notes that the NCSIP sets the stage for such an assessment in the future.

⁹ There may be output-based (rather than outcome-based) measures that could be put into place; however, without demonstrated correlation to outcomes, their use could result in programs that optimize measures in a way that, at best, does not actually improve cybersecurity – and, at worst, exacerbates challenges.

GAO acknowledges that NCSIP Initiative 1.2.4 requires CISA and SRMAs to investigate new and improved information sharing and collaboration mechanisms.¹⁰ GAO also recognizes that Initiative 1.2.4 calls for the development of a maturity model for collaboration based on emerging collaboration methods. Such a maturity model is expected to form the basis of the very type of assessment GAO is requesting.

ONCD would welcome a GAO recommendation that the maturity model be used to conduct such an assessment in a future National Cybersecurity Strategy Implementation Plan; however, because of the timelines associated with the initiatives in the 2023 NCSIP,¹¹ it did not make sense to require an assessment that would not begin until 2026. ONCD does not take a position on GAO's existing recommendation, which is directed to CISA.

Conclusion

Thank you again for the opportunity to comment on this product and on your collaborative approach throughout this review. ONCD would welcome further conversations on how to update the report to reflect our concerns.

Sincerely,

James Halpert
General Counsel

¹⁰ GAO also notes that the initiative in question (1.2.4) does not require CISA to collaborate with the FBI, despite the fact that the FBI operates more than half of the cyber threat information sharing methods identified in the report. However, GAO ignores initiative 1.2.3, which requires CISA collaborate with the FBI and specifically addresses sharing of information across government to ensure that all agencies that collect and analyze relevant information are able to distribute it, regardless of whether a centralized or federated model is deemed most effective going forward. ONCD suggests GAO update the finding to reflect this fact.

¹¹ The NCSIP is a living document that will be updated on an annual basis.

Appendix III: Comments from the Department of Homeland Security

**Appendix III: Comments from the Department
of Homeland Security**

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



August 21, 2023

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

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105468, "CRITICAL
INFRASTRUCTURE PROTECTION: National Cybersecurity Strategy Needs to
Address Information Sharing Challenges, Performance Measures, and Methods"

Dear Mses. Cruz Cain and Sherman:

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 of the breadth of Cybersecurity and Infrastructure Security Agency's (CISA) information sharing methods and programs. CISA facilitates—and is working to strengthen—cyber threat information sharing both among federal agencies and between the federal government and non-federal entities. For example, CISA has developed and implemented numerous information sharing programs, including the Multi-State Information Sharing and Analysis Center which is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and tribal governments.

Information sharing is essential to furthering cybersecurity for the nation. Sharing cyber threat information increases awareness about potential threats that might otherwise be

**Appendix III: Comments from the Department
of Homeland Security**

undiscovered by an organization or a community. By rapidly sharing critical information about attacks and vulnerabilities, the scope and magnitude of cyber events can be greatly decreased. DHS is committed to continuing to lead in this important mission-critical focus area and will continue to meet current and future related threat information sharing objectives established by and with its partners and those envisioned for CISA in the recently released “National Cybersecurity Strategy,” dated March 1, 2023.¹

The draft report contained three recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the 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: 2023.08.21 08:44:35 -04'00'

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

Enclosure

¹ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

Enclosure: Management Response to Recommendation Contained in GAO-23-105468

GAO recommended that the Director of CISA:

Recommendation 1: In coordination with the 14 agencies, should conduct a comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the cyber threat sharing challenges—including whether existing sharing methods should be retired in favor of centralized or federated approaches.

Response: Concur. CISA Cybersecurity Division (CSD) will coordinate with the Office of the National Cyber Director (ONCD), Executive Office of the President to evaluate the feasibility of conducting a comprehensive assessment of whether existing information sharing methods are sufficient. CISA CSD will then determine a path forward, as appropriate once the feasibility evaluation is completed.

Summary of key milestones:

Action	Estimated Completion Date
Engage with ONCD to evaluate the feasibility of conducting a comprehensive assessment of information sharing methods.	October 31, 2023
If determined efforts should move forward, CSD will work with ONCD to complete feasibility evaluation.	March 31, 2024
Based on results of feasibility evaluation, CSD will work with ONCD to conduct and complete comprehensive assessment.	August 31, 2025

Overall ECD: August 31, 2025.

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

August 21, 2023

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

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105468, “CRITICAL
INFRASTRUCTURE PROTECTION: National Cybersecurity Strategy Needs to
Address Information Sharing Challenges, Performance Measures, and Methods”

Dear Mses. Cruz Cain and Sherman:

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 of the breadth of Cybersecurity and Infrastructure Security Agency’s (CISA) information sharing methods and programs. CISA facilitates—and is working to strengthen—cyber threat information sharing both among federal agencies and between the federal government and non- federal entities. For example, CISA has developed and implemented numerous information sharing programs, including the Multi-State Information Sharing and Analysis Center which is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and tribal governments.

Information sharing is essential to furthering cybersecurity for the nation. Sharing cyber threat information increases awareness about potential threats that might otherwise be undiscovered by an organization or a community. By rapidly sharing critical information about attacks and vulnerabilities, the scope and magnitude of cyber events can be greatly decreased. DHS is committed to continuing to lead in this important mission-critical focus area and will continue to meet current and future related threat information sharing objectives established by and with its partners and those envisioned for CISA in the recently released “National Cybersecurity Strategy,” dated March 1, 2023.¹

The draft report contained three recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the 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,

Digitally signed by JIM H
JIM H CRUMPACKER CRUMPACKER
Date: 2023.08.21 08:44:35 -04'00'

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

Enclosure

Enclosure: Management Response to Recommendation Contained in GAO-23-105468

GAO recommended that the Director of CISA:

Recommendation 1: In coordination with the 14 agencies, should conduct a comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the

¹ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

cyber threat sharing challenges—including whether existing sharing methods should be retired in favor of centralized or federated approaches.

Response: Concur. CISA Cybersecurity Division (CSD) will coordinate with the Office of the National Cyber Director (ONCD), Executive Office of the President to evaluate the feasibility of conducting a comprehensive assessment of whether existing information sharing methods are sufficient. CISA CSD will then determine a path forward, as appropriate once the feasibility evaluation is completed.

Summary of key milestones:

Action	Estimated Completion Date
Engage with ONCD to evaluate the feasibility of conducting a comprehensive assessment of information sharing methods.	October 31, 2023
If determined efforts should move forward, CSD will work with ONCD to complete feasibility evaluation.	March 31, 2024
Based on results of feasibility evaluation, CSD will work with ONCD to conduct and complete comprehensive assessment.	August 31, 2025

Overall ECD: August 31, 2025.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Tina Won Sherman, (202) 512-8461 or ShermanT@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Kaelin Kuhn (Assistant Director), Hugh Paquette (Assistant Director), Sukhjoot Singh (Analyst-In-Charge), Tommy Baril, Brandon Berney, Christopher Businsky, Rebecca Eyer, Maxwell Kaufman, Joe Kirschbaum, Ceara Lance, Noah Levesque, Melissa Melvin, Ahsan Nasar, Scott Pettis, Andrew Stavisky, and Adam Vodraska 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



Please Print on Recycled Paper.