United States Government Accountability Office

Report to Congressional Addressees

January 2024

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support

GAO-24-106221

GAO
Highlights

Highlights of GAO-24-106221, a report to congressional addressees

January 2024

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support

Why GAO Did This Study

The nation’s 16 critical infrastructure sectors provide essential services such as electricity, healthcare, and gas and oil distribution. However, cyber threats to critical infrastructure, such as ransomware, represent a significant national security challenge.

This report (1) describes the reported impact of ransomware attacks on the nation’s critical infrastructure, (2) assesses federal agency efforts to oversee sector adoption of leading federal practices, and (3) evaluates federal agency efforts to assess ransomware risks and the effectiveness of related support.

To do so, GAO selected four critical infrastructure sectors—critical manufacturing, energy, healthcare and public health, and transportation systems. For each sector, GAO analyzed documentation, such as incident reporting and risk analysis, and compared efforts to leading cybersecurity guidance. GAO also interviewed sector and federal agency officials to obtain information on ransomware-related impacts, practices, and support.

What GAO Recommends

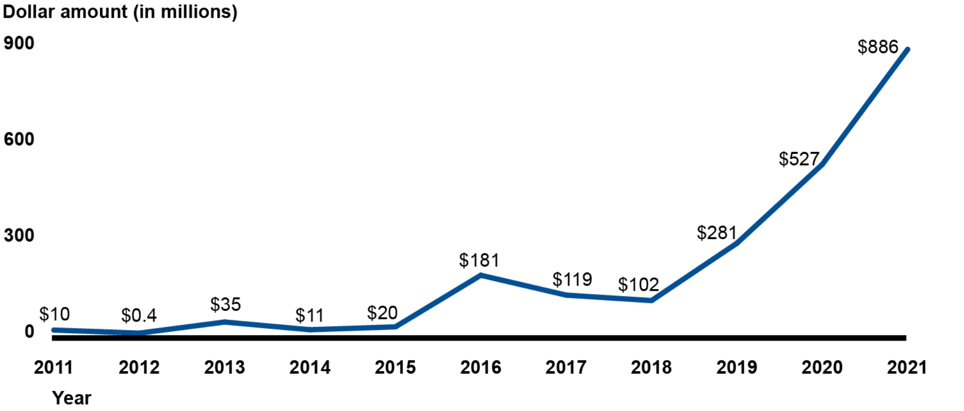
GAO is making 11 recommendations to four agencies to, among other things, determine selected sectors’ adoption of cybersecurity practices. DHS and HHS agreed with their recommendations. DOE partially agreed with one recommendation and disagreed with another. DOT agreed with one recommendation, partially agreed with one, and disagreed with a third. GAO continues to believe that the recommendations are valid.

View GAO-24-106221. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

What GAO Found

Ransomware—software that makes data and systems unusable unless ransom payments are made—is having increasingly devastating impacts. For example, the Department of the Treasury reported that the total value of U.S. ransomware-related incidents reached $886 million in 2021, a 68 percent increase compared to 2020 (see figure).

Treasury Reported Dollar Value of U.S. Ransomware-Related Incidents



Source: GAO analysis of Department of the Treasury data. | GAO-24-106221

In addition to monetary losses, ransomware has led to other impacts, such as the inability to provide emergency care when hospital IT systems are unusable. The FBI reported that 870 critical infrastructure organizations were victims of ransomware in 2022, affecting 14 of the 16 critical infrastructure sectors. Among those incidents, almost half were from four sectors—critical manufacturing, energy, healthcare and public health, and transportation systems. The full impact of ransomware is likely not known because reporting is generally voluntary. The Department of Homeland Security is planning to issue new reporting rules by March 2024 that could provide a more complete picture of ransomware’s impact.

The four selected sectors’ adoption of leading practices to address ransomware is largely unknown. None of the federal agencies designated as the lead for risk management for selected sectors have determined the extent of adoption of the National Institute of Standards and Technology’s recommended practices for addressing ransomware. Doing so would help the lead federal agencies be a more effective partner in national efforts to combat ransomware.

Most of the six selected lead federal agencies have assessed or plan to assess risks of cybersecurity threats including ransomware for their respective sectors, as required by law. Regarding lead agencies assessing their support of sector efforts to address ransomware, half of the agencies have evaluated aspects of their support. For example, agencies have received and assessed feedback on their ransomware guidance and briefings. However, none have fully assessed the effectiveness of their support to sectors, as recommended by the National Infrastructure Protection Plan. Fully assessing effectiveness could help address sector concerns about agency communication, coordination, and timely sharing of threat and incident information.

Contents

Tables

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
Coast Guard	United States Coast Guard
CSF	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
K-12	kindergarten through grade 12
NIST	National Institute of Standards and Technology
NDAA	National Defense Authorization Act
SCC	Sector Coordinating Council
SRMA	Sector Risk Management Agency
TSA	Transportation Security Administration

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.

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

January 30, 2024

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

The Honorable Sam Graves
Chairman
Committee on Transportation and Infrastructure
House of Representatives

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

The nation's 16 critical infrastructure sectors provide essential services—such as electricity distribution, transportation, and hospital care—that underpin American society and are vital to the nation's safety and security.[1] Cyber threats to critical infrastructure illustrate the pressing need to strengthen federal efforts to protect critical infrastructure. For example, a May 2021 cyberattack on an American oil pipeline system led to regional gas shortages. In addition, ransomware attacks targeted health care and essential services during the Coronavirus Disease 2019 (COVID-19) pandemic.

Ransomware—a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable unless ransom payments are made—is a serious and growing threat to

[1] The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

government operations and critical infrastructure organizations. In September 2022, we reported that ransomware threats have escalated over time, and are becoming more sophisticated, pervasive, and costly.[2] In addition, the Cyentia Institute's Information Risk Insights Study, sponsored by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), reported that ransomware became the fourth most frequently reported cybersecurity incident among all cyber incidents in 2022.[3] The institute also reported that ransomware accounted for 15 percent of financial losses from cybersecurity incidents that year.

Recognizing the threat of ransomware to national security, public safety, and economic prosperity, Congress and the Administration have taken steps to help CISA and sector risk management agencies (SRMAs) prioritize efforts to combat ransomware.[4] For example, Congress and the President enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which required CISA to form a Joint Ransomware Task Force.[5] Subsequently, CISA established the interagency task force with the Federal Bureau of Investigation (FBI) as a co-lead agency. According to its charter, the task force is intended to facilitate coordination and collaboration among federal entities and other relevant entities to improve federal actions against ransomware threats.

Further, the White House released its National Cybersecurity Strategy and National Cybersecurity Strategy Implementation Plan in March 2023

[2] GAO, *Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767 (Washington, D.C.: Sept. 14, 2022).

[3] Cyentia Institute, *Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents*, (2022), https://www.cyentia.com/wp-content/uploads/IRIS-2022_Cyentia.pdf.

[4] SRMAs are federal agencies that are designated as the lead for one or more critical infrastructure sectors. Their responsibilities are to facilitate and support the security and resilience programs and associated activities of their designated sector.

[5] The Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted as division Y of the Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (Mar. 15, 2022), required the CISA Director to establish the Joint Ransomware Task Force in consultation with the National Cyber Director, Attorney General, and FBI Director. The act also will require covered entities across critical infrastructure sectors to report "covered cyber incidents" to CISA within 72 hours of reasonably determining a "covered cyber incident" occurred and ransom payments within 24 hours of payment. 6 U.S.C. § 681b(a). CISA has not yet issued rules for such reporting. It has 24 months from the date the act was signed into law to issue the proposed rule, and 18 months from the publication of the proposed rule to publish a final rule. 6 U.S.C. § 681b(b).

and July 2023, respectively.[6] The strategy established an objective to combat cybercrime and defeat ransomware because of ransomware's threat to national security and its impacts on key critical infrastructure services. Among other actions, the implementation plan requires CISA, in coordination with the Joint Ransomware Task Force, SRMAs, and other stakeholders, to support private sector and state, local, tribal, and territorial efforts to mitigate ransomware risk.

We performed our work under the authority of the Comptroller General to conduct an examination of federal efforts to understand sectors' adoption of leading practices against ransomware and support mitigation of related threats. Specifically, our objectives were to (1) describe the reported impact of ransomware attacks on selected critical infrastructure sectors, (2) assess SRMAs' efforts to oversee selected sectors' adoption of leading federal practices to prevent and respond to ransomware attacks, and (3) evaluate the extent to which SRMAs for selected sectors assessed ransomware risks and the effectiveness of their support to help owners and operators address threats.

To do so, we selected four of the 16 critical infrastructure sectors to review. We selected sectors that (1) represented a mix of sectors that were and were not designated as lifeline sectors by DHS; and (2) had experienced relatively high numbers of ransomware incidents and cost impacts based on reports from the public sector, private sector, and academia.[7] The four sectors we selected were critical manufacturing, energy, healthcare and public health, and transportation systems.

To address our first objective, we reviewed reports based on publicly disclosed ransomware incidents and vendor research on ransomware attacks within critical infrastructure sectors. We summarized statistics and trends on the number of ransomware incidents among the selected critical infrastructure sectors from these reports. We also obtained and reviewed data, where available, from CISA and other SRMAs on the number of incidents that sector entities reported. We compared data from

[6] White House, *National Cybersecurity Strategy*, (Washington, D.C.: Mar. 1, 2023); and *National Cybersecurity Strategy Implementation Plan*, (Washington, D.C.: July 13, 2023).

[7] DHS defines a lifeline sector as a sector that is essential to the operation of most critical infrastructure sectors. There are four lifeline sectors: communications, energy, transportation systems, and water and wastewater systems.

federal agencies to public reporting on the ransomware incidents to identify any discrepancies.

To address our second objective, we identified guidance established by the National Institute of Standards and Technology (NIST) that provides a set of practices to address ransomware.[8] We compiled a list of practices that were applicable to all sectors or that were specific to selected sectors. We conducted background research and held discussions with SRMA officials to help identify leading practices to address ransomware. We then asked officials from sector coordinating councils (SCC) (including sub-sector coordinating councils) and information sharing and analysis centers (ISAC)—associated with the four selected sectors—about their sectors' use of NIST or other practices to address ransomware.[9] We also analyzed the extent to which documentation describing the practices demonstrated how they aligned with NIST. We reviewed federal agency documentation to determine if the SRMAs were tracking the implementation of either the NIST ransomware profile practices, or other federal and nonfederal practices in their selected sectors.

To address the third objective, we reviewed agency documentation and summarized the support that SRMAs for selected sectors offered to owners and operators to help address ransomware threats. Based on our review of agency documentation, we identified information, such as risk analysis and feedback, that SRMAs gathered about their efforts to help sectors address ransomware. We then made determinations about the extent to which the agencies had demonstrated that they had gathered information on sector ransomware risks and assessed the risks and effectiveness of their support. Specifically, we identified whether the agency had documented efforts to gather and analyze information on sector ransomware risks. We then assessed whether the agency documented efforts to assess the effectiveness of all, some, or none of its ransomware-related support.

[8] National Institute of Standards and Technology, *Ransomware Risk Management: A Cybersecurity Framework Profile*, NISTIR 8374 (Gaithersburg, MD: February 2022).

[9] SCCs 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. The SRMAs and the SCCs coordinate and collaborate in a voluntary fashion on issues pertaining to their respective critical infrastructure sectors.

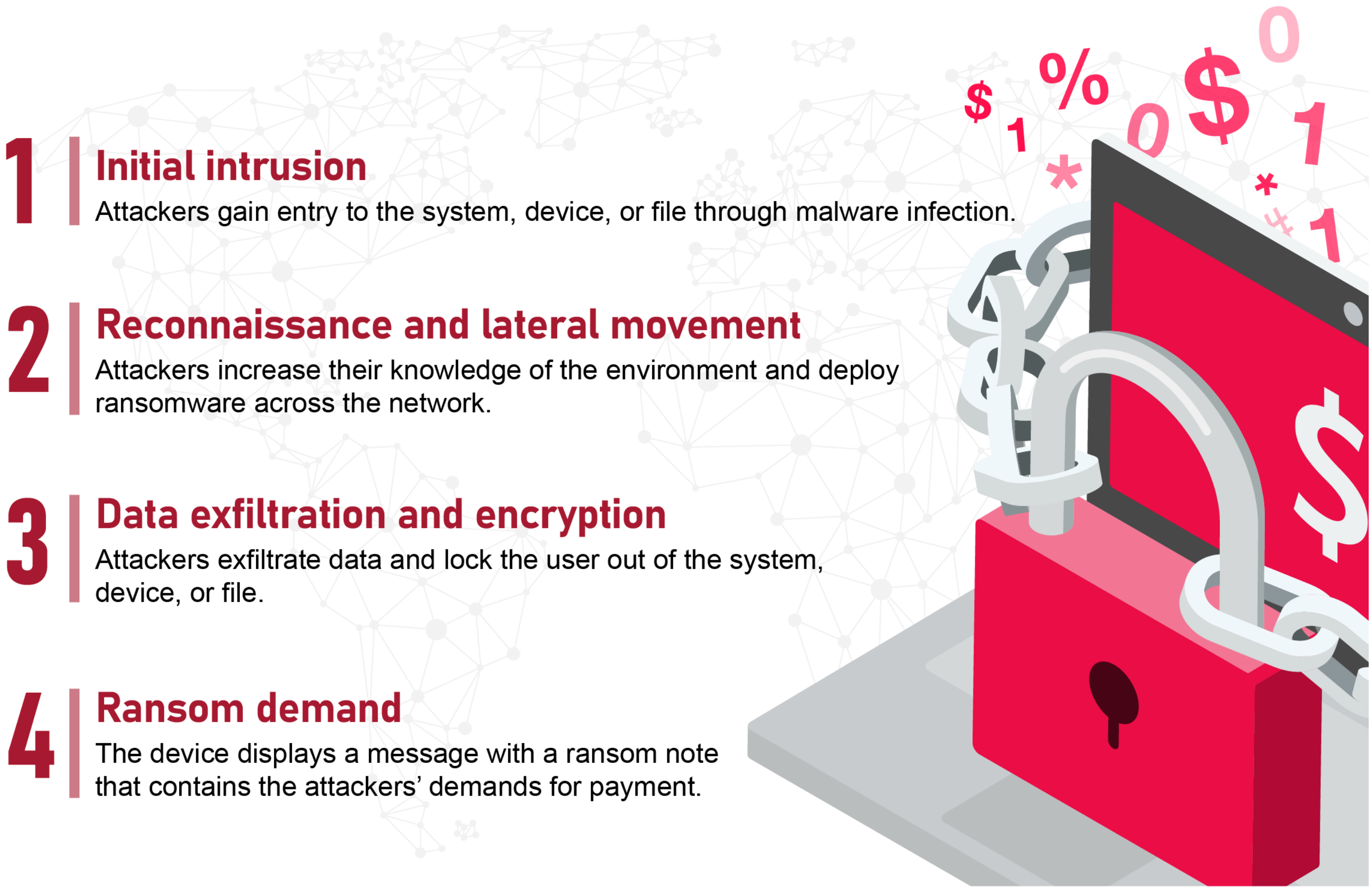
For all objectives, we conducted interviews with officials from six SRMAs, two SCCs, three subsector coordinating councils, and three ISACs to obtain data and perspectives on ransomware trends and statistics, the sectors' adoption of leading federal and nonfederal practices to address ransomware, and federal ransomware assistance efforts. The results from these semi-structured interviews are not generalizable, but provide insight into ransomware impacts and federal support. For more information on our objectives, scope, and methodology, see appendix I. We summarized the results of our interviews in appendix II.

We conducted this performance audit from August 2022 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

A ransomware attack is not a single event. The attack occurs in a series of events or stages that include initial intrusion, reconnaissance and lateral movement, data exfiltration and encryption, and ransom demand. Figure 1 depicts four stages of a common ransomware attack.

Figure 1: Four Stages of a Common Ransomware Attack



1 Initial intrusion

Attackers gain entry to the system, device, or file through malware infection.

2 Reconnaissance and lateral movement

Attackers increase their knowledge of the environment and deploy ransomware across the network.

3 Data exfiltration and encryption

Attackers exfiltrate data and lock the user out of the system, device, or file.

4 Ransom demand

The device displays a message with a ransom note that contains the attackers’ demands for payment.

Sources: GAO analysis based on information from the Cybersecurity and Infrastructure Security Agency, Center for Internet Security, and Federal Bureau of Investigation; tomasknopp/stock.adobe.com (images). | GAO-24-106221

According to CISA and the Multi-State Information Sharing and Analysis Center, malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.[10] Malicious actors may also inform the victim's partners, shareholders, or suppliers about the incident to further damage the business or existing relationships.[11]

In certain instances, federal agencies have taken actions to disrupt ransomware actors. For example:

- In January 2023, the Department of Justice announced that it disrupted the Hive ransomware group and thwarted $130 million in demanded ransom payments by infiltrating its network, obtaining decryption keys, and offering them to victims worldwide. In coordination with international law enforcement, the department also seized control of Hive's servers and websites disrupting its ability to communicate with its members and attack victims. The Department of Justice stated that Hive targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.[12]
- In April 2022, Treasury reported that it sanctioned Hydra Market, a prominent dark web market, to disrupt proliferation of malicious cybercrime services (such as ransomware-as-a-service), dangerous drugs, and other illegal offerings available through the Russia-based site.[13] It also reported that the department identified approximately $8

[10] The Multi-State Information Sharing and Analysis Center is a division of the Center for Internet Security, an independent, nonprofit organization. The Multi-State Information Sharing and Analysis Center was organized in 2002 to provide cyber threat information to state governments. Since fiscal year 2010, DHS has provided funding to the Multi-State Information Sharing and Analysis Center through a cooperative agreement. The funding enables cyber threat information sharing and services to enhance state, local, tribal, and territorial governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises.

[11] CISA, FBI, Multi-State Information Sharing and Analysis Center, and National Security Agency, *#StopRansomware Guide* (Oct. 19, 2023), https://www.cisa.gov/stopransomware/ransomware-guide.

[12] Department of Justice, *U.S. Department of Justice Disrupts Hive Ransomware Variant*, (Jan. 26, 2023), https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

[13] Department of the Treasury, Press Releases: *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, (Apr. 5, 2022), https:/home.treasury.gov/news/press-releases/jy0701. Ransomware-as-a-service describes a subscription-based business model that allows malicious actors, including those with little to no technical skill, to pay to launch ransomware attacks developed by operators.

million in ransomware proceeds that transited Hydra's virtual currency accounts.

Law and Directives Assign Responsibilities for the Protection of Critical Infrastructure Sectors

Presidential Policy Directive 21, issued in February 2013, 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.[14] Since then, the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 has updated the name for these agencies, stating that the term "sector risk management agency" (SRMA) holds the meaning previously given to the term "sector-specific agency."[15] The act also amended the Homeland Security Act of 2002 by adding a section on SRMAs and their responsibilities.

As leads for facilitating and supporting the security and resilience programs and associated activities of their designated critical infrastructure sectors, SRMAs' specific responsibilities include assessing sector risk, facilitating sector coordination and information sharing, and contributing to incident management and emergency preparedness. SRMAs maintain the day-to-day relationships with the private industry in their sectors and provide sector-specific expertise and programs to help mitigate risk.

Presidential Policy Directive 21 identified 16 critical infrastructure sectors and designated the nine associated SRMAs, which were referenced in the Fiscal Year 2021 NDAA. SRMAs are responsible for at least one sector each and may be responsible for multiple sectors. For example, for this review, we examined four sectors with six associated SRMAs. Specifically, we reviewed the critical manufacturing (led by DHS's CISA), energy (led by the Department of Energy), healthcare and public health (led by the Department of Health and Human Services), and

[14] The White House, Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). In CISA's March 2023 response to its Cybersecurity Advisory Committee, the agency noted that the administration is currently updating this directive to clarify and, as necessary, create new federal policy. Among other things, the update is to address how sectoral, cross-sectoral, and systemic risk is identified, assessed, and managed and the roles and responsibilities of SRMAs to manage and respond to risk in their sectors; and CISA's role as national coordinator to lead the national effort to secure and protect critical infrastructure against the myriad of threats and risks faced by the United States. As of September 2023, CISA did not identify a time frame for the administration's efforts to complete the update to the directive.

[15] Pub. L. No. 116-283, § 9002(a)(7), 134 Stat. 3388, 4768 (2021).

transportation systems (co-led by DHS's Coast Guard and Transportation Security Administration, and the Department of Transportation) sectors. Figure 2 illustrates these 16 sectors and each sector's SRMA.

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

Sector	Sector Risk Management Agency	Description
Chemical	DHS	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The sector produces essential products for a range of necessities, including automobiles, pharmaceuticals, food supply, water treatment, and health.
Commercial facilities	DHS	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
Communications	DHS	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.
🟩 Critical manufacturing	DHS	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances, and components, and transportation equipment.
Dams	DHS	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
Defense industrial base	DOD	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Emergency services	DHS	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.
🟩 Energy	DOE	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.
Financial services	TREASURY	Provides the financial infrastructure of the nation. This sector consists of institutions like commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.
Food and agriculture	USDA HHS	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.
Government facilities	DHS GSA	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.
🟩 Healthcare and public health	HHS	Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.
Information technology	DHS	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
Nuclear reactors, materials, and waste	DHS	Provides nuclear power and materials used in a range of settings. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.
🟩 Transportation systems	DHS DOT	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Water and wastewater systems	EPA	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.

Sector Risk Management Agency

🟩 Reflects the four selected sectors in this report.

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

Sources: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; motorama/stock.adobe.com (icons). | GAO-24-106221

In addition to its role as a SRMA for eight sectors (on behalf of DHS), CISA serves as the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. As part of its mission, CISA collaborates with other SRMAs to understand, manage, and help reduce risk to all cyber and physical infrastructure.

To work with the government, SCCs were formed to serve as the voice of each sector and principal entry point for the government to collaborate with each sector. SCCs are self-organized and self-governed 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. The SCCs coordinate and collaborate with the SRMAs in a voluntary fashion regarding issues within their respective sectors.

CISA Provides General Ransomware Support to Sectors

CISA provides general ransomware support to all critical infrastructure sectors in its role as the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. For example, CISA interacts with owners and operators to provide education and awareness; technical information sharing and analysis; cybersecurity review and assessment, and incident response support, by request, to help them combat the threat of ransomware.[16] Specifically:

- CISA provides education and awareness assistance to owners and operators through its publication of guidance and alerts, as well as exercises and campaigns. For example, in collaboration with other federal partners, CISA developed the www.stopransomware.gov website to provide a central location for ransomware protection, detection, and response guidance to assist ransomware victims. The website provides central access to general and sector-specific ransomware-related resources such as alerts, advisories, and reports from multiple federal agencies and partners. In addition, the website includes guidance, such as the #StopRansomware Guide,[17] that provides ransomware and data extortion prevention best practices

[16] CISA may proactively share information with organizations for prevention and mitigation purposes. Additionally, agencies provide certain services by request, such as technical analyses and assessments.

[17] CISA, FBI, Multi-State Information Sharing and Analysis Center, and National Security Agency, *#StopRansomware Guide* (Oct. 19, 2023), https://www.cisa.gov/stopransomware/ransomware-guide.

and a response checklist for organizations.[18] Additionally, the website also includes a dedicated webpage with sector-specific ransomware guidance for the healthcare and public health sector.

- CISA also offers technical information sharing and analysis. For example, it collects and analyzes security- and ransomware-related information—such as threat indicators, incident alerts, and vulnerability data—and shares this information by issuing alerts and advisories. Specifically, the agency has an ongoing joint effort with other federal agencies, such as the FBI, to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These advisories include recently and historically observed tactics, techniques, and procedures and indicators of compromise to help organizations protect against ransomware. As of October 2023, CISA and its partners have published 64 alerts and advisories on its ransomware webpage.

  CISA also is beginning to take proactive measures to identify, notify, and help mitigate vulnerabilities to support certain ransomware attacks. Specifically, the agency launched its ransomware vulnerability warning pilot in January 2023 pursuant to a requirement from the Cyber Incident Reporting for Critical Infrastructure Act of 2022.[19] According to the agency, this initiative proactively identifies information systems belonging to critical infrastructure entities that contain vulnerabilities commonly associated with ransomware intrusions.

  According to CISA, its ransomware vulnerability warning pilot included the number of enrollees for its vulnerability scanning service, which was at least 659 enrollees for the four sectors. The agency also noted that the pilot included additional entities it identified through commercial sources. According to the agency, it issued 93 notifications of potential vulnerabilities associated with a specific type of ransomware.[20]

  Further, CISA began its Pre-Ransomware Notification Initiative, which the agency asserted is intended to help it share and jointly analyze

[18] According to CISA, the best practices and recommendations in the ransomware guide are based on operational insight from itself, the Multi-State Information Sharing and Analysis Center, the National Security Agency, and the FBI.

[19] Pub. L. No. 117-103, div. Y, § 105, 136 Stat. 1038, 1055 (Mar. 15, 2022).

[20] According to the Cyber Incident Reporting for Critical Infrastructure Act of 2022, CISA is required to submit to Congress an annual report on the effectiveness of the pilot. CISA submitted its first annual report to Congress on April 3, 2022.

threat intelligence related to potential early stage ransomware activity through collaboration with sector entities and other partners. CISA reported that it uses the threat intelligence to send rapid notifications to affected entities to help remove malicious actors from their networks before a ransomware attack occurs. According to CISA, it sent 602 pre-ransomware notifications from January 2023 through August 2023.

- CISA conducts cybersecurity review and assessment services upon request, such as vulnerability scanning and remote penetration testing. The review and assessment services are available at no cost to critical infrastructure owners and operators. For example, CISA provides a suite of scanning, testing, and assessment services to help sector entities assess, identify, and reduce their exposure to threats, including ransomware. This suite includes:
  - Vulnerability scanning: This assessment scans information systems for known weaknesses. According to CISA, once entities are enrolled, scans begin and reports of all findings are delivered on a weekly basis and ad-hoc notifications are sent within 24 hours of any urgent findings.
  - Web application scanning: These scans evaluate publicly accessible websites for potential defects and weak configurations to provide recommendations for mitigating web application security risks. According to CISA, its web application scanning service can be conducted monthly, biweekly, or as needed by request.
  - Remote penetration testing: These tests simulate the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service tests perimeter defenses, the security of externally available applications, and the potential for exploitation of open source information.
  - Ransomware readiness assessment: This service is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

Table 1 depicts the number of sector entities enrolled in CISA's scanning, testing, and assessment services from May 2021 through May 2023.

Table 1: Number of Enrollments in the Cybersecurity and Infrastructure Security Agency's (CISA) Scanning, Testing, and Assessment Services from May 2021 through May 2023

Products and services	Enrollments/requests: critical manufacturing	Enrollments/ requests: energy	Enrollments/requests: healthcare and public health	Enrollments/requests: transportation systems
Vulnerability scanning	118	136	320	85
Web application scanning	32	67	133	44
Remote penetration testing	3	3	11	0
Ransomware readiness assessment	6	27	82	7

Source: GAO analysis of data reported by CISA. | GAO-24-106221

- CISA can provide incident response assistance to nonfederal entities upon request. Specifically, CISA's Threat Hunting team and 24x7 watch floor provide situational awareness and incident response assistance. CISA can help sector entities scope the severity of their incidents and provide actionable guidance and recommendations to assist with response, containment, and remediation. The agency can also support owners and operators by analyzing system images and logs from network devices and security appliances for signs of malicious activity at no cost. For example, CISA can provide technical assistance such as forensic analysis of the attack and recommended mitigations.

SRMAs Provide Sector-Specific Support for Ransomware

Several of the SRMAs for the selected sectors provide or reported that they provide specific support that leverages or goes beyond the services that CISA makes available to all critical infrastructure sectors to address ransomware threats. SRMAs help facilitate threat briefings, develop ransomware guidance or requirements tailored for sector owners and operators, and provide subject matter expertise on ransomware threats and related incidents. For example:

- According to the Transportation Security Administration (TSA), it shared 189 unclassified ransomware-specific products (e.g., briefings, advisories, and other reports) and an additional 357 ransomware-related products with aviation and surface transportation owners and operators from May 2021 to May 2023.[21]

[21] According to TSA, the shared products were from varying agencies and sources including, among others, CISA, DHS Intelligence and Analysis, TSA, FBI, and open source reports.

- CISA held at least seven cybersecurity roundtable meetings with critical manufacturing sector owners and operators as part of Critical Infrastructure Partnership Advisory Council from March 2021 through May 2022. Ransomware was discussed in several of these meetings.
- The Department of Health and Human Services (HHS) provided ransomware-related support to the sector through various programs. For example, HHS's 405(d) program issued ransomware-related cyber hygiene infographics, facts sheets, job aids, and trainings.[22] In addition, HHS reported that its Health Sector Cybersecurity Coordination Center issued 40 alerts, conducted 30 threat briefings, and published three threat profiles from May 2021 to May 2023. Specifically, in March 2023 HHS's Health Sector Cybersecurity Coordination Center published a threat profile for the healthcare and public health sector regarding a ransomware group known for its extortion approach by executing ransomware and operating a cybercrime marketplace to publicly release sensitive data, should a victim fail to pay a ransom. The threat profile contained impacts to the sector, known affiliations, relationships, motivations, tactics, techniques, procedures, defenses, and mitigations.[23]

  According to HHS, since 2020, its Heath Sector Cybersecurity Coordination Center has collected information on approximately 1,400 sector incidents related to ransomware from a variety of sources. HHS stated that the center's analysts synthesized the incident information to develop executive summaries and formal products about threat actors; tactics, techniques, and procedures; and indicators of compromise and shared these documents along with recommended mitigation steps with HHS leadership and the broader sector, as appropriate.

  HHS's Office of Critical Infrastructure Protection within the Administration for Strategic Preparedness and Response has also issued bulletins to stakeholders of the healthcare and public health sector. According to HHS, these bulletins are used to share need to know information, useful resources, and timely incident alerts that allow sector stakeholders to personalize the information they receive.

[22] The 405(d) Program—mandated under the Cybersecurity Act of 2015 Section 405(d)—is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health sector's cybersecurity posture against cyber threats.

[23] HHS, Health Sector Cybersecurity Coordination Center, *Threat Profile – Black Basta*, Report: 202303151200 (Mar. 15, 2023).

Stakeholders can choose from six different bulletin distribution lists, one of which is focused solely on cybersecurity. HHS stated that in calendar year 2023, it released 27 cyber-specific bulletins on a weekly basis, and all of these contained information specifically about ransomware.

Further, HHS developed tools and enhanced other resources to address ransomware in the sector. For instance, HHS developed its Risk Identification and Site Criticality Toolkit, which is intended to provide an objective, all-hazards risk assessment that can be used by sector entities to inform emergency preparedness planning, risk management activities, and resource investments.[24] Further, according to HHS, the Administration for Strategic Preparedness and Response's Office of Security and Intelligence has recently hired cybersecurity staff to focus on collaborating with partners within HHS and with other federal agencies to collect, analyze, and report on cybersecurity threats. HHS stated that it has placed a full-time cybersecurity liaison with the FBI's National Cyber Investigative Joint Task Force to ensure effective communication of and coordination around cyber threat intelligence relevant to the healthcare and public health sector.[25]

Moreover, HHS identified that its Administration for Strategic Preparedness and Response manages the department's activities in support of the multi-agency Joint Ransomware Task Force with the objective of improving the hospital defenses and their resiliency against ransomware attacks.[26] According to HHS, the task force has initially focused on kindergarten through grade 12 (K-12) schools and

[24] HHS, *RISC Toolkit 2.0: The Risk Identification and Site Criticality*, https://aspr.hhs.gov/RISC/Pages/default.aspx (accessed Sept. 22, 2023).

[25] The FBI's National Cyber Investigative Joint Task Force is a multiagency cyber center that serves as the national focal point for whole-of-government campaigns against cyber threats and adversaries. Among other things, it is responsible for coordinating, integrating, and sharing information on cyber threat investigations. It also synchronizes joint efforts across over 30 partnering agencies from across law enforcement, the intelligence community, and the federal government that focus on identifying and pursuing malicious actors.

[26] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires the Director of CISA, in consultation with the National Cyber Director, the Attorney General, and the Director of the FBI, to establish and chair a Joint Ransomware Task Force. The task force is to, among other things, coordinate an ongoing nationwide campaign against ransomware attacks, consult with relevant private sector and state, local, tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the task force, and facilitate coordination and collaboration between federal entities and other relevant entities to improve federal actions against ransomware threats.

hospitals, and HHS has developed a total of 145 deliverables in support of the ransomware campaign for the healthcare and public health sector.

- Coast Guard maintains Maritime Commons, which is an online platform it uses to increase awareness of Coast Guard information released to the public. The repository includes cybersecurity guidance, alerts, and bulletins most relevant to the maritime environment, such as the Coast Guard Cyber Command's second annual Cyber Trends and Insights in the Marine Environment report. Additionally, according to Coast Guard, the agency conducts missions to assess if sector entities are vulnerable to cyberattacks, including ransomware, and recommends actions to mitigate risks. Coast Guard's Maritime Cyber Readiness Branch will reach out to ransomware victims within the sector to provide support, if requested. According to Coast Guard officials, the agency provided ransomware-related support to sector entities by conducting six threat briefings, 31 assessments, five advisories, and 40 ransomware-related investigations from May 2021 to May 2023.

NIST Established Guidance to Strengthen Critical Infrastructure against Ransomware

In response to Executive Order 13636, in February 2014, the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity (CSF), a voluntary framework of cybersecurity standards and procedures for industry to adopt.[27] The CSF consists of 108 leading practices intended to guide cybersecurity activities and consider cybersecurity risks as part of an organization's risk management processes. The CSF stated that its framework can help an organization to align and prioritize cybersecurity activities with business/mission requirements, risk tolerances, and resources.

The CSF is composed of three main components: the framework core, implementation tiers, and profiles.

- The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes. Through the use of the framework core,

[27] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). Version 1.1 of the framework was issued Apr. 16, 2018. Subsequent to Executive Order 13636, Congress enacted the Cybersecurity Enhancement Act of 2014, which placed the same responsibility on NIST to develop the framework. See 15 U.S.C. § 272(c)(15),(e).

organizations can better communicate cybersecurity practices between teams using simple, nontechnical language.

- Implementation tiers characterize an organization's approach to managing cybersecurity risks over a range of four tiers. The four tiers are partial, risk informed, repeatable, and adaptive. They reflect a progression from informal, reactive responses to approaches that are flexible and risk informed.
- Profiles enable organizations to establish road maps for reducing cybersecurity risks that are well aligned with organizational and sector goals, consider legal/regulatory requirements and industry best practices, and reflect risk management priorities. Organizations can use the framework profiles to describe the current state (the cybersecurity outcomes that are currently being achieved) or the desired target state (the outcomes needed to achieve the desired cybersecurity risk management goals) of specific cybersecurity activities.

In February 2022, NIST developed Ransomware Risk Management: A Cybersecurity Framework Profile.[28] According to NIST, the ransomware profile is intended to help organizations identify and prioritize opportunities for improving their security and resilience against ransomware attacks. The ransomware profile also is to identify the NIST CSF security objectives that support identifying, protecting against, detecting, responding to, and recovering from ransomware events. The profile is made up of a subset of 69 leading practices (referred to as subcategories by NIST) from the CSF's 108 core practices. According to NIST, organizations can use the ransomware profile as a guide for assessing their states of readiness and assisting in determining cybersecurity gaps.

GAO Has Reported on Cybersecurity Challenges Faced by Critical Infrastructure

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we first designated federal information security as a government-wide high-risk area in our biennial report to Congress in 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information. We continue to identify the protection of critical cyber infrastructure as a high-

[28] NIST, *Ransomware Risk Management: A Cybersecurity Framework Profile*, NISTIR 8374, (Gaithersburg, MD: February 2022).

risk area, as shown in our April 2023 high-risk update on major cybersecurity challenges.[29]

We have conducted numerous reviews of federal efforts to protect critical infrastructure cybersecurity, such as medical device information security considerations, cybersecurity risks facing the electric grid, oversight of avionics cybersecurity risks, adoption of NIST cybersecurity guidance, and cybersecurity of internet-connected devices.[30] In addition, we recently reported on federal coordination and assistance efforts in addressing ransomware attacks on state, local, tribal, and territorial governments and K-12 schools.[31] For example, in September 2022, we reported that CISA, the U.S. Secret Service, and the FBI provided direct assistance aimed at preventing and responding to ransomware attacks on state, local, tribal, and territorial organizations within the government facilities sector.[32] While this assistance was reported to be helpful, we noted that federal agencies lacked processes for more effective federal coordination on ransomware assistance. We made three recommendations—two to DHS and one to the Attorney General—to direct CISA, FBI, and Secret Service to incorporate key collaboration practices. As of October 2023, the agencies have not yet fully implemented our recommendations.

Additionally, in October 2022 we identified that schools have increasingly reported ransomware and other cyberattacks that can cause significant

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

[30] GAO, *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices,* GAO-12-816 (Washington, D.C.: Aug.12, 2012); *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid,* GAO-19-332 (Washington, D.C.: Aug. 26, 2019); *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks,* GAO-21-86 (Washington, D.C.: Oct. 9, 2020); *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021); *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance,* GAO-22-105103 (Washington, D.C.: Feb. 9, 2022); *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, GAO-23-105327 (Washington, D.C.: Dec.1, 2022); and *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods,* GAO-23-105468 (Washington, D.C.: Sept. 26, 2023).

[31] GAO, *Ransomware: Federal Coordination and Assistance Challenges,* GAO-23-106279 (Washington, D.C.: Nov. 16, 2022).

[32] GAO, *Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767 (Washington, D.C.: Sept. 14, 2022).

disruptions to school operations.[33] While the Department of Education and CISA offered cybersecurity resources to K-12 schools, such as online safety guidance, they had little to no interaction with schools regarding their cybersecurity due, in part, to the lack of a government coordinating council, as called for in the 2013 National Infrastructure Protection Plan. Among other things, we recommended that the Department of Education and DHS improve coordination of K-12 schools' cybersecurity. As of October 2023, the agencies have not yet fully implemented our recommendations.

In addition, in response to a provision in the Fiscal Year 2021 NDAA, we reported on the effectiveness of SRMAs in carrying out responsibilities set forth in the act, including the extent to which CISA helped agencies implement their responsibilities.[34] Among other things, we found that CISA had undertaken efforts to help SRMAs implement their statutory responsibilities such as updating the 2013 National Infrastructure Protection Plan. However, CISA had not yet developed milestones and timelines for efforts underway to improve coordination and we recommended the agency do so. As of October 2023, CISA had not yet implemented our recommendation.

Ransomware Attacks Have Significantly Impacted Selected Sectors, but Reporting Has Limitations

Ransomware attacks are having increasingly devastating impacts to the nation's critical infrastructure. One academic institution estimated that between January 2020 and November 2022 there have been at least 347 public reports concerning ransomware attacks targeting critical infrastructure.[35] In addition, FBI's Internet Crime Complaint Center[36]

[33] GAO, *Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity,* GAO-23-105480, (Washington, D.C.: Oct. 20, 2022).

[34] GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806 (Washington, D.C.: Feb. 7, 2023).

[35] Rege, A. (2023). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset." Version 12.8. Temple University. Online at *https://sites.temple.edu/care/cira/*. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

[36] FBI's Internet Crime Complaint Center obtains and analyzes reports of internet-related crimes from victims such as business and the general public.

reported that 870 critical infrastructure organizations were victims of ransomware in 2022, affecting 14 of the 16 critical infrastructure sectors.[37]

Ransomware attacks of critical infrastructure are a concern among owners and operators who have much to lose when this type of cyberattack targets sensitive data or locks down critical IT systems. The lack of access to systems and data supporting critical infrastructure due to a ransomware attack has threatened critical services.[38]

For example, in July 2022, a joint alert from CISA, the Department of the Treasury, and the FBI stated that a North Korean ransomware attack targeted assets responsible for healthcare services—including electronic health records services, diagnostics services, imaging services, and intranet services.[39] Federal agencies assessed that North Korean state-sponsored actors are likely to continue targeting the healthcare and public health sector because its organizations would be willing to pay ransoms to continue providing services that are critical to human life and health. In addition, an August 2021 attack on the Ohio-based Memorial Health System reportedly led to canceled urgent care surgeries and radiology appointments and diverted care for emergency patients.[40]

SCC officials from the healthcare and public health sector noted that it could take up to 45 days for hospitals to recover from a ransomware attack. During this recovery period, hospitals in the region may not be equipped to absorb the disruptions to patient services caused by the incident, even if they were not directly attacked. According to the CyberPeace Institute—a Geneva-based nonprofit organization—for the period between June 5, 2020, and September 28, 2022, the average operational disruption due to a ransomware attack within the healthcare and public health sector lasted about 18 days. Additionally, for that same period, the institute reported that 85 percent of incidents resulted in a data

[37] FBI Internet Crime Complaint Center, *Internet Crime Report 2022*, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

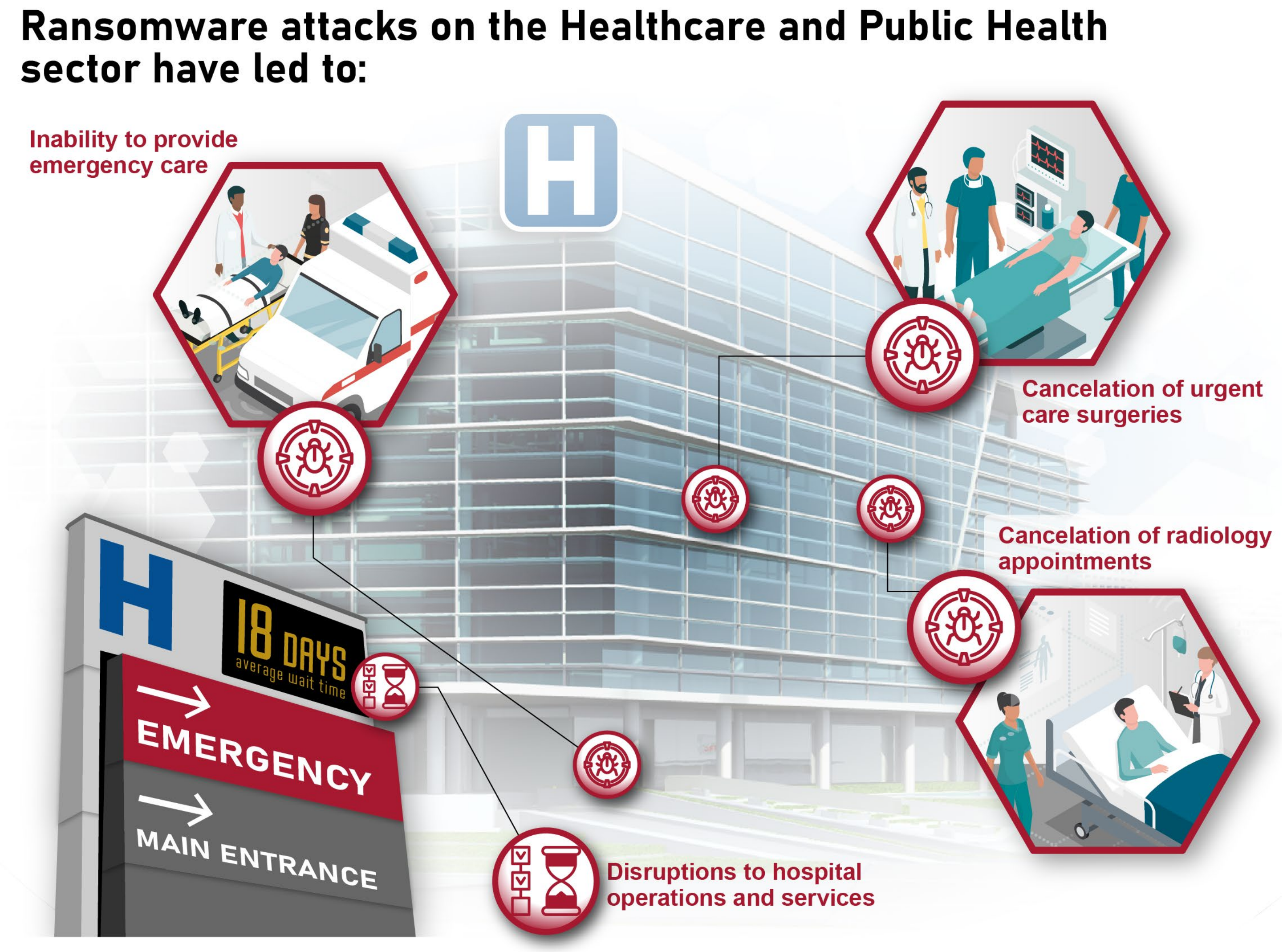
[38] GAO, *Ransomware—Holding IT Systems and Data Hostage*. Web Blog. WatchBlog, June 30, 2021. https://www.gao.gov/blog/ransomware-holding-it-systems-and-data-hostage

[39] CISA, *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector*, Alert (AA22-187A), (July 7, 2022), accessed Aug. 28, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a.

[40] Memorial Health System, *Memorial Health System Experiences Cyber Attack*, (Aug. 15, 2021), https://www.mhsystem.org/news/memorial-health-system-experiences-cyber-attack/.

leak and 45 percent led to systems going offline.[41] Figure 3 illustrates examples of reported impacts to the healthcare and public health sector as a result of ransomware attacks.

Figure 3: Reported Examples of Ransomware Impacts to the Healthcare and Public Health Sector


Ransomware attacks on the Healthcare and Public Health sector have led to:
Inability to provide emergency care
Cancelation of urgent care surgeries
Cancelation of radiology appointments
Disruptions to hospital operations and services
H
18 DAYS
average wait time
EMERGENCY
MAIN ENTRANCE

Sources: GAO analysis of publicly reported incident information; GAO (sign); elenabsl/stock.adobe.com (images); archipoch/stock.adobe.com (hospital); motorama/stock.adobe.com (icons). | GAO-24-106221

[41] CyberPeace Institute, Cyber Incident Tracer, https://cit.cyberpeaceinstitute.org/explore.

In addition to the healthcare and public health sector, a variety of other reports demonstrate the disruptive nature of ransomware on critical infrastructure. For example, a May 2021 ransomware attack on an American oil pipeline resulted in regional gasoline shortages in the Eastern U.S. for several days. In addition, in February 2023 Pierce County Public Transportation Benefit Area Corporation experienced a ransomware attack that resulted in disruptions to agency systems and communications. According to media reporting, the ransomware group LockBit demanded almost $2 million in ransom.

Further, the operational technology that our nation's critical infrastructure relies on to function has experienced rising threats from ransomware in recent years.[42] CISA has recognized the threat that ransomware posed to operational technology assets and control systems which support critical industries that provide electricity, transportation services, water and wastewater treatment, oil and natural gas, and chemicals. In June 2021, CISA issued guidance for owners and operators to adopt a heightened state of awareness to protect critical infrastructure against ransomware threats affecting operational technology.[43]

The private sector has also identified ransomware threats to operational technology. In January 2022, Mandiant—a cyber defense firm—reported that across 1,300 ransomware extortion attacks on industrial organizations,[44] one in seven attacks exposed sensitive information on operational technology such as network and engineering diagrams, images of operator panels, and information on third-party services.[45] Malicious actors could use this information to launch attacks on operational technology systems that control, regulate, and monitor

[42] According to the National Institute of Standards and Technology, operational technology includes programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

[43] CISA, *Rising Ransomware Threat to Operational Technology Assets*, (June 9, 2021), https://www.cisa.gov/resources-tools/resources/ransomware-threat-ot.

[44] According to Mandiant, the sample included organizations in industrial sectors that are likely to use operational technology systems, such as energy and water utilities, or manufacturing.

[45] Mandiant, *1 in 7 OT Ransomware Extortion Attacks Leak Critical Operational Technology Information*, (Jan. 31, 2022), https://www.mandiant.com/resources/blog/ransomware-extortion-ot-docs.

processes that prevent hazardous conditions within industrial sectors such as critical manufacturing, energy, and transportation.

Four of the 16 critical infrastructure sectors—critical manufacturing, energy, healthcare and public health, and transportation systems—have experienced a relatively large number of ransomware attacks. For instance:

- CISA identified more than 250 reported ransomware incidents across the four sectors from October 2021 to October 2022.[46]
- Among the 870 critical infrastructure organizations that FBI reported were victims of ransomware, almost half of those incidents were from the four sectors.
- Temple University's ransomware database—funded by the National Science Foundation—identified more than 270 publicly disclosed incidents across the four sectors from November 2013 through October 2022.[47] Based on the dataset, three of the four sectors were among those most affected by ransomware.

With the increasing number of attacks, ransomware continues to be a costly type of cyberattack to critical infrastructure owners and operators. For example, according to CISA, the monetary value of ransom demands has increased over time, with some demands exceeding $1 million today. In addition, the Department of the Treasury reported that ransomware remains a significant threat to critical infrastructure with the reported total value of ransomware in the U.S. reaching a total of $886 million in 2021. According to the department, this represents a 68 percent increase compared to the $527 million in total value reported in 2020.[48] Figure 4

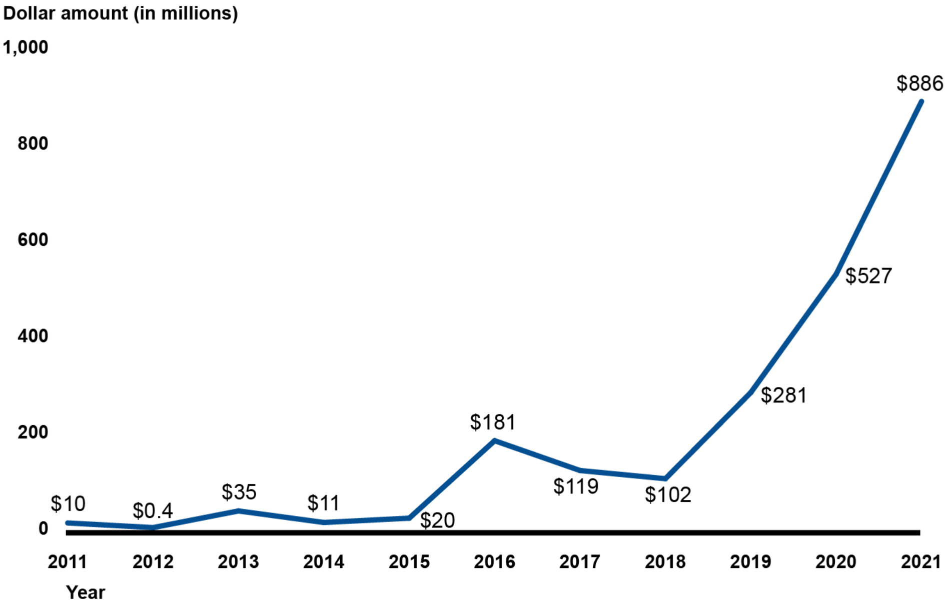
[46] According to CISA, the total number of reported ransomware incidents are based on open source data and owners and operators who reported directly to CISA's 24x7 watch floor.

[47] Rege, A. (2023). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset." Version 12.8. Temple University. Online at *https://sites.temple.edu/care/cira/*. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

[48] Treasury, Financial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021*, Retrieved from https://www.fincen.gov/resources/financial-trend-analyses. According to Treasury, financial institutions should determine if a suspicious activity report filing is required or appropriate when dealing with a ransomware incident to comply with their Bank Secrecy Act obligations. Treasury conducted its analysis based on suspicious activity report filings.

illustrates Treasury's reporting on the total dollar value of ransomware-related incidents in the U.S. from 2011 through 2021.

Figure 4: Treasury Reported Dollar Value of U.S. Ransomware-Related Incidents



Source: GAO analysis of Department of the Treasury data. | GAO-24-106221

Private sector organizations have also reported on the costly nature of ransomware attacks. For example, Sophos, a cybersecurity vendor, reported that ransom payments have increased across all critical infrastructure sectors. Specifically, it reported that the average ransom payment was $812,000 in 2021, representing almost a five-time increase from $170,000 reported in 2020.[49] Sophos also reported that the critical manufacturing and energy sectors had the highest average payments at $2 million for each sector. In contrast, the healthcare and public health

[49] Sally Adam, *State of Ransomware 2022*,Sophos, (Abington, UK; Apr. 27, 2022), https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/.

sector had the lowest average payment across the four sectors at $197,000.[50]

As another example, NetDiligence, a cyber risk assessment and data breach services company, reported that ransom demands reached a combined average of $377,000 during 2017 through 2021 across the four selected sectors. It also reported that the energy and critical manufacturing sectors had the second and third highest average ransom demands, respectively, across all sectors.[51]

SRMAs Rely on Various Sources of Reporting on Ransomware Impacts

SRMAs rely on reporting from CISA, the FBI, Treasury, and private sector organizations, such as vendors who conduct cybersecurity research, for information concerning ransomware incidents and their impacts. Officials noted that those organizations already have resources and mechanisms in place to collect such data.

As the SRMA for the critical manufacturing sector, CISA collects information internally about ransomware incidents affecting the sector. However, CISA supplements the data it collects with information from external sources.

HHS officials asserted that it collects incident data on the healthcare and public health sector via phone calls and emails with federal partners and direct connections with impacted private sector entities when possible. HHS noted that it focuses on the technical aspects of the attack when available (e.g., tactics, techniques, and procedures; and indicators of compromise) as well as the impacts to the facility and patient care. To help gather information about impacts to patient care, HHS developed a standardized set of questions to ask about cyber incidents in the sector. However, HHS did not provide supporting documentation to corroborate its assertions that it collects and analyzes incident data.

TSA stated that its Office of Intelligence and Analysis conducts open source analysis, evaluates unclassified cybersecurity reporting, and reviews transportation-specific cyber incident reporting for trends in cyber threats to the sector, including ransomware. TSA acknowledged that its

[50] According to Sophos, this research is based on independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries. The payment information is based on the 965 respondents whose organizations paid ransom and shared the exact amount.

[51] NetDiligence, *Ransomware 2022 Spotlight Report*, (Gladwyne, PA: October 2022), https://netdiligence.com/cyber-claims-studies/.

information is limited to what industry directly reports to CISA and TSA, what is published in open source media outlets, or what is available through third party databases. However, it believes that its analysis reflects the full scope of ransomware events within the transportation sector.

Other SRMA officials within the energy and transportation systems sectors stated that they generally do not collect data directly on the number of reported ransomware incidents and their impacts for their respective sectors. SRMA officials noted that a key reason for not collecting this information directly is that they do not always have requirements in place to compel sector entities to provide such data and thus, rely on voluntary reporting. Certain sectors, such as the energy and transportation systems sectors, have federal requirements and statutory authorities that call for entities to report certain incidents affecting operations. However, there may be ransomware incidents that do not meet the sectors' mandatory reporting requirements. In addition, SRMA and ISAC officials stated that when an owner or operator reports an incident to CISA or the sector's ISAC, the primary focus is to obtain the technical details of the incident to support mitigation efforts rather than collect information about impacts.

The CISA, FBI, Treasury, and private sector reporting that SRMAs rely on for understanding ransomware impacts has certain limitations. Specifically, the reporting is at times incomplete, not comparable, or not broken down by sector. For example:

- Information on ransomware incidents is incomplete. The number of reported incidents cannot be precisely identified, in part, due to the voluntary nature of the reporting and potential reluctance to report being a victim. For instance, victims may voluntarily report ransomware incidents to CISA, FBI, or sector ISACs. In certain circumstances, victims may be required to report ransomware attacks to regulatory agencies.

  Given the variety of reporting mechanisms, there is not a single source for a total number of ransomware incidents reported to the federal government. Thus, the reporting to federal agencies likely does not capture full information on ransomware incidents across the four sectors.

- Impact data are not always comparable or sector specific. For example, Treasury and Sophos both report on ransom payments within critical infrastructure sectors, but the reporting on financial impacts was not comparable and was not always broken down by sector. Specifically, Treasury reported on the total dollar value of ransomware (which may include extortion amounts, attempted transactions, and payments that were unpaid) without a summary by sector and Sophos reported on the average ransom payment overall and by sector. In addition, other reporting by private sector organizations have focused on reporting ransom demands versus payment data. Further, the data reported by Treasury and Sophos used different datasets.

Also, while private sector organizations have reported on impacts beyond ransomware payments and demands, the data were limited to nongeneralizable case studies. For example, the CyberPeace Institute reported on the sector-wide impacts of ransomware to the healthcare and public health sector.

The implementation of requirements pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires covered entities across critical infrastructure sectors to report “covered cyber incidents” to CISA within 72 hours of reasonably believing that a “covered cyber incident” occurred and ransom payments resulting from a ransomware attack within 24 hours of making payment.[52] According to CISA, it is still developing the rules for such reporting and expects to issue the notice of proposed rulemaking in March 2024 and the final rules by September 2025. If implemented effectively, CISA’s reporting rules could help to provide the federal government more complete and comparable data on ransomware impacts on the nation’s critical infrastructure.

SRMAs Have Not Overseen Selected Sectors’ Adoption of Ransomware Practices

As previously mentioned, in February 2022 NIST developed a ransomware profile to help organizations identify and prioritize opportunities for improving their security and resilience against ransomware attacks. As of September 2023, the federal government’s central resource for ransomware guidance, www.stopransomware.gov, featured the NIST ransomware profile on its home page as a key resource for protection and response guidance.[53]

[52] The Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted as division Y of the Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (Mar. 15, 2022).

[53] CISA, in collaboration with other federal partners, developed the www.stopransomware.gov website to provide a central location for ransomware guidance, alerts, advisories, and reports from federal agencies and partners.

The National Infrastructure Protection Plan recommends that entities take steps to evaluate progress toward the achievement of goals—in this case, implementation or adoption of leading practices to address ransomware. Specifically, the National Infrastructure Protection Plan directs SRMAs and their federal and nonfederal sector partners (including SCCs) to measure the effectiveness of risk management goals by identifying high-level outcomes to facilitate the evaluation of progress toward national goals and priorities, including securing critical infrastructure against cyber threats.

Selected sectors' adoption of leading practices to address ransomware is largely unknown. Specifically, none of the SRMAs for the four selected sectors—critical manufacturing, energy, healthcare and public health, and transportation systems—determined the extent of adoption of the NIST ransomware profile. Similarly, none of the SRMAs reported taking action to measure implementation of the profile by their respective sectors.

Nevertheless, several SRMAs have acknowledged the importance of understanding sector-wide protection efforts and have measured the adoption of broader areas of the NIST CSF, which includes a subset of practices from the ransomware profile.[54] However, SRMAs efforts did not measure the entirety of practices from the NIST ransomware profile. For example:

- The Department of Energy (DOE) demonstrated that it conducted research with the assistance of a contractor to help the department understand high-level insights regarding the adoption and impact of the CSF and DOE's Cybersecurity Capability Maturity Model. According to an official in its office of Cybersecurity, Energy Security, and Emergency Response, the research is intended to help the department understand cybersecurity needs of the energy sector, which it can use to inform decisions about future research and development, tools, and guidance.

  However, these assessments were limited to high-level insights about broad categories of the CSF and Cybersecurity Capability Maturity Model where sector entities reported highest and lowest levels of adoption. As of August 2023, DOE did not have insights into the adoption of specific practices, including those that align with the NIST

[54] The NIST ransomware profile is a subset of the practices contained in the CSF. While the profile provides additional context for why certain practices are important to ransomware protection and response, the core practices included in the profile are no different than the same practice in the broader CSF.

ransomware profile. An official in DOE's office of Cybersecurity, Energy Security, and Emergency Response noted that this research is still in the early stages and there is no estimated completion date, but the department's intention is to further expand these efforts to develop a more granular understanding of the sector's cyber practices.

- HHS and the SCC for the healthcare and public health sector partnered to issue the Hospital Cyber Resiliency Initiative: Landscape Analysis in April 2023 to highlight findings and issues affecting the cybersecurity resiliency of U.S. hospitals.[55] Among other things, the study measured the adoption of the CSF in hospitals. The study found that participating hospitals claimed they had adopted 70.7 percent of the CSF based on organizations' self-assessment of the adoption of the framework's five major functional areas (Identify, Detect, Protect, Respond, and Recover) and 23 subcategories. However, HHS was not yet tracking the extent of adoption of ransomware-specific practices within those categories and subcategories.

  In addition, HHS officials stated that version 2.0 of its Risk Identification and Site Criticality Toolkit has a section of 94 cybersecurity questions derived from the NIST CSF.[56] HHS noted that in this updated version of the toolkit, HHS can analyze aggregate data to assess implementation of key NIST CSF key concepts. However, HHS did not provide support on its ability to analyze data from the toolkit.

- TSA, in coordination with its co-SRMAs the Department of Transportation (DOT) and Coast Guard, developed and distributed a survey to the transportation systems sector from March 2021 to June 2021, and finalized analysis of the survey results in January 2023. The survey collected information on 857 sector entities' awareness, implementation, and use of the CSF. Similar to HHS's efforts, the analysis identified adoption of the framework's five functional areas. However, the SRMAs were unable to determine the level of adoption of specific practices from the CSF or the ransomware profile based on the survey responses.

[55] Department of Health and Human Services, *Hospital Cyber Resiliency Initiative: Landscape Analysis* (Washington, D.C.: Apr. 17, 2023).

[56] HHS's Risk Identification and Site Criticality Toolkit is intended to provide an objective, all-hazards risk assessment that can be used by sector entities to inform emergency preparedness planning, risk management activities, and resource investments. *RISC Toolkit 2.0: The Risk Identification and Site Criticality*, https://aspr.hhs.gov/RISC/Pages/default.aspx (accessed Sept. 22, 2023).

Selected Sectors Manage Ransomware Risks Using a Variety of Practices

SRMAs, SCCs, and ISACs for the four selected sectors identified seven other sets of practices from federal agencies and industry that they use in conjunction with or in lieu of the NIST CSF and ransomware profile to manage cybersecurity risks, such as ransomware. The practices address foundational cybersecurity protections that can help manage a wide variety of cyber threats beyond ransomware. Table 2 identifies the seven sets of cybersecurity practices that sectors reported using to address ransomware.

Table 2: Cybersecurity Practices That Selected Critical Infrastructure Sectors Reported Using to Address Ransomware

Cybersecurity practices	Sector that reported using the practices	Description
Center for Internet Security, Critical Security Controls (version 8)	Energy	Provides a set of safeguards designed to help organizations define a starting point for their cybersecurity defenses. According to the Center for Internet Security, the controls are designed to mitigate the most prevalent cyberattacks against systems and networks.
Cybersecurity and Infrastructure Security Agency, Cross-sector Cybersecurity Performance Goals (version 1.0.1)	Energy	Documents minimum baseline IT and operational technology cybersecurity practices aimed at reducing risks to both critical infrastructure operations and the American people. According to the Cybersecurity and Infrastructure Security Agency, the practices can be used as a quick-start guide and a way for smaller or less mature cybersecurity programs to prioritize which protections to implement.
Department of Energy, Cybersecurity Capability Maturity Model (version 2.1)	Energy	Focuses on the implementation and management of cybersecurity practices associated with IT, operational technology, and information assets and the environments in which they operate. The Department of Energy, energy sector coordinating councils, the energy sector information sharing and analysis center, and other public- and private-sector organizations developed these practices for energy sector entities. According to the model, the practices can be used by any entity in any sector.
North American Electric Reliability Corporation, Critical Infrastructure Protection Standards	Energy	Includes requirements developed by the North American Electric Reliability Corporation and approved by the Federal Energy Regulatory Commission—the federal regulator for the interstate transmission of electricity. The requirements are intended for systems in the energy sector that would impact the reliable operation of the bulk electric system.[a] The practices are designed to mitigate the risk of a compromise that could lead to misoperation or instability in the bulk electric system.
Department of Health and Human Services, Health Industry Cybersecurity Practices	Healthcare and public health	Outlines cybersecurity best practices for small, medium, and large healthcare organizations.
Federal Transit Administration, Cybersecurity Assessment Tool for Transit	Transportation systems	Provides mass transit agencies with guidance for building foundational elements of a cybersecurity program. The tool includes a set of practices intended to improve IT operational resilience of organizations in the transportation systems sector.

Cybersecurity practices	Sector that reported using the practices	Description
Transportation Security Administration emergency amendments for airport and aircraft operators and security directives for freight and passenger rail, pipelines, public transportation, and surface transportation entities	Transportation systems	Requires owners and operators of airports and aircraft, freight and passenger rail, pipelines, public transportation, and surface transportation to implement certain cybersecurity measures as a protection against malicious cyber intrusions.

Source: GAO analysis of agency documents. | GAO-24-106221

[a] The bulk electric system is defined as (1) all transmission elements operated at 100 kilovolts or higher and (2) real power and reactive power resources connected at 100 kilovolts or higher. This does not include facilities used in the local distribution of electric energy.

While sector entities reported adopting practices other than the NIST ransomware profile and CSF, HHS was the only SRMA that tracked implementation of the other practices through its assessment of hospitals' adoption of the Health Industry Cybersecurity Practices. The SRMAs for the other three sectors provided anecdotal examples of entities in their sectors using various practices or high-level insights, but they were not tracking implementation of specific practices.

Moreover, six of the seven sets of practices did not fully align to leading federal practices that NIST established to address ransomware. Specifically, DOE and NIST developed a mapping that identified alignment between the Cybersecurity Capability Maturity Model and CSF practices (including practices that were in the ransomware profile). The other six cyber practices ranged from 0 percent to 93 percent alignment. For instance, TSA officials stated that its emergency amendments and security directives aligned with 71 percent of the practices to address ransomware. However, TSA did not demonstrate that its amendments and security directives had such alignment. The remaining five sets of practices also did not demonstrate alignment with the practices. Table 3 shows the extent to which the seven sets of practices demonstrated alignment with the NIST ransomware profile practices.

Table 3: Extent to Which Selected Cybersecurity Practices Demonstrated Alignment with NIST's Ransomware Profile Practices

Cybersecurity practices	Percentage of practices that demonstrated alignment to the ransomware profile
Center for Internet Security, Critical Security Controls (version 8)	36 of 69 practices (52%)
Cybersecurity and Infrastructure Security Agency, Cybersecurity Performance Goals	22 of 69 practices (32%)
Department of Energy, Cybersecurity Capability Maturity Model (version 2.1)	69 of 69 practices (100%)
Department of Health and Human Services, Health Industry Cybersecurity Practices	33 of 69 practices (48%)
Federal Transit Administration, Cybersecurity Assessment Tool for Transit	54 of 69 practices (78%)
North American Electric Reliability, Corporation Critical Infrastructure Protection Standards	64 of 69 practices (93%)
Transportation Security Administration, emergency amendments for airport and aircraft operators and security directives for freight and passenger rail, pipelines, public transportation, and surface transportation entities	0 of 69 practices (0%)

Source: GAO analysis of agency documents. | GAO-24-106221

Notes: NIST – National Institute of Standards and Technology

SRMAs Did Not Track Selected Sectors' Adoption of NIST's Ransomware Profile for Various Reasons

SRMA, SCC, and ISAC officials from the critical manufacturing, energy, and transportation systems sectors identified several reasons for not tracking implementation of practices included in the NIST ransomware profile or other practices used to address ransomware. For example, six of the eight SCCs and ISACs stated that they were not familiar with the ransomware profile or did not identify it as one of the adopted sets of practices within the sector. In addition, officials noted that they lacked mechanisms or resources for tracking implementation of the ransomware profile and other cybersecurity practices they used, did not see it as their role to measure adoption, or that they lacked the regulatory authority to collect such data.[57]

[57] In both February 2020 and February 2022, we reported that SRMAs for most critical infrastructure sectors—including the selected sectors in this report—had not yet determined the adoption of the NIST CSF. The lack of such mechanisms inhibits the SRMAs' ability to measure the adoption of the NIST ransomware profile. As of August 2023, SRMAs for the critical manufacturing, energy, and transportation systems sector had not yet completed efforts that they initiated to determine NIST CSF adoption in their respective sectors.

In addition, SRMA, SCC, and ISAC officials in the critical manufacturing, energy, and transportation systems sectors stated that their sectors focus on basic cybersecurity protections and general guidance rather than attempt to address specific threats like ransomware. For example, officials from DOT's Office of the Secretary stated that the best way to deal with ransomware is to have better foundational cybersecurity practices. Officials from the DOE's Office of Cybersecurity, Energy Security, and Emergency Response stated that the agency aims to help the energy sector address risks from the full range of malicious cyber incidents, including ransomware, by focusing on cybersecurity protections that ensure the reliability of the sector's operations.

It is important for SRMAs to encourage and assist sectors in adopting foundational cybersecurity practices, many of which can also help mitigate ransomware. For instance, NIST included foundational practices such as conducting, maintaining, and testing information backups and performing vulnerability scans in its ransomware profile and such practices can help address a wide variety of cyber threats.

However, ransomware threats pose an elevated risk to the nation's critical infrastructure. Thus, understanding if sectors have implemented practices to mitigate ransomware's impact is increasingly important.[58] As discussed earlier, the impacts of a ransomware attack on critical infrastructure can be severe. These attacks can result in costly and time consuming loss of data for affected organizations. Additionally, these attacks can create negative, cascading effects for organizations and individuals not directly attacked.

Until SRMAs understand sectors' adoption of NIST or similar other practices that are intended to improve security and resilience against ransomware attacks, the White House's goal of bolstering critical infrastructure resilience to withstand ransomware threats will be more difficult to achieve.[59] Further, improved awareness of the sectors' adoption of cybersecurity practices will help SRMAs to better understand their sectors' exposure to ransomware threats and decide where to focus their resources.

[58] CISA, *2021 Trends Show Increased Globalized Threat of Ransomware*, Alert (AA22-040A) (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[59] The White House, *National Cybersecurity Strategy* (Washington, D.C.: Mar. 1, 2023).

Selected SRMAs Have Assessed Ransomware Risks, but Have Not Fully Evaluated Their Support

The Fiscal Year 2021 NDAA assigned SRMAs the responsibility for supporting risk management efforts, including providing specialized expertise that support their respective sectors, such as assessment and prioritizing of risks and consideration of cybersecurity threats, vulnerabilities, and risks.[60] In addition, according to the 2013 National Infrastructure Protection Plan and its supplementary guidance, SRMAs should assess risks within their sectors and use metrics and other evaluation procedures to measure the progress and assess the effectiveness of their efforts that support their sectors and enhance the cybersecurity of critical infrastructure.[61] DHS guidance states that use of metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure informs the process of prioritizing and selecting the most effective and cost-efficient ways to manage risk.

Selected SRMAs Have Assessed Ransomware Risks in Their Sectors

Most of the selected SRMAs have assessed or plan to assess ransomware risks within their respective sectors. For example:

- CISA developed a sector-wide cyber risk summary that analyzed common vulnerabilities from sector entities enrolled in its cyber hygiene and vulnerability scanning service to identify sector risks (including ransomware), highlight trends, and make recommendations for safeguarding vulnerable assets. CISA also held roundtable discussions with sector entities through the Critical Infrastructure Partnership Advisory Council to discuss risks to the critical manufacturing sector, including ransomware threats.
- Coast Guard published its 2021 Cyber Trends and Insights in the Maritime Environment report in August 2022, which identified ransomware as a top cyber risk to maritime assets. The report included best practices to help secure critical systems based on Coast Guard's findings.
- HHS published its Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients report as part of its 405(d) initiative, which identified ransomware as one of the top five cyber threats to the

[60] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002(c)(1), 134 Stat. 3388, 4770 (Jan. 1, 2021), codified at 6 U.S.C. § 665d.

[61] Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013) and *2013 National Infrastructure Protection Plan, Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*, (Dec. 17, 2020).

sector. The report included best practices to help mitigate against ransomware.

- TSA's Office of Intelligence and Analysis developed a quarterly report in 2023 and an annual report in 2022 that reviewed cyber incidents within the transportation systems sector to understand and summarize the threats across the sector. TSA's Office of Intelligence and Analysis also conducted a study in July 2022 that examined the ransomware threat across the sector since 2017. Among other things, the study addressed threats from nation-state actors, identified trends among ransomware attacks, and highlighted the business impact to the sector.
- Officials in DOE's Office of Cybersecurity, Energy Security, and Emergency Response stated that the agency received dashboard reports from CISA to understand the prevalence of ransomware incidents. However, DOE did not demonstrate its use of the incident data to assess risks. Officials in DOE's Office of Cybersecurity, Energy Security, and Emergency Response stated that the office plans to conduct a comprehensive risk assessment in early 2024 to identify high-priority risks to the energy sector's assets.

However, DOT did not demonstrate that it assessed ransomware risks for the transportation systems sector. DOT noted that its co-SRMAs assessed ransomware risks for the sector. For instance, as mentioned earlier, TSA assessed threats across the sector based on its analysis of ransomware incidents and Coast Guard assessed risks in the maritime environment. However, DOT did not participate in the sector risk analysis with its co-SRMAs. Further, the department did not identify other efforts to assess risks or plans to assess risks in the transportation systems sector.

Determining ransomware risks would help SRMAs carry out their Fiscal Year 2021 NDAA and National Infrastructure Plan responsibilities. Without conducting sector-wide risk assessments, to include ransomware, SRMAs and sector entities will not know what additional security protections could be needed to address growing and evolving threats.

None of the Selected SRMAs Fully Assessed Effectiveness of Their Support Addressing Ransomware

SRMAs for the selected sectors have taken, or reported taking, steps to gather useful information about their sectors' efforts to address ransomware. In certain instances, SRMAs assessed and made revisions to improve the effectiveness of ransomware-related support based on the information they gathered.

To their credit, selected SRMAs are providing various support to help sector entities manage ransomware risks. Several SRMAs are also obtaining information on risks and feedback to understand ransomware within their respective sectors. SRMAs have also taken steps to use the risk and feedback information they gathered to modify select support, such as guidance and briefings for their respective sectors. SRMA officials also noted that they have prioritized support that emphasizes foundational cybersecurity practices, which can provide a baseline level of protection against ransomware threats.

However, the SRMAs have not fully assessed the effectiveness of their support to sectors in addressing ransomware. Specifically, three of the six selected SRMAs have evaluated aspects of their support and three SRMAs did not demonstrate efforts to evaluate any of their support. Table 4 discusses the extent to which SRMAs' assessed the effectiveness of their ransomware-related support.

Table 4: Extent to Which SRMAs Assessed Effectiveness of Ransomware-Related Support

SRMA (sector)	Description
CISA (critical manufacturing)	Partially demonstrated. CISA held roundtable discussions with sector entities through the Critical Infrastructure Partnership Advisory Council to discuss risks to the critical manufacturing sector and obtain feedback on sector needs and upcoming initiatives. CISA responded to the feedback from the Critical Infrastructure Partnership Advisory Council by providing updated guidance on supply chain risks and conducting a ransomware briefing for the sector. However, CISA did not demonstrate how it assessed the effectiveness of its support overall or other types of support to the sector in addressing ransomware.
DOE (energy)	Not demonstrated. DOE stated that industry members provided direct insights on ransomware threats and recommended additional guidance and clarifications, which were incorporated to help improve the effectiveness of the Cybersecurity Capability Maturity Model. However, the department did not provide documentation for the feedback it received or what aspects of its model were changed based on the feedback. Moreover, DOE did not demonstrate how it used feedback or other evaluation procedures to assess the effectiveness of its support overall or other types of support to the sector in addressing ransomware.
HHS (healthcare and public health)	Partially demonstrated. HHS, through its 405(d) initiative, developed and released ransomware awareness training, stakeholder job aids, and threat briefings to improve support based on ransomware threats it identified within the sector. However, it did not demonstrate that it took steps to evaluate which support would be the most effective in addressing the risks. In addition, HHS stated that its 2023 Health Industry Cybersecurity Practices guide is the result of feedback solicited from industry. HHS also conducted a Hospital Resiliency Landscape Analysis study to, among other things, measure the adoption of recommended cybersecurity practices across hospitals. However, HHS did not demonstrate how it used data, feedback, or other evaluation procedures to assess the effectiveness of its support overall or other types of support to the sector in addressing ransomware.

SRMA (sector)	Description
DOT (transportation systems)	Not demonstrated. The department stated that it obtained informal feedback on its support from owners and operators through sector coordinating council meetings. However, the department did not demonstrate that it obtained and used informal feedback from sector coordinating councils or other evaluation procedures to assess the effectiveness of ransomware-related support.
TSA (transportation systems)	Partially demonstrated. TSA used information from its analysis of cyber incidents to update security measures for the sector. In addition, the department stated that it obtained informal feedback from owners and operators on its support through sector coordinating council meetings. However, the agency did not demonstrate how it used incident analysis, feedback, or other evaluation procedures to measure the effectiveness of ransomware-related support overall or other types of support beyond sector security measures.
Coast Guard (transportation systems)	Not demonstrated. The agency stated that it obtained informal feedback from owners and operators on its support through sector coordinating council meetings. The agency also stated that it updated its online repository of cybersecurity guidance, alerts, and bulletins most relevant to the maritime environment based on the informal feedback form the sector. However, the agency did not demonstrate that it obtained informal feedback or how it used the information or evaluation procedures to assess the effectiveness of the repository or other ransomware-related support.

Source: GAO analysis of agency information. | GAO-24-106221

Notes: CISA – Cybersecurity and Infrastructure Security Agency; Coast Guard - United States Coast Guard; DOE – Department of Energy; DOT – Department of Transportation; TSA – Transportation Security Administration; SRMA – Sector Risk Management Agency.

Demonstrated = SRMA documented its assessment of the effectiveness of the entirety of its ransomware-related support; Partially demonstrated = SRMA documented its assessment of some, but not all, of its ransomware-related support; Not demonstrated = SRMA did not document its assessment of any ransomware-related support.

Agencies are lacking in their assessments of support because they do not have routine evaluation procedures for determining whether the support they provide to their respective sectors is effective in helping address ransomware threats. Such procedures could include, for example, outcome-oriented performance measures to assess the effectiveness of actions taken or an assessment of the optimal mix of support in addressing ransomware threats.

Assessing the effectiveness of the full range of support could help SRMAs determine which support, if any, to modify in providing the most helpful assistance to sectors against ransomware. For example, CISA stated that based on its experience it is currently modifying its phishing campaign service to go beyond human behavior assessments and build out additional capabilities to help prevent phishing attacks, which is the primary attack vector for ransomware attacks. Such efforts help demonstrate the importance for SRMAs to evaluate their ransomware support.

In addition, although sector entities cited positive experiences with the federal assistance, they identified concerns about agency communication, coordination, and timely sharing of threat and incident information. Fully assessing effectiveness could help address sector concerns. See appendix II for more details regarding sector entities' views on SRMAs' ransomware support.

Conclusions

Ransomware has had devastating impacts on the operations and vital services provided by critical infrastructure sectors. In recent years, these attacks have led to widespread disruptions such as regional gas shortages and cancelled urgent care surgeries. Public and private sector reporting of the impacts is not always required and comparable, which makes it more challenging for SRMAs to know the full impact of ransomware on their respective sectors. CISA is developing reporting rules that could help address the limitations of current reporting on ransomware impacts.

Additionally, SRMAs for the four selected sectors did not know the level of adoption of the NIST ransomware profile for their sectors, nor had they determined the level of adoption of other cybersecurity practices that sectors reported using to address ransomware. Adopting such practices can help sectors curb the significant impact of ransomware and improve their resiliency against related attacks. Given the significant role that SRMAs play in protecting our nation's critical infrastructure, improving their understanding of their respective sectors' cybersecurity practices will make the SRMAs a more effective partner in national efforts to combat ransomware.

Although CISA and the selected SRMAs provide important support to owners and operators, not all SRMAs have assessed ransomware risks and none of the SRMAs fully assessed the effectiveness of their ransomware support. Given that ransomware remains one of the most serious and concerning cybersecurity challenges to our nation's critical infrastructure, it is vital that the SRMAs assess risks and measure the effectiveness of their support activities to better protect their respective sectors from this pervasive threat.

Recommendations for Executive Action

We are making a total of 11 recommendations, including two to DOE, two to HHS, four to DHS, and three to DOT.

The Secretary of Energy should, in coordination with CISA and sector entities, determine the extent to which the energy sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. (Recommendation 1)

The Secretary of Energy should, in coordination with CISA and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the energy sector. (Recommendation 2)

The Secretary of Health and Human Services should, in coordination with CISA and sector entities, determine the extent to which the healthcare and public health sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. (Recommendation 3)

The Secretary of Health and Human Services should, in coordination with CISA and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the healthcare and public health sector. (Recommendation 4)

The Secretary of Homeland Security should, in coordination with CISA and sector entities, determine the extent to which the critical manufacturing sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. (Recommendation 5)

The Secretary of Homeland Security should, in coordination with CISA and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the critical manufacturing sector. (Recommendation 6)

The Secretary of Homeland Security should, in coordination with CISA, co-SRMAs, and sector entities, determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. (Recommendation 7)

The Secretary of Homeland Security should, in coordination with CISA, co-SRMAs, and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the transportation systems sector. (Recommendation 8)

The Secretary of Transportation should, in coordination with CISA, co-SRMAs, and sector entities, assess ransomware risks to the transportation systems sector. (Recommendation 9)

The Secretary of Transportation should, in coordination with CISA, co-SRMAs, and sector entities, determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. (Recommendation 10)

The Secretary of Transportation should, in coordination with CISA, co-SRMAs, and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the transportation systems sector. (Recommendation 11)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, HHS, DOE, and DOT for review and comment. We received written comments from all four agencies. Two agencies agreed with their recommendations; one agency partially agreed with one recommendation and disagreed with one recommendation; and one agency agreed with one recommendation, partially agreed with one recommendation, and disagreed with one recommendation. In addition, three agencies provided technical comments, which we incorporated as appropriate.

- In its written comments, reprinted in appendix III, DHS agreed with our four recommendations and described planned actions to address the recommendations. For example, DHS stated that CISA plans to determine the extent of cybersecurity practices that address ransomware for the critical manufacturing and transportation systems sectors. In addition, the department noted that CISA plans to routinely evaluate stakeholder feedback and sector implementation of cybersecurity practices to measure effectiveness of federal support.
- In its written comments, reprinted in appendix IV, HHS agreed with our two recommendations. However, the department stated that it believes it has already met the intent of one of our recommendations because it has conducted an initial evaluation of the sector's adoption of cybersecurity practices through prior efforts, such as its April 2023 analysis and its toolkit. HHS also noted that it would continue to coordinate with CISA and sector entities to evolve its activities and strategies in measuring adoption.

As discussed in this report, we recognize HHS's initial evaluation of NIST CSF practices through its analysis and toolkit, and acknowledge the importance of this effort. However, HHS is not yet tracking the sector's adoption of specific practices that reduce ransomware risk. If effectively implemented, HHS's plan to further evolve its activities and strategies could meet the intent of our recommendation and encourage the department to continue to strengthen its efforts in this regard. As such, we believe our recommendation is still valid.

- In its written comments, reprinted in appendix V, DOE partially agreed with our recommendation to measure the effectiveness of federal support to reduce ransomware risks and described planned and ongoing actions. DOE did not explicitly note what aspects of the recommendation it disagreed with. However, DOE stated that it will continue to work with its subsector coordinating councils to ensure that federal support is provided where needed through a risk-based approach, in accordance with statutory authorities and available resources. The department also plans to annually assess feedback from its cyber hygiene training effort and ensure that the training is based on risks and threats.

  Nevertheless, as discussed in our report, DOE had not demonstrated that it obtained feedback from subsector coordinating councils or how it used feedback or other evaluation procedures to assess the effectiveness of federal support. DOE's plan to annually assess feedback from its cyber hygiene training effort would be a positive step towards measuring effectiveness of federal support. However, as part of its responsibilities as a SRMA, DOE is also responsible for evaluating the effectiveness of the full range of support to secure the sector. Accordingly, we continue to believe that our recommendation is warranted.

  Additionally, DOE disagreed with our recommendation to determine the extent the sector has adopted leading cybersecurity practices. Specifically, DOE stated that it does not have the regulatory authority over the cybersecurity of the energy sector, and thus does not have the authority to assess adoption. Further, DOE stated that it does not have the authority to mandate specific actions by sector entities, as such authority resides with the Federal Energy Regulatory Commission.

  We are not recommending that DOE exercise any regulatory authority, however. We are recommending that it determine the extent to which the energy sector is adopting certain practices. As a designated SRMA, DOE has the responsibility to strengthen the sector's security and resilience against cyber threats. Obtaining information on the sector's adoption of cybersecurity practices, even if only voluntarily provided, can give DOE insight into the sector's resilience and help better inform the department's efforts to curb the significant impact of ransomware within the sector.

As discussed in our report, DOE conducted research to obtain high-level insights on the adoption and impact of leading practices. While its research did not have insights into specific practices that address ransomware, it demonstrated that DOE has the ability to obtain voluntary information on adoption. Furthering its understanding of the sector's use of leading practices will make DOE a more effective partner in national efforts to combat ransomware. Accordingly, we continue to believe that our recommendation is warranted.

- In its written comments, reprinted in appendix VI, DOT agreed with our recommendation to assess risks to the transportation systems sector and partially agreed with our recommendation to measure the effectiveness of federal support to reduce ransomware risks.

  Specifically, DOT stated that it believes DHS and CISA, in coordination with the FBI and SRMAs, would be the appropriate cross-sector lead for a more comprehensive evaluation of federal support within the transportation systems sector. However, as a co-SRMA, DOT is one of the two co-leads for supporting the security of the transportation systems sector. As part of these co-lead responsibilities, DOT is responsible for evaluating the effectiveness of the full range of support to secure the sector. Our recommendation acknowledges this responsibility and notes that DOT should coordinate, as appropriate, with CISA, co-SRMAs, and sector partners. Accordingly, we continue to believe that our recommendation is warranted.

  Additionally, DOT disagreed with our recommendation for the department to determine the extent the sector has adopted leading cybersecurity practices. Specifically, DOT stated that it believes that determining measures of adoption would only provide a snapshot in time. Further, DOT expressed concerns that the department and co-SRMAs can neither verify nor cite voluntary information as comprehensive. Rather than take our recommended action, the department stated that it will increase efforts to encourage adoption of leading cybersecurity practices.

  Although DOT's plan to encourage leading cybersecurity practices may help spread awareness, this approach does not assess the sector's adoption of the practices. Regarding the department's concern about a measurement of adoption providing only a snapshot in time, such an evaluation would still have value because it can help determine the sector's initial level of adoption of the practices and establish a baseline for DOT's assessment of sector risks. Further, even collecting limited, voluntary information from the sector can help SRMAs to better identify gaps, assess risks, and prioritize cybersecurity-related support. Improving its understanding of the transportation systems sector's practices that address ransomware will make DOT a more effective partner in national efforts to combat ransomware. Accordingly, we continue to believe that our recommendation is warranted.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Energy, Health and Human Services, Homeland Security, and Transportation; and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at 214-777-5719 or at hinchmand@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 key contributions to this report are listed in appendix VII.

David B Hinchman

David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the reported impact of ransomware attacks on selected critical infrastructure sectors, (2) assess Sector Risk Management Agencies' (SRMA) efforts to oversee selected sectors' adoption of leading federal practices to prevent and respond to ransomware attacks, and (3) evaluate the extent to which SRMAs for selected sectors assessed ransomware risks and the effectiveness of their support to help owners and operators address threats.

To select critical infrastructure sectors for our review, we examined Federal Bureau of Investigation's (FBI) Internet Crime Report 2021,[1] the Cybersecurity and Infrastructure Security Agency's (CISA) internal data on the number of reported attacks by sector, and Temple University's Critical Infrastructure Ransomware Attacks dataset.[2] From these sources, we selected four sectors to review based on their designation as a lifeline or non-lifeline sector,[3] the number of reported ransomware incidents in the sector, and the reported cost impacts to organizations in the sector as a result of ransomware attacks. We excluded the government facilities sector from our selection process because we recently reported on federal efforts to address ransomware in the sector.[4]

Specifically, we selected two lifeline sectors and two non-lifeline sectors that were among those with the largest number of reported ransomware incidents. We then confirmed that these sectors were also among those with greatest reported cost impacts based on reported ransomware payments and demand data. The four sectors we selected were the critical manufacturing, energy, healthcare and public health, and transportation systems sectors.

[1] FBI, Internet Crime Complaint Center, *Internet Crime Report 2021* (Washington D.C.: March 22, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

[2] Rege, A. (2023). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset." Version 12.8. Temple University. Online at *https://sites.temple.edu/care/cira/*. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

[3] The Department of Homeland Security defines a lifeline sector as sectors that are essential to the operation of most critical infrastructure sectors. There are four lifeline sectors: communications, energy, transportation systems, and water.

[4] GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats*, GAO-22-105024 (Washington, D.C.: Oct. 13, 2021) *Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767 (Washington, D.C.: Sept. 14, 2022); and *Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity*, GAO-23-105480 (Washington, D.C.: Oct. 20, 2022).

To assess the reliability of data provided by Temple University and CISA, we compared the results to other documentation, such as FBI and private sector reporting, interviewed knowledgeable officials from CISA, and performed manual testing for missing values and obvious errors. We determined that the data were sufficiently reliable for the purpose of selecting sectors to review.

To address our first objective, we analyzed reports based on publicly disclosed ransomware incidents from Temple University's Critical Infrastructure Ransomware Attacks dataset. We also reviewed vendor research on ransomware attacks from Sophos' The State of Ransomware 2022 report [5] and the NetDiligence Ransomware 2022 Spotlight Report. We summarized statistics and trends on the number of ransomware incidents among the selected critical infrastructure sectors from these reports.[6] We also reviewed data from CISA, the Transportation Security Administration (TSA), and the Department of the Treasury on the number of incidents that sector entities reported to the SRMAs. We compared data from federal agencies to public reporting on the ransomware incidents to identify any discrepancies. To determine the reliability of this data, we reviewed related documentation, interviewed knowledgeable officials, and performed manual testing for missing values and obvious errors, where appropriate. We determined the data were sufficiently reliable for the purpose of describing potential impacts of ransomware. Where we identified limitations in the data, we describe those in the report.

We also determined that the information and communication component of internal control was significant to this objective, along with the underlying principles that management should use quality information to achieve the entity's objectives and externally communicate the necessary quality information to achieve the entity's objectives. We assessed the quality and quantity of information available to SRMAs and sector entities, as well as SRMAs' efforts to collect and disseminate relevant and accurate data on the number of ransomware attacks, and the impacts of those ransomware attacks, across the four selected sectors.

To address the second objective, we identified guidance established by the National Institute of Standards and Technology's (NIST),

[5] Sally Adam, *The State of Ransomware 2022,* Sophos (Abington, UK; Apr. 27, 2022).

[6] NetDiligence, *Ransomware 2022 Spotlight Report* (Gladwyne, PA: October 2022*),* https://netdiligence.com/cyber-claims-studies/.

Ransomware Risk Management: A Cybersecurity Framework Profile (ransomware profile). NIST's guidance provides a set of leading federal practices to address ransomware. We then reviewed sector-specific plans, prior GAO reporting on ransomware, and interviews with SRMAs to compile a list of known sets of federal and nonfederal practices that were applicable to all sectors, as well as practices that were sector-specific. We verified our list of federal and nonfederal practices by asking officials from the sector coordinating councils (SCC), subsector coordinating councils, and information sharing and analysis centers (ISAC) to verify if entities in the sector used the leading federal and nonfederal practices, and if there were any additional practices used in the sector.

We analyzed the extent to which documentation describing the sets of practices demonstrated how they aligned with NIST's ransomware profile. We also reviewed agency documentation to determine if the SRMAs in the selected sectors were tracking the implementation of either the NIST ransomware profile practices, or other federal and nonfederal practices.

We determined that the information and communication and control activities components of internal control was significant to this objective, along with the underlying principles that management should design control activities to achieve objectives and respond to risks, use quality information to achieve the entity's objectives, and externally communicate the necessary quality information to achieve the entity's objectives. We reviewed the practices in the ransomware profile to determine the suggested baseline activities recommended to protect against ransomware attacks. We then assessed the selected SRMAs' efforts to track the sectors' implementation of the selected leading federal and nonfederal practices.

To address the third objective, we reviewed agency documentation on agency support that SRMAs provide to help address ransomware threats, such as risk analysis, incident summaries, informal feedback, and briefings to sector entities.

We then identified whether each SRMA documented efforts to gather and analyze information on sector ransomware risks, as called for by the Fiscal Year 2021 National Defense Authorization Act.[7] We also made determinations about the extent to which the SRMAs had demonstrated

[7] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002(c)(1), 134 Stat. 3388, 4770 (Jan. 1, 2021), codified at 6 U.S.C. § 665d.

that they evaluated the effectiveness of support addressing ransomware, as called for in the 2013 National Infrastructure Protection Plan.[8] A rating of "demonstrated" reflected that the SRMA documented its assessment of the effectiveness of the entirety of its ransomware-related support. A rating of "partially demonstrated" reflected that the SRMA documented its assessment of some, but not all, of its ransomware-related support. A rating of "not demonstrated" reflected that the SRMA did not document its assessment of any ransomware-related support.

We determined that the risk assessment, control activities, and information and communication components of internal control were significant to this objective, including their underlying principles. Among others, we reviewed underlying principles, such as management should identify, analyze, and respond to risks, design control activities, and use quality information to achieve objectives. We reviewed agency documentation to determine what efforts SRMAs have made to identify ransomware risks to their sectors, and any attempts to communicate those risks to sector entities. We also reviewed SRMAs' attempts to assess the effectiveness of those initiatives based on evolving risks and feedback from sector entities.

For all objectives, we conducted interviews with officials from SRMAs, SCCs, and ISACs to obtain data and perspectives on ransomware trends and statistics, the sectors' adoption of leading federal and nonfederal practices to address ransomware, and federal ransomware assistance efforts. Specifically, we interviewed officials from the six federal agencies that serve as SRMAs for the four sectors we selected to review. The six agencies were CISA (critical manufacturing sector); Department of Energy (energy sector); HHS (healthcare and public health sector); and Department of Transportation, TSA, and U.S. Coast Guard (transportation systems sector).

With respect to interviews with sector entities, we interviewed officials from two SCCs, three subsector coordinating councils, and three ISACs. Specifically, we interviewed SCC officials that represented the critical manufacturing and healthcare and public health sector. For the energy and transportation systems sectors, we interviewed officials from the electricity, oil and natural gas, and mass transit and passenger rail subsector councils since the energy and transportation systems sectors

[8] Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013).

did not have a sector-wide SCC.[9] We also interviewed officials from the electricity, healthcare and public health, and oil and natural gas ISACs.[10]

We analyzed responses from our interviews with officials from SCCs and ISACs. To do so, we systematically coded the qualitative data in order to identify common trends across the interviews. Specifically, we coded the relevant statements made in each documented interview using five general categories of responses, which were leading practices, services, concerns, impacts, and feedback. We also used 37 subcategories to further analyze and draw conclusions on the five broad categories such as overall themes, benefits, challenges, and improvement opportunities expressed by the coordinating council and ISAC officials we interviewed.

Prior to the coding process, we verified that the categories and their definitions were accurate, applicable, and clear. To do this, two analysts coded a sample of two interviews using the five categories and supporting subcategories to identify any inconsistencies and potential revisions to the categories or their definitions. Once we reviewed all of the responses from the interviewees using the categories, we had two analysts verify the coded statements.

In addition, we interviewed officials from relevant federal agencies to gain additional perspectives on any existing or planned efforts that may address the challenges or improvement opportunities that coordinating council and ISAC officials identified. Due to the sensitivity of coordinating councils' and ISACs' interactions with the federal government, we are reporting information on coordinating councils and ISAC officials' perspectives in the aggregate. The results from these semi-structured interviews are not generalizable, but provide insight into sector financial and nonfinancial impacts from ransomware attacks, adoption of leading federal and nonfederal practices, and perspectives on the federal government's efforts with ransomware.

[9] For the energy sector, we interviewed each of the two subsectors, (1) electricity and (2) oil and natural gas. For the transportation systems sector, we selected three of the seven transportation systems subsectors to interview that were among those most targeted by ransomware, as reported in Temple University's *Critical Infrastructure Ransomware Attacks* dataset. We met with the mass transit and passenger rail subsectors while the highway and motor carrier declined our invitation to meet. At the time of our review, there was no private sector representative for the postal and shipping subsector to interview.

[10] The critical manufacturing sector, unlike the other three selected sectors, did not have a dedicated ISAC at the time of our review.

We conducted this performance audit from August 2022 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Sector Entity Viewpoints on Federal Support Addressing Ransomware

Seven of the eight sector entities (sector coordinating councils (SCC) and information sharing and analysis centers (ISAC)) we interviewed identified positive impacts resulting from the sector risk management agencies' (SRMA) assistance and support efforts to address ransomware threats. Among other assistance, sector entities cited helpful ransomware guidance, detailed threat alerts, and helpful technical tools. For example, one sector official stated that phishing campaigns have been an effective way to minimize the risk of ransomware. The official explained that when owners and operators know what to block, they could potentially avoid becoming a victim or expedite their response and recovery efforts and minimize the impact to the sector.

Although sector entities cited positive experiences with the federal assistance, they identified challenges and opportunities for improvement related to communication, information sharing, and coordination. For example, of the eight sector entities:

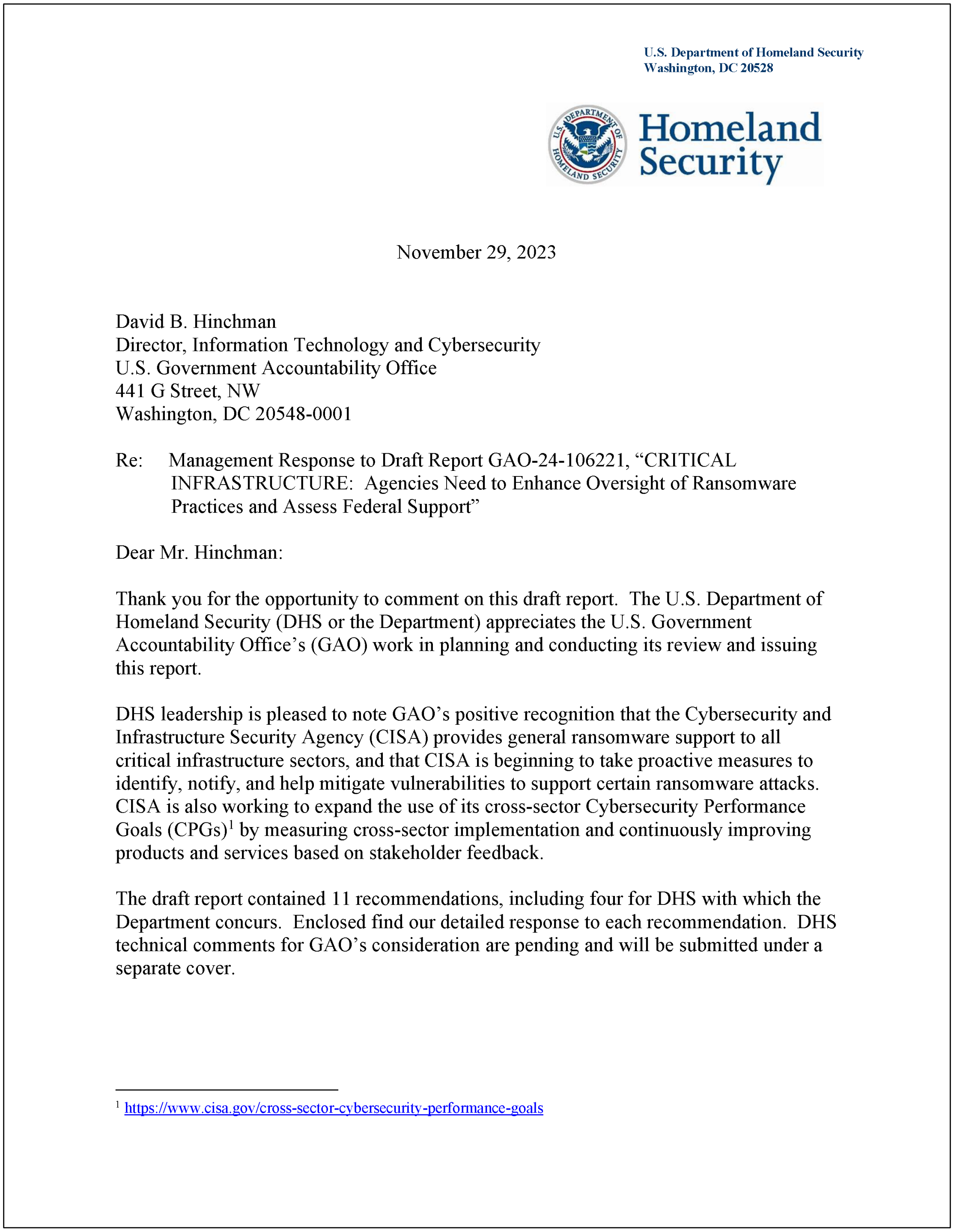
- Five sector entities reported inconsistent communication regarding ransomware assistance from the Cybersecurity and Infrastructure Security Agency (CISA) and the SRMAs. For example, one sector entity felt that CISA had not met its promises to provide a sufficient number of technical cybersecurity services. One entity stated that it requested a penetration test twice and never heard back from CISA. CISA acknowledged that it had not provided a penetration test and stated that it has since changed its service model to ensure timely delivery of services. In addition, four sector entities expressed that they did not always receive communication on the ways that CISA responded to sector-specific concerns.

  Two sector entities also stated that they lacked clarity on where to report a ransomware incident, who to contact for assistance, what assistance was available from CISA and the SRMAs, and whether the reported information would be shared or made public.

- Three sector entities reported a lack of timely and actionable sharing of threat and incident information. For example, two entities stated that while CISA's threat briefings were helpful to the sector, they did not always include actionable information, such as tactics and techniques, or information not already reported in the media. Additionally, sector entities believed that CISA's and the SRMAs' efforts to share information on threats were generally slow. Five sector entities noted that they would like agencies to send out incident notifications earlier, hold more threat briefings, and disseminate active threat information anonymously for ongoing incidents especially if incidents could impact multiple sectors.

- All eight sector entities reported that CISA and SRMAs could enhance coordination with sector entities, such as when developing federal initiatives and best practices. For example, one sector entity expressed frustration with CISA's initial efforts to release its Cybersecurity Performance Goals. Officials noted that while CISA created best practices for all sectors, the agency's effort was not inclusive and did not include adequate coordination or input from sector entities. As a result, sector owners and operators were unsure of which practices to adopt. As another example, an SCC noted that they did not get an opportunity to review a cybersecurity assessment of its sector to help CISA ensure it was protecting sensitive information. According to CISA, it held public and cross-sector workshops to discuss feedback on its Cybersecurity Performance Goals and it reviewed approximately 1,900 comments from across all sectors and stakeholders. While one sector entity stated that CISA acknowledged that the initial release of its Cybersecurity Performance Goals was not inclusive, it stated that CISA has since taken steps to fix it.

Appendix III: Comments from the Department of Homeland Security



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

Homeland
Security

November 29, 2023

David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106221, “CRITICAL INFRASTRUCTURE: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support”

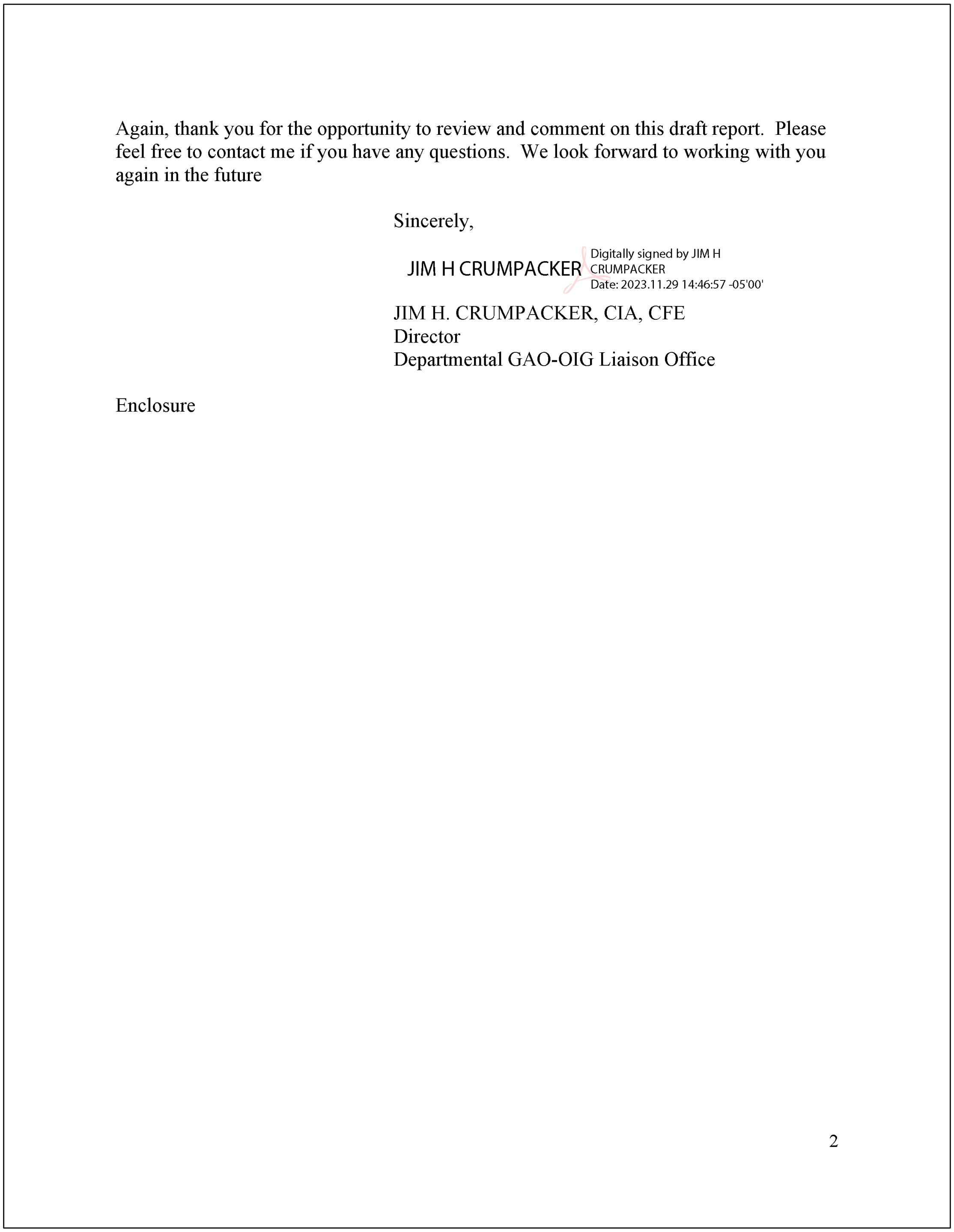
Dear Mr. Hinchman:

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

DHS leadership is pleased to note GAO’s positive recognition that the Cybersecurity and Infrastructure Security Agency (CISA) provides general ransomware support to all critical infrastructure sectors, and that CISA is beginning to take proactive measures to identify, notify, and help mitigate vulnerabilities to support certain ransomware attacks. CISA is also working to expand the use of its cross-sector Cybersecurity Performance Goals (CPGs)[1] by measuring cross-sector implementation and continuously improving products and services based on stakeholder feedback.

The draft report contained 11 recommendations, including four for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS technical comments for GAO’s consideration are pending and will be submitted under a separate cover.

[1] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals



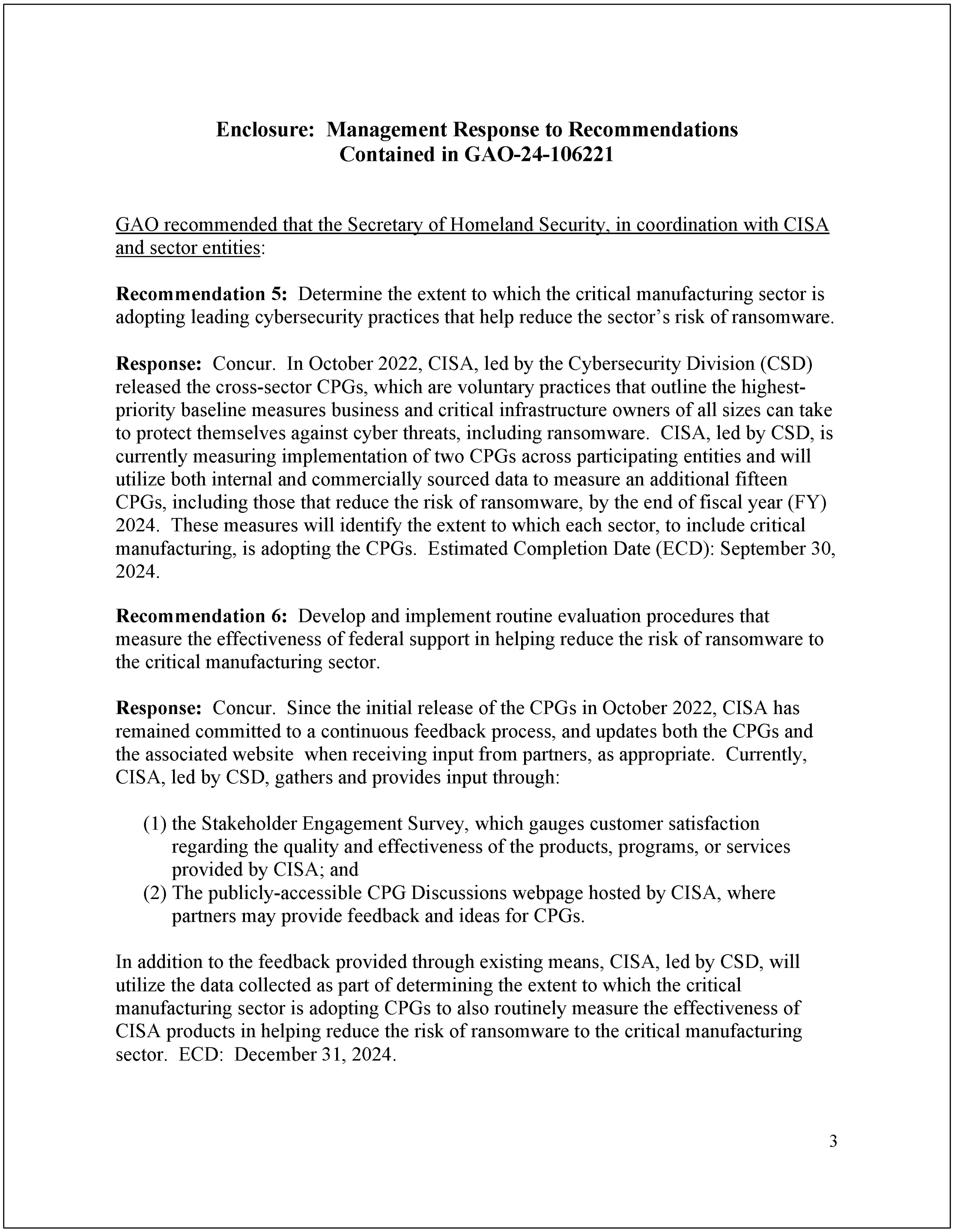
Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.11.29 14:46:57 -05'00'

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

Enclosure



Enclosure: Management Response to Recommendations Contained in GAO-24-106221

GAO recommended that the Secretary of Homeland Security, in coordination with CISA and sector entities:

Recommendation 5: Determine the extent to which the critical manufacturing sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.

Response: Concur. In October 2022, CISA, led by the Cybersecurity Division (CSD) released the cross-sector CPGs, which are voluntary practices that outline the highest-priority baseline measures business and critical infrastructure owners of all sizes can take to protect themselves against cyber threats, including ransomware. CISA, led by CSD, is currently measuring implementation of two CPGs across participating entities and will utilize both internal and commercially sourced data to measure an additional fifteen CPGs, including those that reduce the risk of ransomware, by the end of fiscal year (FY) 2024. These measures will identify the extent to which each sector, to include critical manufacturing, is adopting the CPGs. Estimated Completion Date (ECD): September 30, 2024.

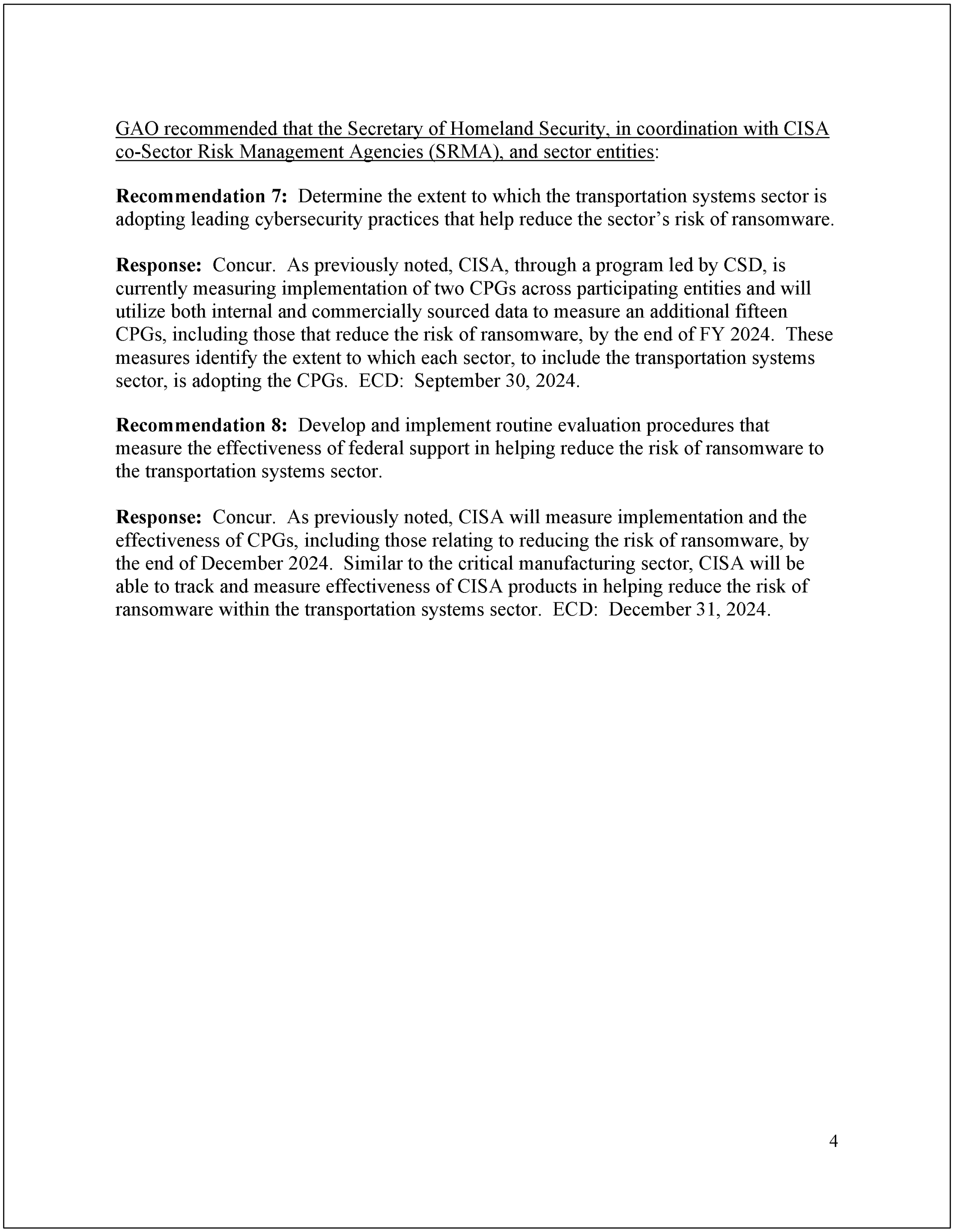
Recommendation 6: Develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the critical manufacturing sector.

Response: Concur. Since the initial release of the CPGs in October 2022, CISA has remained committed to a continuous feedback process, and updates both the CPGs and the associated website when receiving input from partners, as appropriate. Currently, CISA, led by CSD, gathers and provides input through:

(1) the Stakeholder Engagement Survey, which gauges customer satisfaction regarding the quality and effectiveness of the products, programs, or services provided by CISA; and
(2) The publicly-accessible CPG Discussions webpage hosted by CISA, where partners may provide feedback and ideas for CPGs.

In addition to the feedback provided through existing means, CISA, led by CSD, will utilize the data collected as part of determining the extent to which the critical manufacturing sector is adopting CPGs to also routinely measure the effectiveness of CISA products in helping reduce the risk of ransomware to the critical manufacturing sector. ECD: December 31, 2024.

3



GAO recommended that the Secretary of Homeland Security, in coordination with CISA co-Sector Risk Management Agencies (SRMA), and sector entities:

Recommendation 7: Determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.

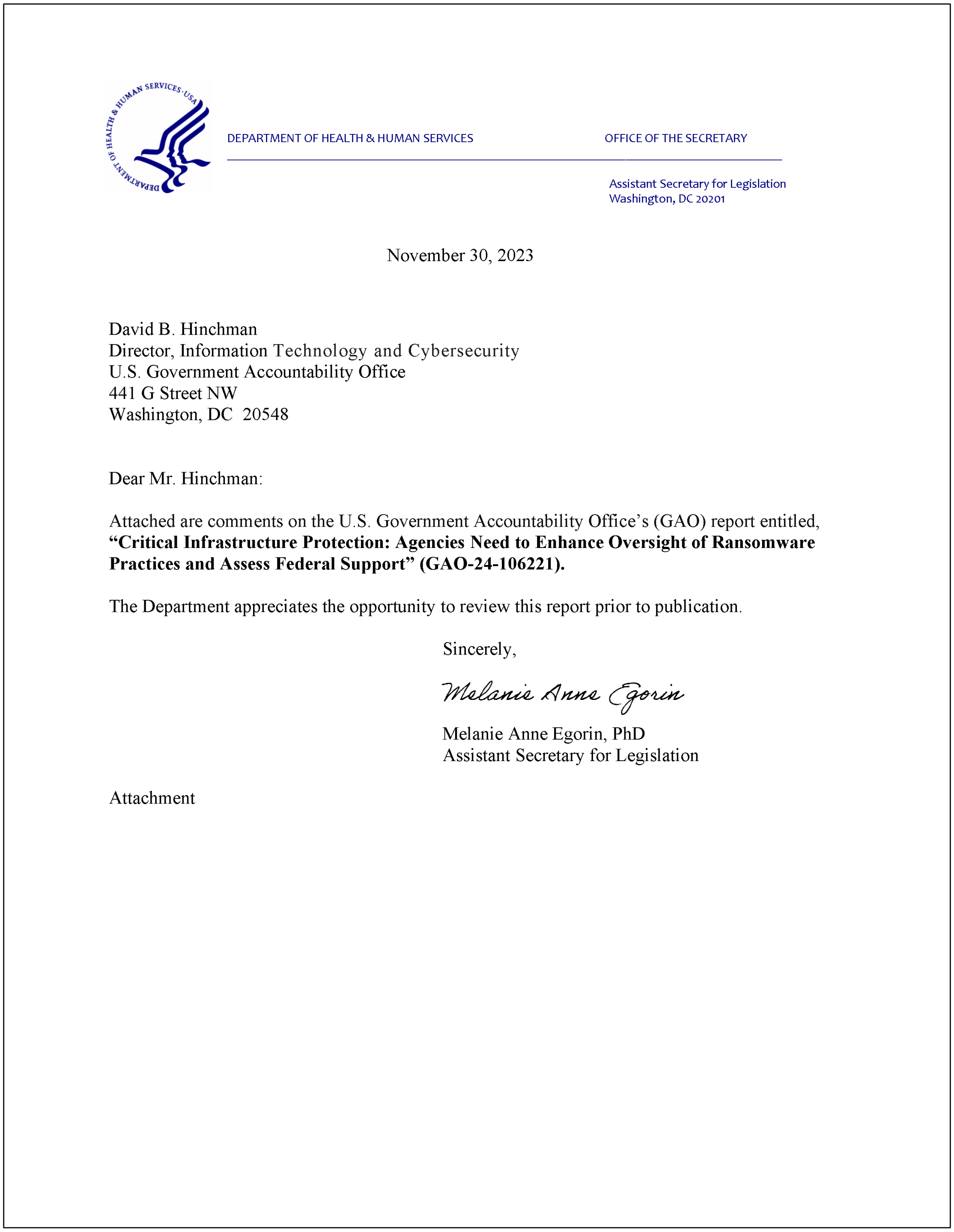
Response: Concur. As previously noted, CISA, through a program led by CSD, is currently measuring implementation of two CPGs across participating entities and will utilize both internal and commercially sourced data to measure an additional fifteen CPGs, including those that reduce the risk of ransomware, by the end of FY 2024. These measures identify the extent to which each sector, to include the transportation systems sector, is adopting the CPGs. ECD: September 30, 2024.

Recommendation 8: Develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the transportation systems sector.

Response: Concur. As previously noted, CISA will measure implementation and the effectiveness of CPGs, including those relating to reducing the risk of ransomware, by the end of December 2024. Similar to the critical manufacturing sector, CISA will be able to track and measure effectiveness of CISA products in helping reduce the risk of ransomware within the transportation systems sector. ECD: December 31, 2024.

4

Appendix IV: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES — OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

November 30, 2023

David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support" (GAO-24-106221).**

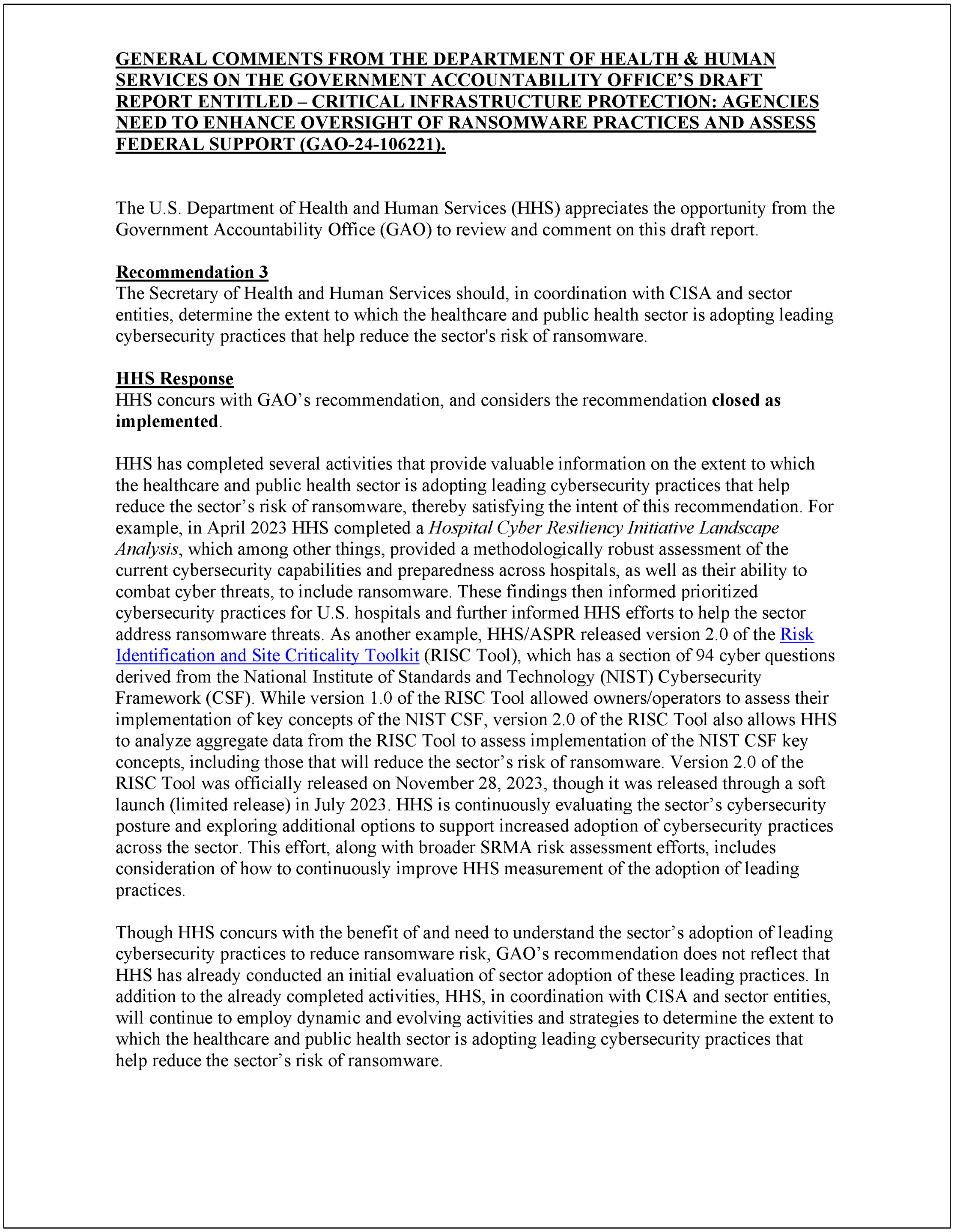
The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CRITICAL INFRASTRUCTURE PROTECTION: AGENCIES NEED TO ENHANCE OVERSIGHT OF RANSOMWARE PRACTICES AND ASSESS FEDERAL SUPPORT (GAO-24-106221).

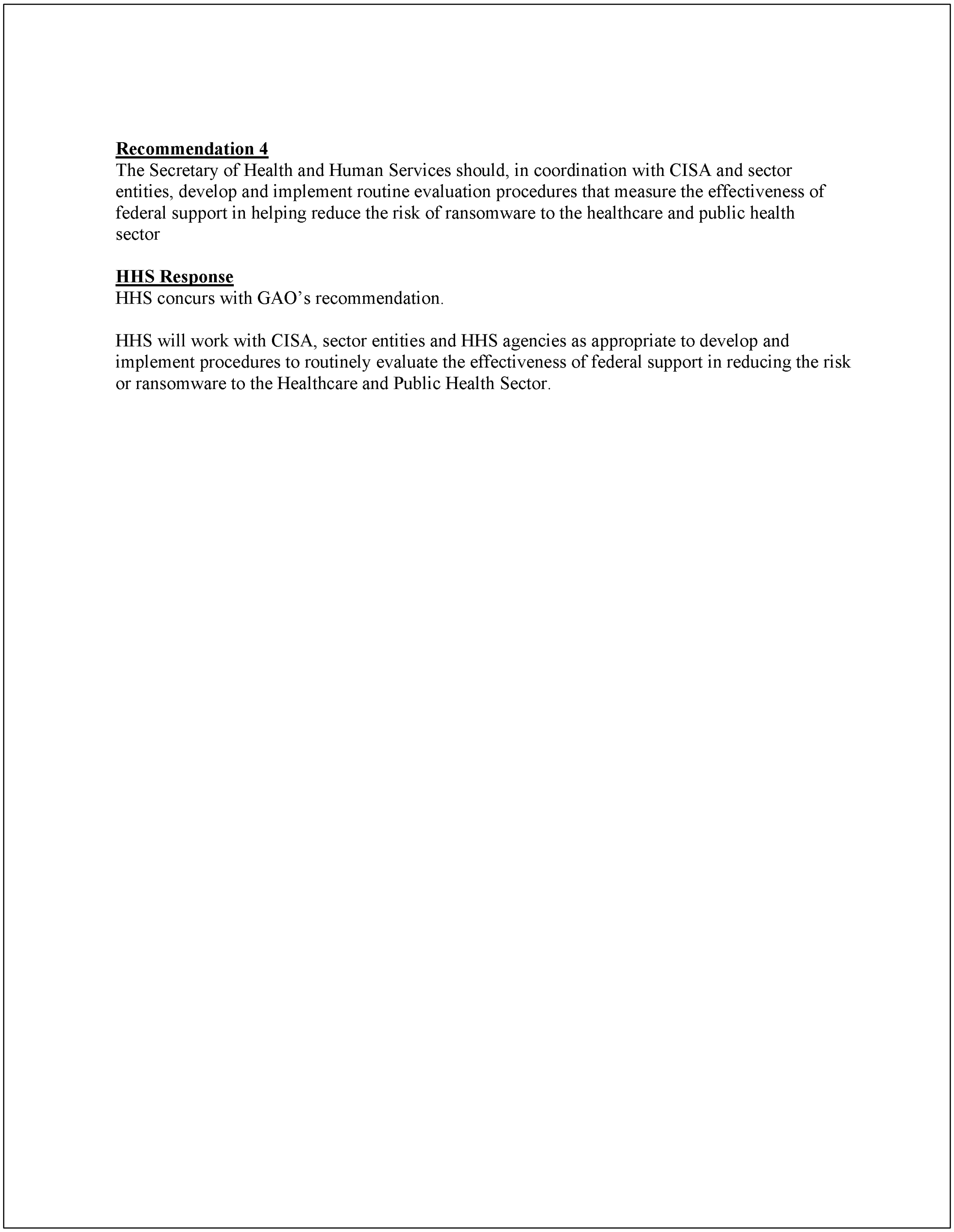
The U.S. Department of Health and Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 3
The Secretary of Health and Human Services should, in coordination with CISA and sector entities, determine the extent to which the healthcare and public health sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.

HHS Response
HHS concurs with GAO's recommendation, and considers the recommendation **closed as implemented**.

HHS has completed several activities that provide valuable information on the extent to which the healthcare and public health sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware, thereby satisfying the intent of this recommendation. For example, in April 2023 HHS completed a *Hospital Cyber Resiliency Initiative Landscape Analysis*, which among other things, provided a methodologically robust assessment of the current cybersecurity capabilities and preparedness across hospitals, as well as their ability to combat cyber threats, to include ransomware. These findings then informed prioritized cybersecurity practices for U.S. hospitals and further informed HHS efforts to help the sector address ransomware threats. As another example, HHS/ASPR released version 2.0 of the Risk Identification and Site Criticality Toolkit (RISC Tool), which has a section of 94 cyber questions derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). While version 1.0 of the RISC Tool allowed owners/operators to assess their implementation of key concepts of the NIST CSF, version 2.0 of the RISC Tool also allows HHS to analyze aggregate data from the RISC Tool to assess implementation of the NIST CSF key concepts, including those that will reduce the sector's risk of ransomware. Version 2.0 of the RISC Tool was officially released on November 28, 2023, though it was released through a soft launch (limited release) in July 2023. HHS is continuously evaluating the sector's cybersecurity posture and exploring additional options to support increased adoption of cybersecurity practices across the sector. This effort, along with broader SRMA risk assessment efforts, includes consideration of how to continuously improve HHS measurement of the adoption of leading practices.

Though HHS concurs with the benefit of and need to understand the sector's adoption of leading cybersecurity practices to reduce ransomware risk, GAO's recommendation does not reflect that HHS has already conducted an initial evaluation of sector adoption of these leading practices. In addition to the already completed activities, HHS, in coordination with CISA and sector entities, will continue to employ dynamic and evolving activities and strategies to determine the extent to which the healthcare and public health sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.

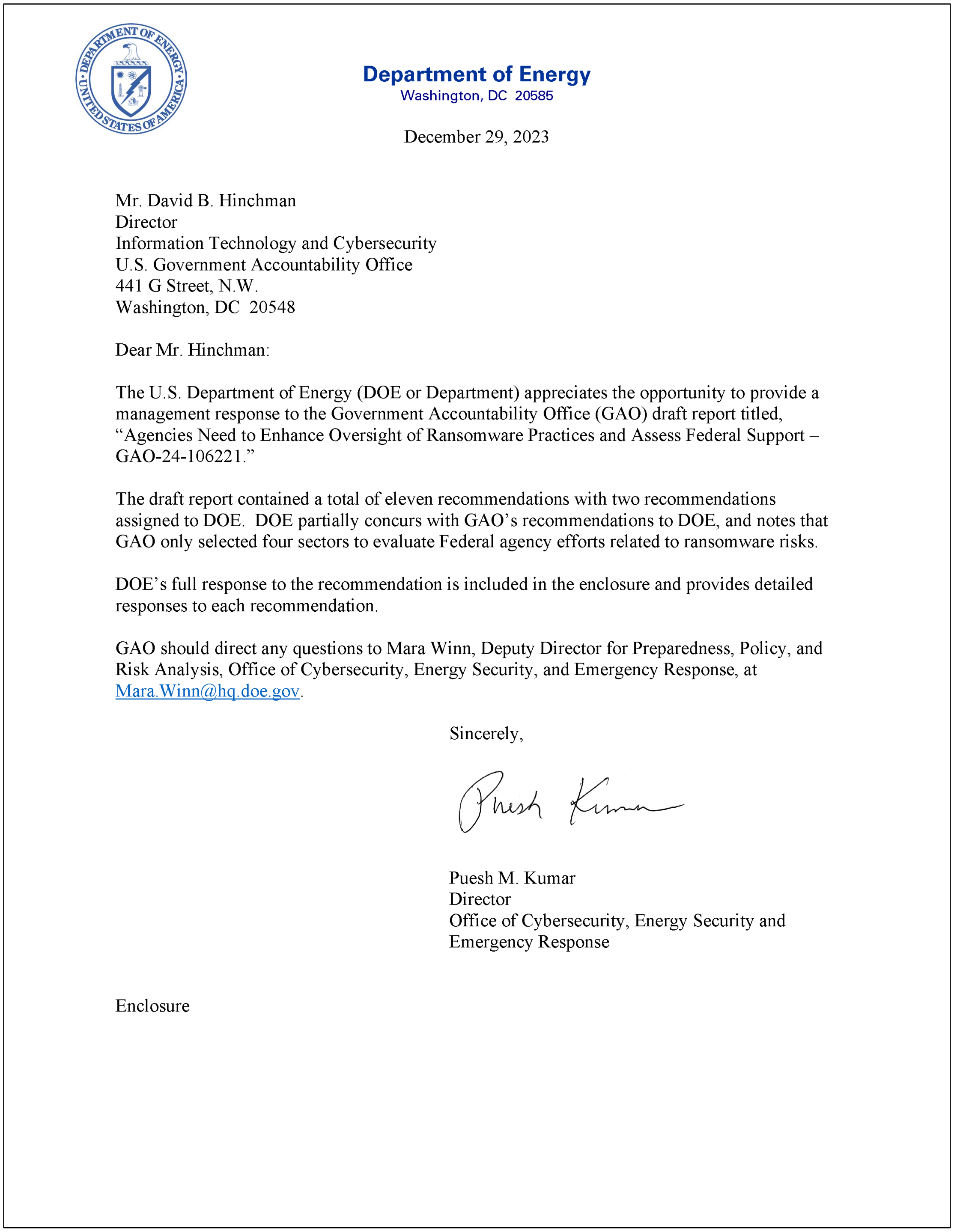


Recommendation 4
The Secretary of Health and Human Services should, in coordination with CISA and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the healthcare and public health sector

HHS Response
HHS concurs with GAO's recommendation.

HHS will work with CISA, sector entities and HHS agencies as appropriate to develop and implement procedures to routinely evaluate the effectiveness of federal support in reducing the risk or ransomware to the Healthcare and Public Health Sector.

Appendix V: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

December 29, 2023

Mr. David B. Hinchman
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Hinchman:

The U.S. Department of Energy (DOE or Department) appreciates the opportunity to provide a management response to the Government Accountability Office (GAO) draft report titled, "Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support – GAO-24-106221."

The draft report contained a total of eleven recommendations with two recommendations assigned to DOE. DOE partially concurs with GAO's recommendations to DOE, and notes that GAO only selected four sectors to evaluate Federal agency efforts related to ransomware risks.

DOE's full response to the recommendation is included in the enclosure and provides detailed responses to each recommendation.

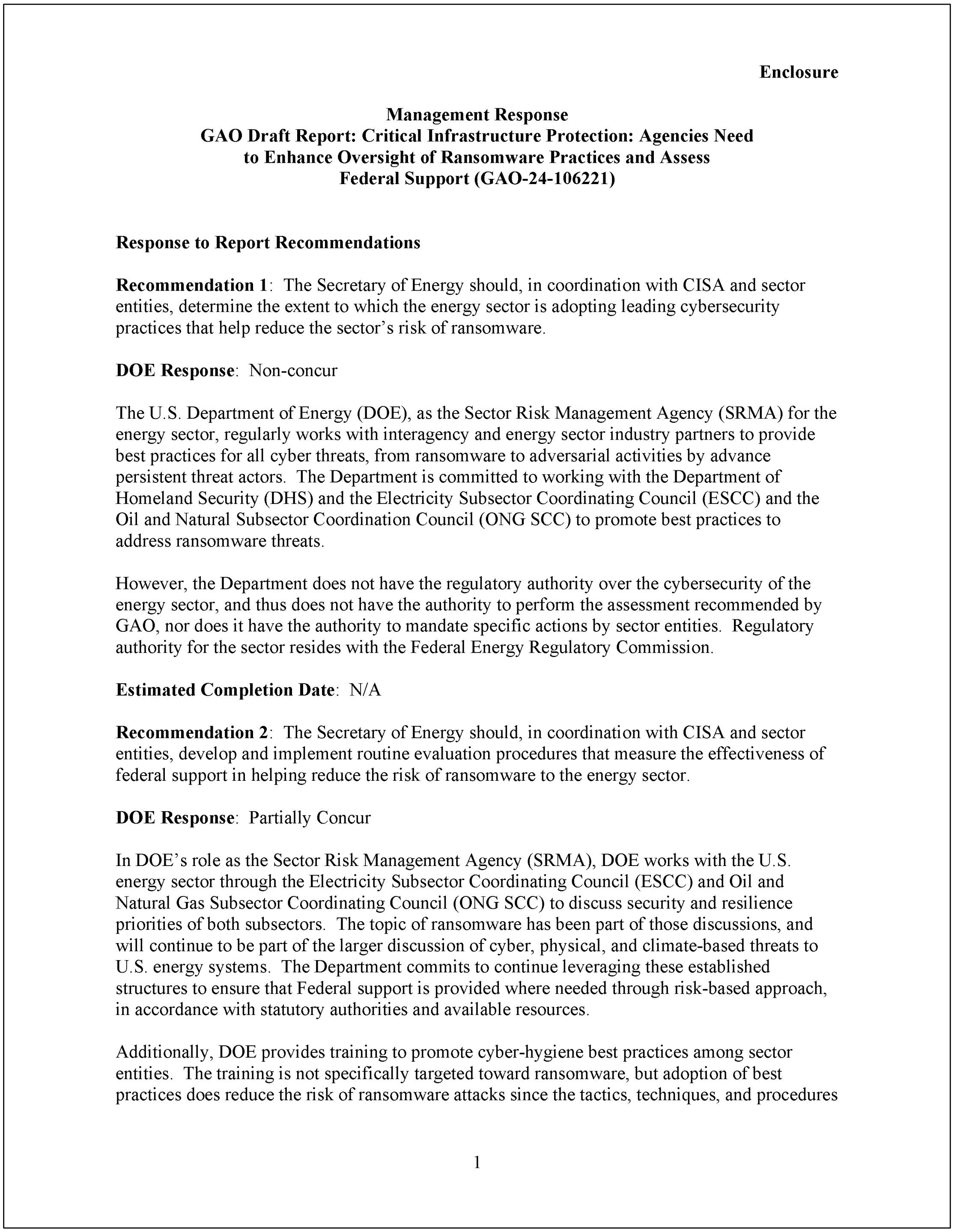
GAO should direct any questions to Mara Winn, Deputy Director for Preparedness, Policy, and Risk Analysis, Office of Cybersecurity, Energy Security, and Emergency Response, at Mara.Winn@hq.doe.gov.

Sincerely,

Puesh Kumar

Puesh M. Kumar
Director
Office of Cybersecurity, Energy Security and
Emergency Response

Enclosure



Enclosure

Management Response
GAO Draft Report: Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support (GAO-24-106221)

Response to Report Recommendations

Recommendation 1: The Secretary of Energy should, in coordination with CISA and sector entities, determine the extent to which the energy sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.

DOE Response: Non-concur

The U.S. Department of Energy (DOE), as the Sector Risk Management Agency (SRMA) for the energy sector, regularly works with interagency and energy sector industry partners to provide best practices for all cyber threats, from ransomware to adversarial activities by advance persistent threat actors. The Department is committed to working with the Department of Homeland Security (DHS) and the Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Subsector Coordination Council (ONG SCC) to promote best practices to address ransomware threats.

However, the Department does not have the regulatory authority over the cybersecurity of the energy sector, and thus does not have the authority to perform the assessment recommended by GAO, nor does it have the authority to mandate specific actions by sector entities. Regulatory authority for the sector resides with the Federal Energy Regulatory Commission.

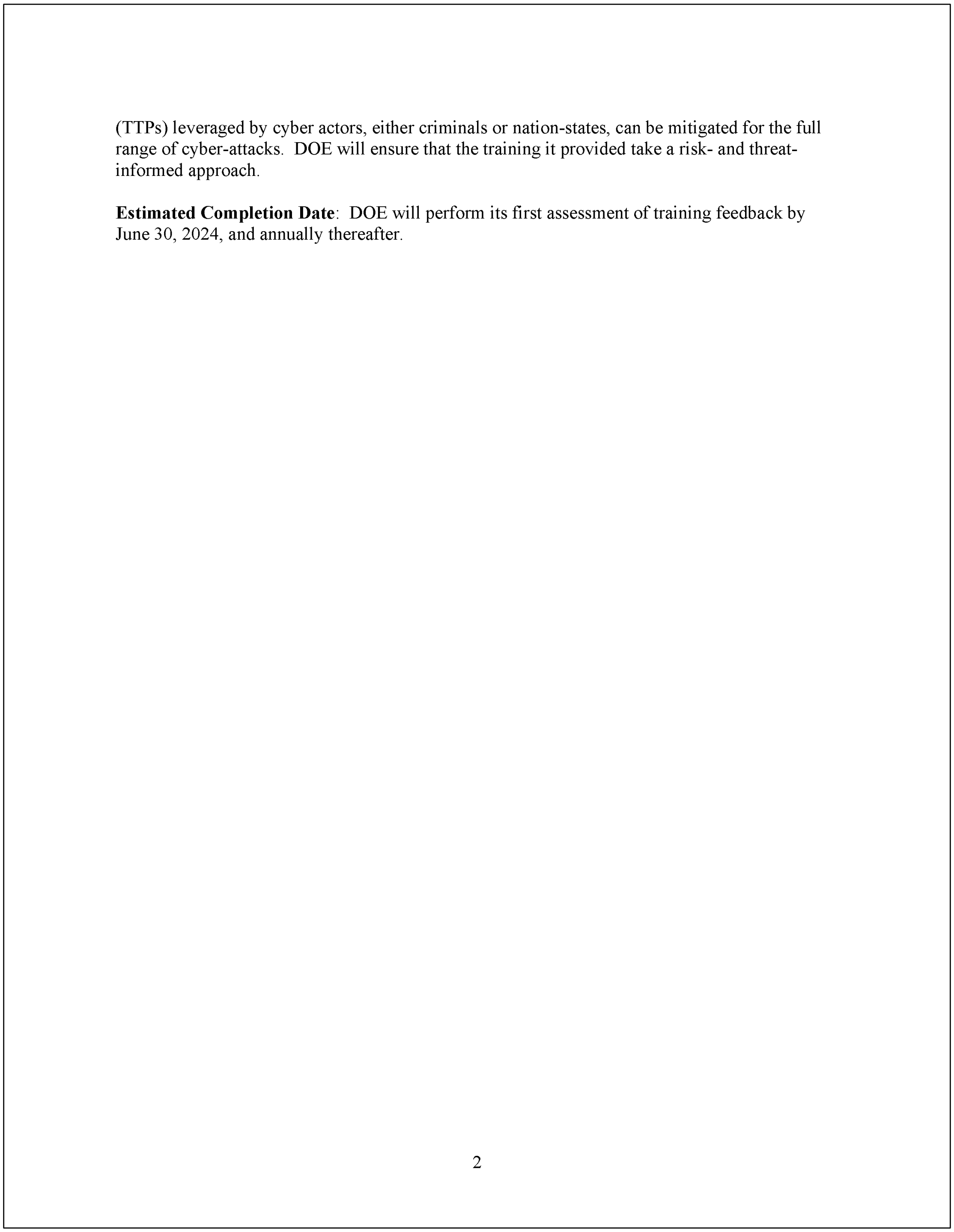
Estimated Completion Date: N/A

Recommendation 2: The Secretary of Energy should, in coordination with CISA and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the energy sector.

DOE Response: Partially Concur

In DOE's role as the Sector Risk Management Agency (SRMA), DOE works with the U.S. energy sector through the Electricity Subsector Coordinating Council (ESCC) and Oil and Natural Gas Subsector Coordinating Council (ONG SCC) to discuss security and resilience priorities of both subsectors. The topic of ransomware has been part of those discussions, and will continue to be part of the larger discussion of cyber, physical, and climate-based threats to U.S. energy systems. The Department commits to continue leveraging these established structures to ensure that Federal support is provided where needed through risk-based approach, in accordance with statutory authorities and available resources.

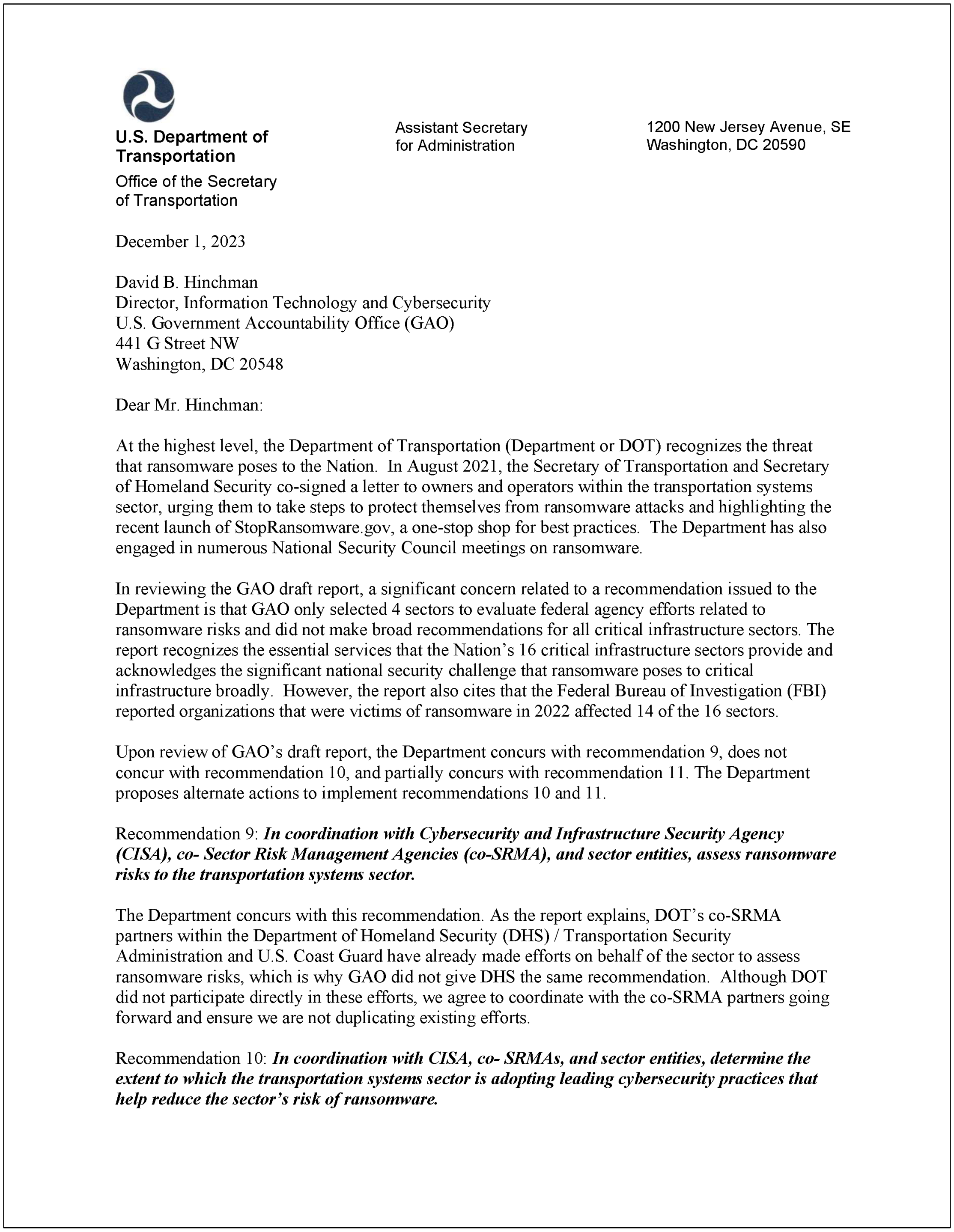
Additionally, DOE provides training to promote cyber-hygiene best practices among sector entities. The training is not specifically targeted toward ransomware, but adoption of best practices does reduce the risk of ransomware attacks since the tactics, techniques, and procedures



(TTPs) leveraged by cyber actors, either criminals or nation-states, can be mitigated for the full range of cyber-attacks. DOE will ensure that the training it provided take a risk- and threat-informed approach.

Estimated Completion Date: DOE will perform its first assessment of training feedback by June 30, 2024, and annually thereafter.

Appendix VI: Comments from the Department of Transportation



U.S. Department of Transportation

Office of the Secretary
of Transportation

Assistant Secretary
for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

December 1, 2023

David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman:

At the highest level, the Department of Transportation (Department or DOT) recognizes the threat that ransomware poses to the Nation. In August 2021, the Secretary of Transportation and Secretary of Homeland Security co-signed a letter to owners and operators within the transportation systems sector, urging them to take steps to protect themselves from ransomware attacks and highlighting the recent launch of StopRansomware.gov, a one-stop shop for best practices. The Department has also engaged in numerous National Security Council meetings on ransomware.

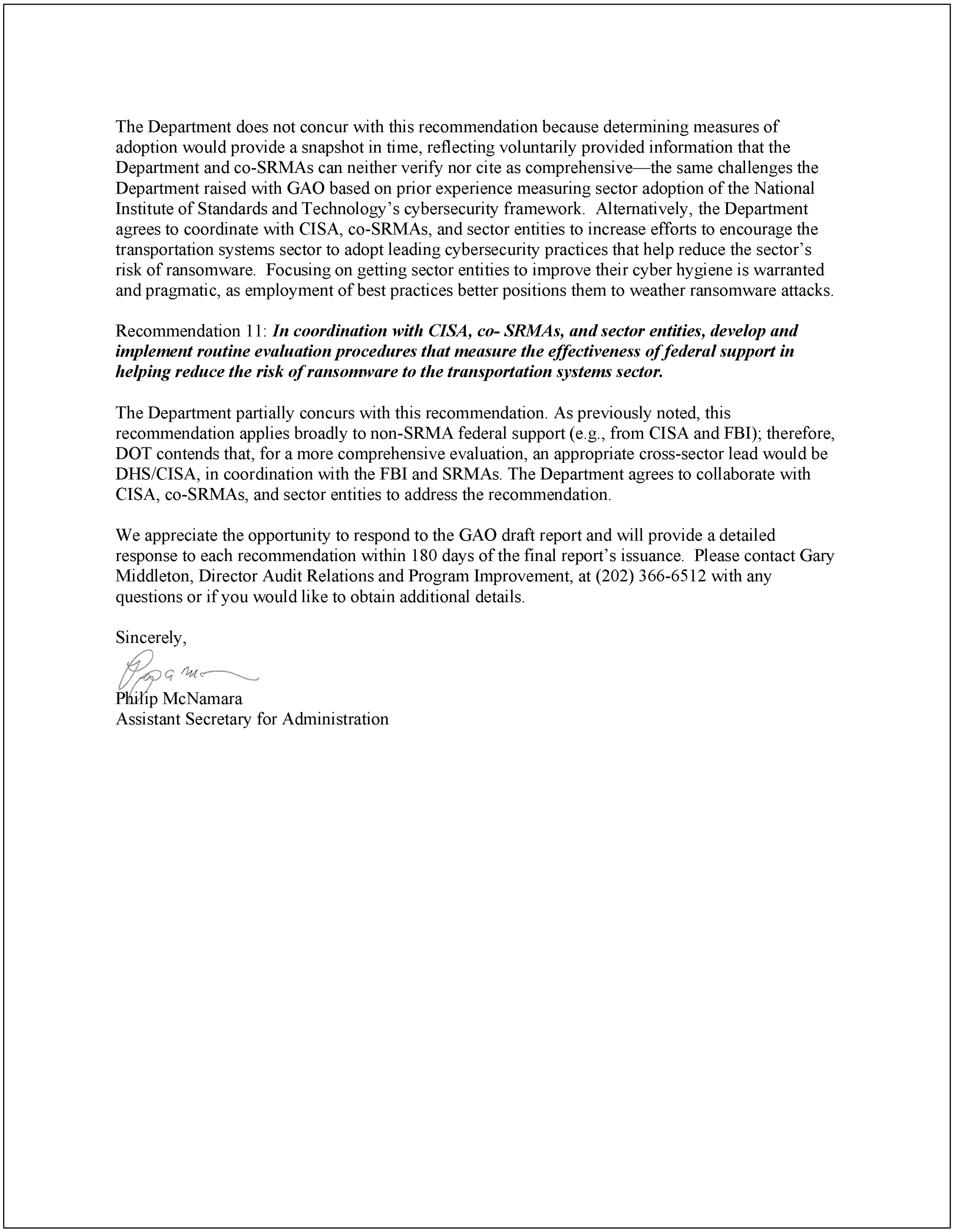
In reviewing the GAO draft report, a significant concern related to a recommendation issued to the Department is that GAO only selected 4 sectors to evaluate federal agency efforts related to ransomware risks and did not make broad recommendations for all critical infrastructure sectors. The report recognizes the essential services that the Nation's 16 critical infrastructure sectors provide and acknowledges the significant national security challenge that ransomware poses to critical infrastructure broadly. However, the report also cites that the Federal Bureau of Investigation (FBI) reported organizations that were victims of ransomware in 2022 affected 14 of the 16 sectors.

Upon review of GAO's draft report, the Department concurs with recommendation 9, does not concur with recommendation 10, and partially concurs with recommendation 11. The Department proposes alternate actions to implement recommendations 10 and 11.

Recommendation 9: ***In coordination with Cybersecurity and Infrastructure Security Agency (CISA), co- Sector Risk Management Agencies (co-SRMA), and sector entities, assess ransomware risks to the transportation systems sector.***

The Department concurs with this recommendation. As the report explains, DOT's co-SRMA partners within the Department of Homeland Security (DHS) / Transportation Security Administration and U.S. Coast Guard have already made efforts on behalf of the sector to assess ransomware risks, which is why GAO did not give DHS the same recommendation. Although DOT did not participate directly in these efforts, we agree to coordinate with the co-SRMA partners going forward and ensure we are not duplicating existing efforts.

Recommendation 10: ***In coordination with CISA, co- SRMAs, and sector entities, determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.***



The Department does not concur with this recommendation because determining measures of adoption would provide a snapshot in time, reflecting voluntarily provided information that the Department and co-SRMAs can neither verify nor cite as comprehensive—the same challenges the Department raised with GAO based on prior experience measuring sector adoption of the National Institute of Standards and Technology's cybersecurity framework. Alternatively, the Department agrees to coordinate with CISA, co-SRMAs, and sector entities to increase efforts to encourage the transportation systems sector to adopt leading cybersecurity practices that help reduce the sector's risk of ransomware. Focusing on getting sector entities to improve their cyber hygiene is warranted and pragmatic, as employment of best practices better positions them to weather ransomware attacks.

Recommendation 11: ***In coordination with CISA, co- SRMAs, and sector entities, develop and implement routine evaluation procedures that measure the effectiveness of federal support in helping reduce the risk of ransomware to the transportation systems sector.***

The Department partially concurs with this recommendation. As previously noted, this recommendation applies broadly to non-SRMA federal support (e.g., from CISA and FBI); therefore, DOT contends that, for a more comprehensive evaluation, an appropriate cross-sector lead would be DHS/CISA, in coordination with the FBI and SRMAs. The Department agrees to collaborate with CISA, co-SRMAs, and sector entities to address the recommendation.

We appreciate the opportunity to respond to the GAO draft report and will provide a detailed response to each recommendation within 180 days of the final report's issuance. Please contact Gary Middleton, Director Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if you would like to obtain additional details.

Sincerely,

Philip McNamara
Assistant Secretary for Administration

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at (214) 777-5719, hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Josh Leiling (Assistant Director), Torrey Hardee (Analyst-in-Charge), Joseph Andrews, Rebecca Eyler, Michele Fejfar, Nate Haggar, Franklin Jackson, and Tommy Luong made significant 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.