



February 2023

CRITICAL INFRASTRUCTURE PROTECTION

Time Frames to
Complete DHS Efforts
Would Help Sector
Risk Management
Agencies Implement
Statutory
Responsibilities

GAO Highlights

Highlights of [GAO-23-105806](#), a report to congressional committees

Why GAO Did This Study

Critical infrastructure provides essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Disruption or destruction of the nation's critical infrastructure could have debilitating effects. CISA is the national coordinator for infrastructure protection.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to report on the effectiveness of sector risk management agencies in carrying out responsibilities set forth in the act. This report addresses (1) how the act changed agencies' responsibilities, and the actions agencies have reported taking to address them; and (2) the extent to which CISA has identified and undertaken efforts to help agencies implement their responsibilities set forth in the act.

GAO analyzed the act and relevant policy directives, collected written responses from all 16 sectors using a standardized information collection tool, reviewed other DHS documents, and interviewed CISA officials.

What GAO Recommends

The Director of CISA should establish milestones and timelines to complete its efforts to help sector risk management agencies carry out their responsibilities. DHS concurred with the recommendation. Additionally, GAO has made over 80 recommendations which, when fully implemented, could help agencies address their statutory responsibilities.

View [GAO-23-105806](#). For more information, contact Tina Won Sherman at (202) 512-8461 or ShermanT@gao.gov.

February 2023

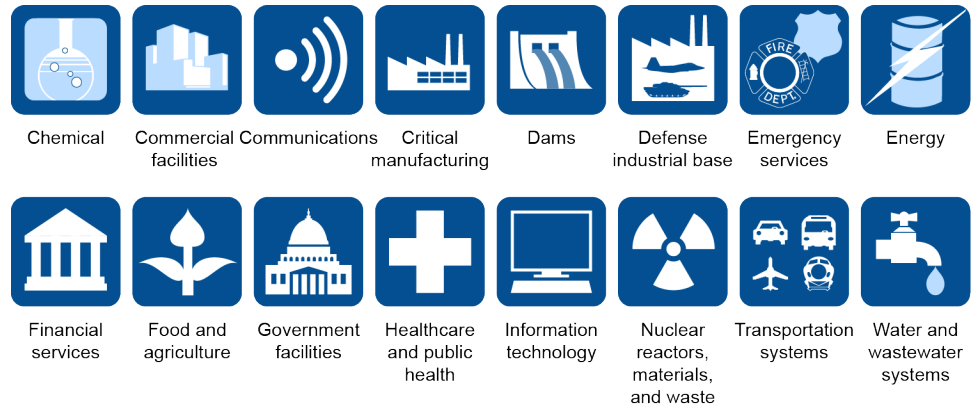
CRITICAL INFRASTRUCTURE PROTECTION

Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities

What GAO Found

GAO found that the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 expanded and added responsibilities for sector risk management agencies. These agencies engage with their public and private sector partners to promote security and resilience within their designated critical infrastructure sectors. Some officials from these agencies described new activities to address the responsibilities set forth in the act, and many reported having already conducted related activities. For example, the act added risk assessment and emergency preparedness as responsibilities not previously included in a key directive for sector risk management agencies. New activities officials described to address these responsibilities included developing a risk analysis capability and updating emergency preparedness products.

The 16 Critical Infrastructure Sectors



Source: GAO analysis of Presidential Policy Directive-21. | [GAO-23-105806](#)

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has identified and undertaken efforts to help sector risk management agencies implement their statutory responsibilities. For example, CISA officials stated they are updating key guidance documents, including the 2013 National Infrastructure Protection Plan and templates for revising sector-specific guidance documents. CISA officials also described efforts underway to improve coordination with sector partners, such as reconvening a leadership council. Sector risk management agency officials for a majority of critical infrastructure sectors reported that additional guidance and improved coordination from CISA would help them implement their statutory responsibilities. However, CISA has not developed milestones and timelines to complete its efforts. Establishing milestones and timelines would help ensure CISA does so in a timely manner.

Contents

Letter		1
	Background	5
	FY21 NDAA Expanded SRMA Responsibilities, and Agencies Have Actions Underway to Address Them	13
	CISA Has Identified and Undertaken Efforts to Help SRMAs, but Does Not Have Milestones and Timelines to Complete Them	24
	Conclusions	30
	Recommendation for Executive Action	31
	Agency Comments	31
Appendix I	Additional Information on the Challenges Sector Risk Management Agencies Reported	33
Appendix II	GAO Recommendations That Could Help Agencies Address FY21 NDAA	37
Appendix III	Comments from the Department of Homeland Security	50
Appendix IV	Comments from the Department of the Treasury	53
Appendix V	GAO Contact and Staff Acknowledgments	55
Tables		
	Table 1: Examples of Risk Components for Critical Infrastructure	8
	Table 2: Expansion and Addition of Sector Risk Management Agency Responsibilities, from Presidential Policy Directive-21 to the National Defense Authorization Act for Fiscal Year 2021	14
	Table 3: Recommendations from GAO Reports Not Yet Implemented Addressing Risk	38
	Table 4: Recommendations from GAO Reports Not Yet Implemented Addressing Coordination	44

Table 5: Recommendations from GAO Reports Not Yet Implemented Addressing Emergency Preparedness and Response	48
--------------------------------------------------------------------------------------------------------------	----

Figures

Figure 1: Timeline of Selected Critical Infrastructure Policy and Guidance	6
Figure 2: The 16 Critical Infrastructure Sectors and Their Respective Sector Risk Management Agencies	10
Figure 3: Cybersecurity and Infrastructure Security Agency (CISA) Selected Divisions and Responsibilities	12
Figure 4: Examples of Actions Sector Risk Management Agencies Reported Taking to Address Expanded Statutory Responsibilities	16
Figure 5: Examples of New Actions Sector Risk Management Agencies Reported Taking to Address Added Risk Assessment Statutory Responsibilities	18
Figure 6: Examples of New Actions Sector Risk Management Agencies Reported Taking to Address Added Emergency Preparedness Statutory Responsibilities	19
Figure 7: Sector Risk Management Agency Officials' Views about Private Sector Voluntary Participation, by Sector	21
Figure 8: Sector Risk Management Agency (SRMA) Officials' Views about Dedicated Resources, by Sector	23
Figure 9: Examples of Sector Risk Management Agency Officials' Views on Requests for Dedicated Resources, by Sector	35

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CISA Act of 2018	Cybersecurity and Infrastructure Security Agency Act of 2018
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EPA	Environmental Protection Agency
FPS	Federal Protective Service
FY21 NDAA	William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021
GSA	General Services Administration
HHS	Department of Health and Human Services
National Plan	National Infrastructure Protection Plan
PPD-21	Presidential Policy Directive-21
SRMA	sector risk management agency
Treasury	Department of the Treasury
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture

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



February 7, 2023

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

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

Events in 2021 demonstrated how disruption or destruction of the nation's critical infrastructure could have debilitating effects. In particular, the cyberattack on the Colonial Pipeline disrupted the nation's largest fuel pipeline, and the extreme weather event in Texas caused widespread power and water outages.¹ Such events also illustrate how the nation's critical infrastructure assets and systems are often interconnected with other systems and the internet, making them more vulnerable to attack. Protecting critical infrastructure is a national security priority because it provides essential functions—such as supplying water, generating energy, and producing food—that underpin American society.

The Cybersecurity and Infrastructure Security Agency Act of 2018 assigned the Cybersecurity and Infrastructure Security Agency (CISA) the responsibility to coordinate a national effort to secure and protect against critical infrastructure risks.² As such, the Secretary of Homeland Security designated the Director of CISA as the national coordinator for critical infrastructure security and resilience. CISA provides a variety of cyber

¹In May 2021, we issued a WatchBlog post addressing the Colonial Pipeline attack and the federal government and private sector response. See <https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic>.

²Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a)(1), 132 Stat. 4168, 4169 (codified at 6 U.S.C. § 652). The act renamed the Department of Homeland Security's National Protection and Programs Directorate as CISA and outlined CISA's responsibilities.

and infrastructure security capabilities and services to federal and non-federal organizations, including assessments and analysis, capacity building, expertise and guidance, and security operations (e.g., incident response).

At the federal level, sector risk management agencies (SRMAs) are departments or agencies, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector. They are also responsible for leading, facilitating, or supporting the security and resilience programs and associated activities within their designated critical infrastructure sector.³ The private sector owns and operates the majority of critical infrastructure. Therefore, it is vital that the public and private sectors work together to protect assets and systems.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) outlined responsibilities for SRMAs, including those related to supporting risk management, information sharing, and incident response.⁴ The act also includes a provision for us to review the effectiveness of SRMAs in carrying out these responsibilities.⁵ This report addresses:

1. how the FY21 NDAA changed sector risk management agency responsibilities, and the actions these agencies reported taking to address them; and

³6 U.S.C. § 651(5). Presidential Policy Directive-21 (PPD-21) previously called these agencies Sector-Specific Agencies. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified Sector-Specific Agencies as SRMAs. In 2013, PPD-21 categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as SRMA for the sector, although the number of sectors and SRMA assignments are subject to review and modification. Those designations are still in effect. See 6 U.S.C. § 652a(b). Additionally, some sectors have subsectors, such as the Education subsector within the Government Facilities sector, with the Department of Education having a lead sector risk management role for the subsector.

⁴6 U.S.C. § 665d.

⁵6 U.S.C. § 652a(d). This report is the first of several that we will issue in response to a provision in the FY21 NDAA. Specifically, the provision is for us to report on the effectiveness of SRMAs in carrying out their responsibilities not later than 2 years after the date of enactment and every 4 years thereafter for 12 years.

-
2. the extent to which CISA has identified and undertaken efforts to help sector risk management agencies implement their responsibilities set forth in the FY21 NDAA.

To address the first objective, we analyzed Presidential Policy Directive-21 (PPD-21), which established SRMA responsibilities prior to the FY21 NDAA.⁶ We compared the responsibilities in the directive to those in the act to identify any changes. We chose to focus the analysis on PPD-21 because it was the most authoritative source of SRMA responsibilities until the enactment of the FY21 NDAA. Additionally, while SRMAs may have other responsibilities as part of their respective missions, PPD-21 is specific to agencies' sector critical infrastructure protection responsibilities. We did not compare the FY21 NDAA to the 2013 National Infrastructure Protection Plan (National Plan)—a key guidance document required to be updated by PPD-21—as the plan largely restated the SRMA responsibilities described in PPD-21.⁷

To address the second objective, we analyzed CISA documents, including the *FY 2021 National Defense Authorization Act Section 9002(b) Report*,⁸ the Federal Senior Leadership Council Charter, and the 2013 National Plan, to assess ways CISA helps SRMAs implement their responsibilities under the FY21 NDAA.⁹ We interviewed CISA officials about ongoing and planned efforts to help SRMAs implement the FY21 NDAA. We compared CISA's efforts against our *Key Questions to Assess Agency Reform Efforts*, which provides guidance regarding agency reform and reorganization efforts.¹⁰ In particular, the key questions related

⁶The White House, Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience (Washington, D.C.: Feb. 12, 2013). As of December 2022, this policy directive remained in effect.

⁷CISA now refers to the National Infrastructure Protection Plan as the National Plan. We use the current terminology throughout the report.

⁸The FY21 NDAA required the Secretary of Homeland Security to review the current framework for securing critical infrastructure and submit a report to appropriate congressional committees and the President that included recommendations related to sector risk management. 6 U.S.C. § 652a(b). In January 2023, CISA officials informed us that the President officially approved the recommendations in the 9002(b) report, and initiated the process to rewrite PPD-21.

⁹The Federal Senior Leadership Council is a cross-sector council for federal departments and agencies with responsibility in critical infrastructure security and resilience.

¹⁰GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, [GAO-18-427](#) (Washington, D.C.: June 13, 2018).

to the use of plans with milestones and timelines to track implementation progress were significant to this objective.

To address both objectives, we requested information from the nine SRMAs responsible for all 16 critical infrastructure sectors.¹¹ Specifically, we obtained written responses to a standard set of questions to ensure we captured consistent information across agencies. We obtained information on any steps they had taken to address the FY21 NDAA responsibilities. We also obtained their perspectives about any challenges they faced previously, or expected to face, in implementing their responsibilities. We obtained information regarding any support CISA has provided to SRMAs to implement their FY21 NDAA responsibilities, and whether CISA could do more. We also reviewed our prior work on critical infrastructure protection for additional context on challenges SRMAs face.

In analyzing the responses to our standard questions, we used critical infrastructure sectors as the unit of analysis given that each sector has unique industries, stakeholders, and standing councils to coordinate critical infrastructure protection activities. Responses to our questions came from components within departments and agencies with specific SRMA responsibilities, as well as from components that support those efforts.¹² We consolidated and analyzed information at the sector level, and for clarity and consistency, we reported specific responses at the SRMA department or agency level. Specifically, one GAO analyst categorized the responses, and a second GAO analyst reviewed the categorizations and indicated agreement or disagreement. The analysts discussed any disagreements regarding the categorizations and reached consensus. The analysts then tallied the number of responses in each category.

We conducted this performance audit from February 2022 to February 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

¹¹Specifically, we requested information from the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; the General Services Administration; and the Environmental Protection Agency.

¹²Although named as a representative for DHS in the Transportation Systems Sector-Specific Plan, the Coast Guard did not provide specific responses for the Transportation Systems sector. We did receive responses from DHS's Transportation Security Administration and the Department of Transportation for the sector.

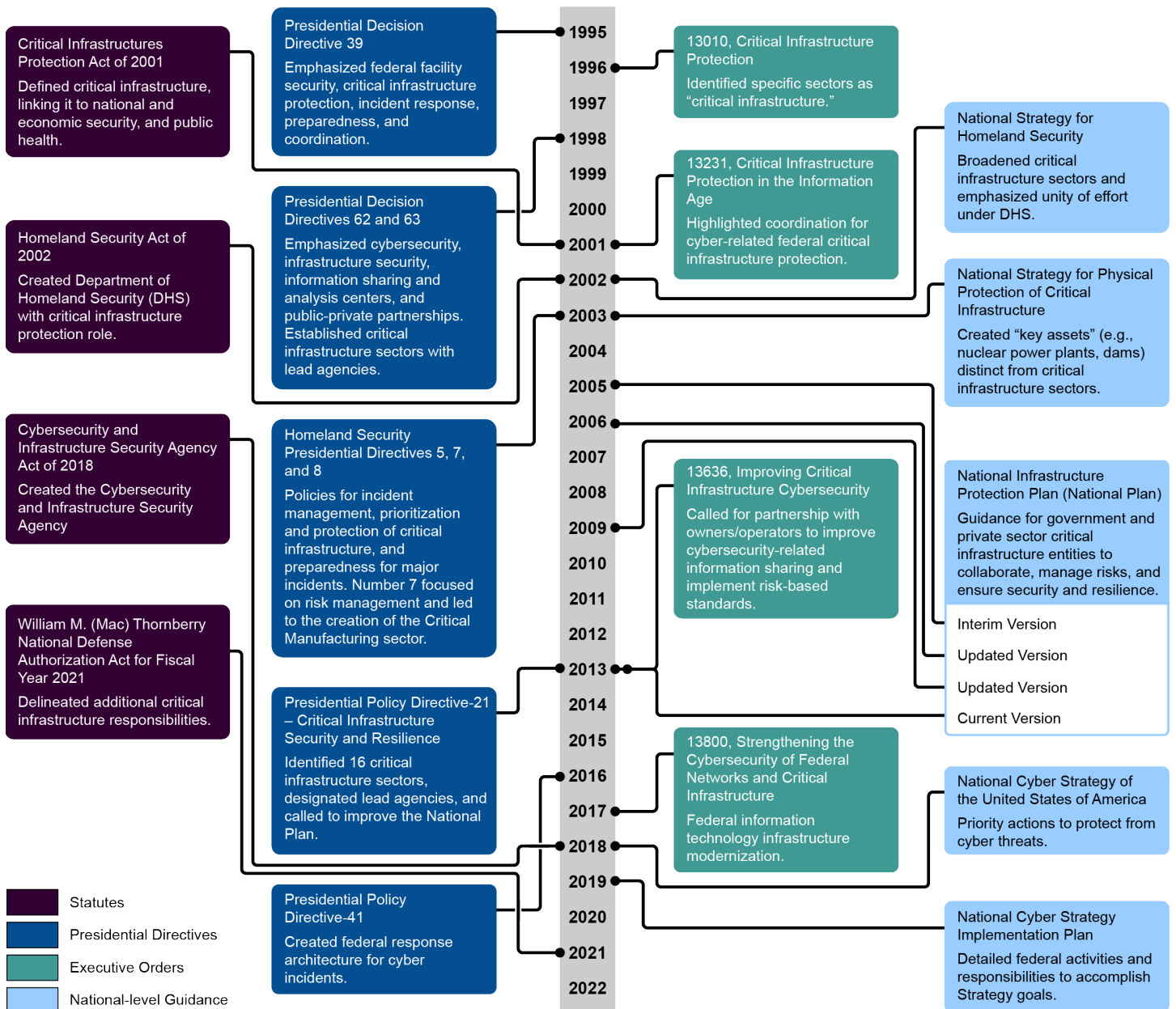
that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Critical Infrastructure Policies and Guidance

For over 25 years, a combination of laws, presidential directives and executive orders, and national-level guidance have guided critical infrastructure protection efforts (see fig. 1). Beginning in the mid-1990s, national policies began to reflect a need to enhance infrastructure protection and domestic preparedness against a range of deliberate, accidental, and naturally occurring threats. As the nation's assets and systems have faced evolving threats and challenges, such as the cybersecurity challenges of increasingly networked and internet-enabled infrastructure systems, policies and guidance have delineated new responsibilities.

Figure 1: Timeline of Selected Critical Infrastructure Policy and Guidance



Source: GAO analysis of statute, directives, and guidance. | GAO-23-105806

Two of the most widely recognized policy and guidance documents regarding critical infrastructure protection are PPD-21 and the 2013 National Plan. PPD-21 shifted the focus from protecting critical infrastructure against terrorism toward protecting and securing critical infrastructure and increasing its resilience against all hazards, including natural disasters, terrorism, and cyber incidents. It identified 16 critical infrastructure sectors and designated specific federal agencies—now referred to as SRMAs—and specified their roles and responsibilities.

The National Plan, required to be updated by PPD-21, provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.¹³ The National Plan details federal roles and responsibilities in protecting the nation's critical infrastructures and how sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. It emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments. The National Plan serves as a foundational document for critical infrastructure protection.

According to the National Plan, the risk environment for critical infrastructure continues to evolve. In particular, critical infrastructure assets, systems, and networks are facing more diverse, sophisticated threats—cyber, physical, technological, or natural—that may have cross-sector impacts. As part of its responsibilities, DHS is to conduct critical infrastructure risk assessments and integrate relevant information and analyses to identify priorities for protective measures. SRMAs also have responsibility for supporting sector risk management and assessing sector risk, which involves the analysis of threats, vulnerabilities, and consequences (see table 1).

¹³The Homeland Security Act of 2002, as amended, required DHS to develop a national plan for securing critical infrastructure, and PPD-21 directed DHS to update that national plan. See 6 U.S.C. § 652(e)(1)(E).

Table 1: Examples of Risk Components for Critical Infrastructure

Component of risk ^a	Examples
Threat	<ul style="list-style-type: none"> Natural hazards, such as extreme weather events with the potential to increase in frequency and severity due to climate change Deliberate acts, including physical or cyberattacks Insider threats from witting or unwitting employees Electromagnetic threats and hazards, which could occur naturally or be deliberate
Vulnerability	<ul style="list-style-type: none"> Physical asset or system weaknesses, such as accessibility, relative locations, visibility, or strength Technical weaknesses, such as susceptibility to cyberattack, energy surges, contamination, or eavesdropping Operational weaknesses, such as operator error or mechanical breakdowns.
Consequence	<ul style="list-style-type: none"> Economic, financial, environmental, health and safety, technological, or operational in nature Cascading effects across sectors, such as the loss of electric power can lead to problems in the supply of safe drinking water

Source: GAO analysis of DHS risk management guidance. | GAO-23-105806

^aRisk Management Fundamentals, Homeland Security Risk Management Doctrine (Washington, D.C.: April 2011); 2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience (Washington, D.C.: December 2013).

Sector Risk Management Agencies

SRMAs are federal departments or agencies, designated by law or presidential directive, with specific responsibilities for their designated critical infrastructure sectors.¹⁴ In coordination with CISA, SRMAs are to provide specialized expertise to critical infrastructure owners within the relevant sector and support programs and associated activities of their sector. In carrying out these activities, SRMAs are to coordinate with DHS and, as appropriate, other federal agencies; collaborate with critical infrastructure owners and operators within their sectors; and coordinate with state, local, tribal and territorial partners. As part of the partnership structure, each sector is to have a government coordinating council, consisting of representatives from various levels of government, and a sector coordinating council, consisting of owner-operators of critical assets and members of relevant trade associations.¹⁵ SRMA

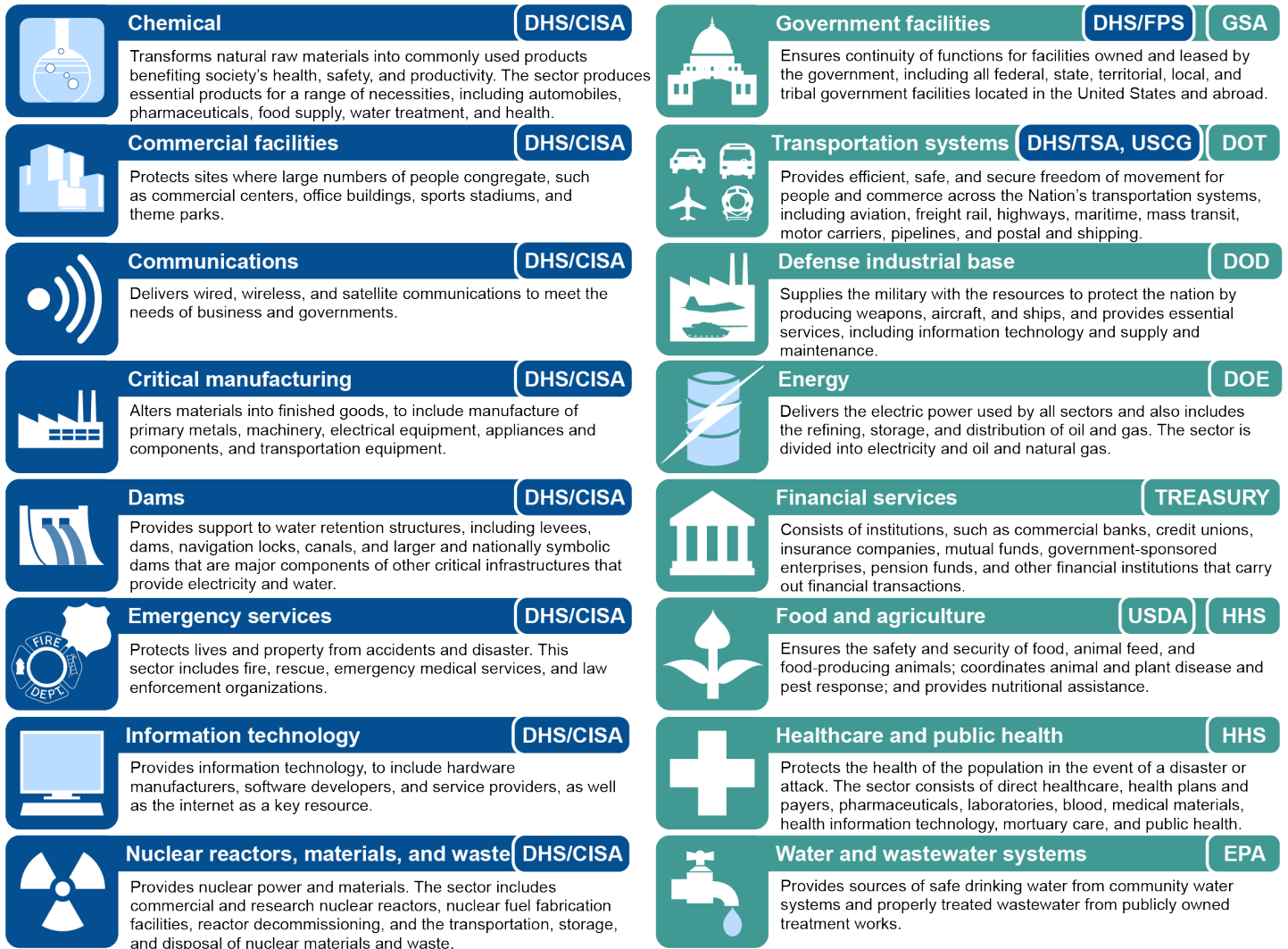
¹⁴ U.S.C. § 651(5). Although sector-specific plans identify specific departments, agencies, or components within departments or agencies as having lead or co-lead responsibilities for carrying out critical infrastructure protection activities, other offices within the SRMA departments and agencies also support sector critical infrastructure protection efforts.

¹⁵The National Plan describes the voluntary partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. The government facilities sector does not have a sector coordinating council, as it is government only.

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

The nation's critical infrastructure is currently categorized into 16 sectors with at least one federal agency designated as lead for the sector based on authorities and capabilities specific to that sector. As shown in figure 2, some sectors have co-lead agencies where more than one agency shares SRMA responsibilities. DHS is unique among the other SRMAs in that it has lead responsibility for eight of the 16 sectors, and co-leads two other sectors.

Figure 2: The 16 Critical Infrastructure Sectors and Their Respective Sector Risk Management Agencies



 Sectors managed by DHS
 Sectors not solely managed by DHS

Sector risk management agency
 Departments of Agriculture (USDA), Defense (DOD), Cybersecurity and Infrastructure Security Agency (CISA), Energy (DOE), Federal Protective Service (FPS), Health and Human Services (HHS), Homeland Security (DHS), Transportation (DOT), Transportation Security Administration (TSA), the Treasury; Environmental Protection Agency (EPA); United States Coast Guard (USCG); and the General Services Administration (GSA)

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013. | GAO-23-105806

CISA's National Coordinator Responsibilities

The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA as a component agency within DHS.¹⁶ As the national coordinator for critical infrastructure protection, the CISA Director is responsible for ensuring a unified approach to risk management that addresses the full spectrum of risks to critical infrastructure. The act assigned CISA specific responsibilities to focus on cybersecurity and critical infrastructure protection efforts.¹⁷ Key responsibilities include:

- securing federal information and information systems;
- coordinating a national effort to secure and protect against critical infrastructure risks;
- coordinating with federal and nonfederal entities, including international partners, to carry out its cybersecurity and critical infrastructure activities;
- responding to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance as needed; and
- carrying out emergency communications responsibilities under existing law.

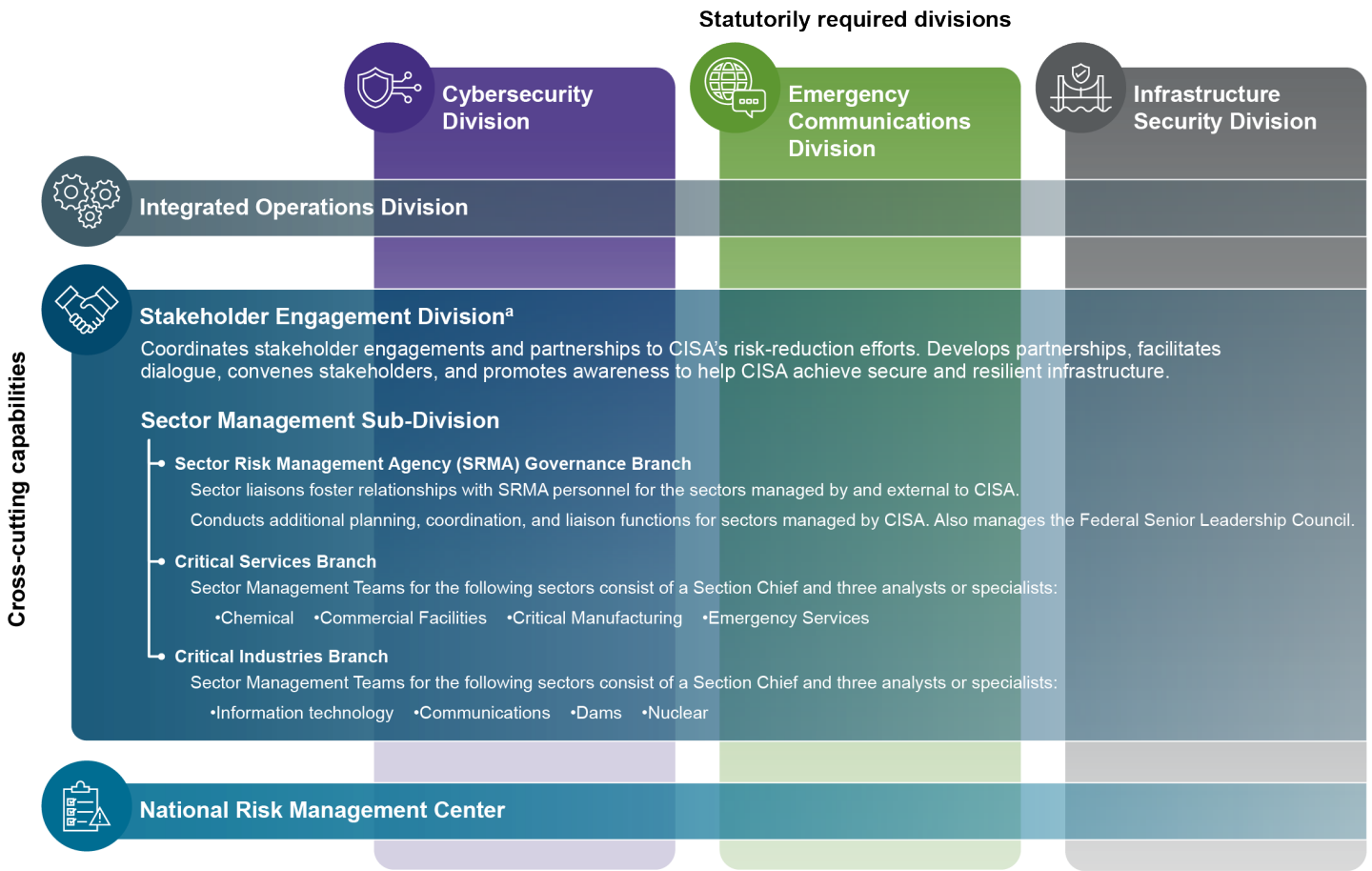
One of CISA's primary responsibilities is coordinating with other government and private sector partners. As the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts, CISA's ability to effectively coordinate and consult with its partners is key. Such partners include other federal agencies; state, local, territorial, and tribal governments; and the private sector. To help it carry out its mission, CISA developed an organizational structure that includes three statutorily defined divisions: Cybersecurity, Emergency Communications, and Infrastructure Security Divisions. CISA also has three divisions intended to provide cross-agency support and integration: Integrated Operations Division, Stakeholder Engagement Division, and the National Risk Management Center. The Stakeholder Engagement Division supports CISA-managed sectors, as well as the eight sectors managed by other agencies. Analysts and other specialists with sector

¹⁶U.S.C. § 652.

¹⁷As we reported in March 2021, since its establishment, CISA has reorganized offices and functions previously organized under the department's National Protection and Programs Directorate and aligned its new organizational structure with its mission. See, GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, [GAO-21-236](#) (Washington, D.C.: Mar. 10, 2021).

subject matter expertise conduct its primary functions of planning, coordination, and liaison activities (see fig. 3).

Figure 3: Cybersecurity and Infrastructure Security Agency (CISA) Selected Divisions and Responsibilities



Sources: Department of Homeland Security, CISA. | GAO-23-105806

^aThe Stakeholder Engagement Division also includes the Council Management, CISA International, and Strategic Relations subdivisions to support sector activities.

Additionally, CISA serves as the chair of the Federal Senior Leadership Council, which is a cross-sector council for federal departments and agencies with responsibility in critical infrastructure security and

resilience.¹⁸ The Federal Senior Leadership Council's primary activities include:

- coordinating implementation of SRMA responsibilities;
- reaching consensus on critical infrastructure risk management strategies;
- promoting implementation of risk-informed approaches;
- advancing collaboration within and across critical infrastructure sectors;
- supporting development of resource requirements to fulfill the federal mission; and
- evaluating and reporting on the progress of federal critical infrastructure security and resilience activities.

FY21 NDAA Expanded SRMA Responsibilities, and Agencies Have Actions Underway to Address Them

The FY21 NDAA Expanded and Added to SRMA Responsibilities

We found that the FY21 NDAA expanded SRMA responsibilities previously outlined in PPD-21 and added risk assessment and emergency preparedness as responsibilities not previously included in the directive for sector risk management agencies. Specifically, prior to the FY21 NDAA, PPD-21 included the following four SRMA responsibilities: (1) serve as a federal interface for the prioritization and coordination of sector-specific activities; (2) carry out incident management responsibilities; (3) provide, support, or facilitate technical assistance and consultations for sectors to support risk management activities; and (4) support the Secretary of Homeland Security by sharing information on sector-specific critical infrastructure. The FY21 NDAA expanded the sector coordination, incident management, risk management, and

¹⁸The National Plan established the Federal Senior Leadership Council as a principal cross-sector council.

information sharing responsibilities found in PPD-21 by adding specific activities for SRMAs to carry out within these areas.

In addition, we found that the FY21 NDAA added two responsibilities not explicitly outlined as SRMA responsibilities in PPD-21: risk assessment and emergency preparedness.¹⁹ Table 2 below provides more information on the responsibilities outlined in PPD-21 and those in the FY21 NDAA. The FY21 NDAA also provides that most SRMA responsibilities are to be carried out in coordination with the CISA Director.

Table 2: Expansion and Addition of Sector Risk Management Agency Responsibilities, from Presidential Policy Directive-21 to the National Defense Authorization Act for Fiscal Year 2021

Category of sector risk management agency (SRMA) responsibility	Responsibilities outlined in Presidential Policy Directive-21	Expanded responsibilities outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (<i>in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) Director</i>)
Sector coordination	Serve as day-to-day federal interface for the prioritization and coordination of sector-specific activities	<ul style="list-style-type: none"> • Conduct sector coordination activities, including: <ul style="list-style-type: none"> • serving as day-to-day federal interface for the prioritization and coordination of sector-specific activities; • serving as federal government coordinating council chair; and • participating in cross-sector coordinating councils, as appropriate
Incident management	Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations	<ul style="list-style-type: none"> • Conduct incident management activities, including: <ul style="list-style-type: none"> • supporting incident management and restoration efforts during or following a security incident; and • supporting CISA in national cybersecurity asset response activities for critical infrastructure

¹⁹CISA and the other SRMAs also have roles related to emergency preparedness efforts under the *National Preparedness Goal* and the *National Response Framework*. PPD-8 directed the Secretary of Homeland Security to develop a national preparedness goal, which defines the core capabilities necessary for emergency response to specific types of incidents. The national framework is a guide to how the nation responds to disasters and emergencies of all types. The most recent edition of the framework identifies 15 emergency support functions that serve as the federal government’s primary coordinating structure for building, sustaining, and delivering response capabilities. According to the framework, existing infrastructure plans and coordination mechanisms such as SRMAs and councils provide strong foundations for strengthening incident response plans and capabilities. As part of the National Plan, the critical infrastructure sectors and agencies have developed sector-specific plans. For more information, see Department of Homeland Security, *National Response Framework*, 4th ed. and GAO, *Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps [Reissued on December 9, 2015]*, GAO-15-20 (Washington, D.C.: Dec. 4, 2014).

Category of sector risk management agency (SRMA) responsibility	Responsibilities outlined in Presidential Policy Directive-21	Expanded responsibilities outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 <i>(in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) Director)</i>
Risk management	Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate	<ul style="list-style-type: none"> • Support sector risk management, including: <ul style="list-style-type: none"> • establishing and carrying out programs to assist critical infrastructure owners and operators within the sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector; and • recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets
Information sharing	Support the Secretary of Homeland Security's statutorily required reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information ^a	<ul style="list-style-type: none"> • Share information with the Department of Homeland Security (DHS) and other appropriate federal departments on physical security and cybersecurity threats within the sector, including: <ul style="list-style-type: none"> • facilitating access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure; • facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in coordination with the Director of National Intelligence and the heads of other federal departments and agencies; • providing to CISA and facilitating awareness in the sector of ongoing, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions; and • supporting the reporting requirements of DHS by annually providing sector-specific critical infrastructure information
Risk assessment	Not included as an SRMA responsibility ^b	<ul style="list-style-type: none"> • Assess sector risk, including: <ul style="list-style-type: none"> • identifying, assessing, and prioritizing sector risks, considering physical security and cybersecurity threats, vulnerabilities, and consequences; • supporting national risk assessment efforts led by DHS
Emergency preparedness	Not included as an SRMA responsibility	<ul style="list-style-type: none"> • Contribute to emergency preparedness efforts, including: <ul style="list-style-type: none"> • coordinating with CISA and critical infrastructure sector owners and operators in developing planning documents for coordinated action in the event of a natural disaster, act of terrorism, other man-made disaster or emergency;; • participating in, conducting, or facilitating sector exercises and simulations of natural disasters, acts of terrorism, other man-made disasters or emergencies; and; • supporting DHS and other Federal departments in developing sector planning documents or conducting exercises or simulations

Source: GAO analysis of Presidential Policy Directive-21 (PPD-21) and the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 6 U.S.C. § 665d. | GAO-23-105806





^aPPD-21 also requires the Secretary of Homeland Security, in coordination with SRMAs, to provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure.

^bPPD-21 requires the Secretary of Homeland Security to conduct comprehensive assessment of the vulnerabilities of critical infrastructure in coordination with the SRMAs.

Some SRMAs Have Actions Underway to Address Their Expanded Statutory Responsibilities

Some SRMAs have actions underway to address their expanded responsibilities under the FY21 NDAA. For example, SRMA officials for four of the 16 critical infrastructure sectors reported adapting activities related to sector coordination, incident management, risk management, or information sharing to address their responsibilities in the act (see fig. 4).²⁰

Figure 4: Examples of Actions Sector Risk Management Agencies Reported Taking to Address Expanded Statutory Responsibilities

Sector and sector risk management agency	Description of actions
 <p>Defense industrial base Department of Defense</p>	Reported efforts to improve information sharing and cybersecurity with the Sector Coordinating Council.
 <p>Financial services Department of the Treasury</p>	Reported starting an unclassified threats exchange forum and enhancing its incident management capabilities.
 <p>Healthcare and public health Department of Health and Human Services</p>	Reported coordinating an effort to analyze the department's existing cyber authorities to identify and mitigate any gaps, as well as developing a cyber-incident response plan.
 <p>Transportation systems Departments of Homeland Security and Transportation</p>	Reported that they plan to update their sector-specific plan and assess resource needs.

Source: GAO analysis of agency responses. | GAO-23-105806

Note: Agencies provided information on the actions they have taken to address the expanded responsibilities in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 related to sector coordination, incident management, technical assistance regarding risk management, and information sharing. See 6 U.S.C. § 665d.

Additionally, some SRMA officials also reported that activities they established prior to the enactment of the FY21 NDAA already address the responsibilities outlined in the act. For example, SRMA officials from the Department of Energy and the Environmental Protection Agency,

²⁰This included co-SRMAs in the transportation systems critical infrastructure sector. When co-SRMAs responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

representing the energy sector and water and wastewater systems sector respectively, reported that they address the responsibilities outlined in the FY21 NDAA. Finally, as the SRMA for eight of the 16 sectors, CISA described established activities that address sector coordination, incident management, risk management, and information sharing. Specifically, CISA officials reported that CISA's Stakeholder Engagement Division focuses on developing relationships with industry and government in CISA's sectors by meeting with Sector Coordinating Councils and issuing advisories and analysis reports to partners.

Some SRMAs Have Actions Underway to Address Added Statutory Responsibilities for Risk Assessment and Emergency Preparedness






In addition to taking action to address the expanded statutory responsibilities, SRMA officials also described actions underway to address the additional risk assessment and emergency preparedness responsibilities included in the FY21 NDAA.

Risk assessment. SRMA officials for five of the 16 critical infrastructure sectors described how they plan to take new actions to address the risk assessment responsibilities outlined in the FY21 NDAA (see fig. 5). Further, SRMA officials for 15 of the 16 critical infrastructure sectors also stated that they had conducted such activities prior to their inclusion in the FY21 NDAA.²¹ For example, CISA officials reported conducting a range of risk assessment activities, such as participating in risk assessments and working groups related to National Critical Functions.²²

²¹As the co-SRMAs in the government facilities sector, both DHS Federal Protective Service and General Services Administration officials did not describe conducting prior risk assessment activities. They stated that prior to the FY21 NDAA, non-CISA co-SRMAs were not required to conduct risk assessments for their sector and did not have the authority to require their federal and nonfederal partners to provide responses or submit information for such assessments.

²²CISA defines National Critical Functions as those functions of the government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Figure 5: Examples of New Actions Sector Risk Management Agencies Reported Taking to Address Added Risk Assessment Statutory Responsibilities

Sector and sector risk management agency	Description of actions
 <p>Communications Department of Homeland Security</p>	<p>Reported plans to develop and maintain a communications risk register that includes cybersecurity risks to emergency communications infrastructure.</p>
 <p>Defense industrial base Department of Defense</p>	<p>Reported plans to augment sector risk assessment activities and analytical capabilities, including a cybersecurity certification.</p>
 <p>Financial services Department of the Treasury</p>	<p>Reported creating a program to develop a risk analysis capability, including a formal methodology and risk reporting to various stakeholders.</p>
 <p>Healthcare and public health Department of Health and Human Services</p>	<p>Reported planning to further develop its risk analysis and management capabilities with key focuses on supply chain and cybersecurity.</p>
 <p>Transportation systems Departments of Homeland Security and Transportation</p>	<p>Reported a plan to adjust their risk assessment activities in accordance with any new guidance, revise the Sector-Specific Plan, and consider revisions to risk assessment roles and processes.</p>







Source: GAO analysis of agency responses. | GAO-23-105806

Note: Agencies provided information on the actions they have taken to address the risk assessment responsibilities in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. See 6 U.S.C. § 665d.

Emergency preparedness. SRMA officials for six of the 16 critical infrastructure sectors described how they plan to take new actions to address the emergency preparedness responsibilities outlined in the FY21 NDAA (see fig. 6). Further, SRMA officials for all 16 critical infrastructure sectors also stated that they had conducted emergency preparedness activities prior to their inclusion in the FY21 NDAA. For example, as the SRMA for the healthcare and public health sector, Department of Health and Human Services officials said they developed all-hazards response playbooks to improve coordination between government and private sector partners. SRMA officials for the financial

services and energy sectors also noted their existing exercise programs to address emergency preparedness responsibilities.²³

Figure 6: Examples of New Actions Sector Risk Management Agencies Reported Taking to Address Added Emergency Preparedness Statutory Responsibilities

Sector and sector risk management agency	Description of actions
 <p>Critical manufacturing Department of Homeland Security</p>	<p>Reported that it will update existing emergency preparedness products and tools in collaboration with sector partners, such as the Sector Playbook.</p>
 <p>Dams Department of Homeland Security</p>	<p>Reported that it will host future information sharing drills, and update emergency preparedness products and tools in collaboration with sector partners.</p>
 <p>Emergency services Department of Homeland Security</p>	<p>Reported that it will update existing emergency preparedness tools, resources, and products in collaboration with sector partners.</p>
 <p>Financial services Department of the Treasury</p>	<p>Reported enhancing a tabletop exercise program, developing a functional exercise platform to improve cybersecurity exercises, and refining incident management and crisis communication toolkits.</p>
 <p>Healthcare and public health Department of Health and Human Services</p>	<p>Reported plans to improve risk analysis and management capabilities, planning for emerging threats, and strategic planning with sector partners.</p>
 <p>Transportation systems Departments of Homeland Security and Transportation</p>	<p>Reported plans to finalize and conduct annual updates to the Transportation Systems Sector Playbook.</p>

Source: GAO analysis of agency responses. | GAO-23-105806

Note: Agencies provided information on the actions they have taken to address the emergency preparedness responsibilities in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. See 6 U.S.C. § 665d.

²³As the SRMA for the financial services sector, Department of the Treasury officials stated that their exercise program studies plausible security incidents to identify incident response gaps and better prepare private and public response efforts. Similarly, as the SRMA for the energy sector, Department of Energy officials stated that the Office of Cybersecurity, Energy Security, and Emergency Response within the department hosts exercises with industry, interagency, and state partners focused on cyber, physical, and natural hazard preparedness.

SRMAs Reported Challenges in Implementing Their Responsibilities

SRMA officials cited two challenges in implementing their responsibilities: (1) the voluntary nature of private sector participation in SRMA activities and (2) limited or no dedicated resources for SRMA duties.²⁴ According to SRMA officials, these challenges pre-dated the enactment of the FY21 NDAA.

Voluntary participation. Participation in SRMA critical infrastructure protection efforts is voluntary, which SRMA officials for 11 critical infrastructure sectors reported as a challenge to conducting their responsibilities.²⁵ For example, they reported that this affected their ability to stay apprised of issues in the sector and to collect information. SRMA officials reported that these challenges existed prior to the FY21 NDAA and they generally expected them to continue.²⁶ See figure 7 below for agency officials' reported views about voluntary program participation and appendix I for additional information.

²⁴Additional challenges SRMA officials identified included coordination issues related to inaccurate SRMA point-of-contact lists and government coordinating council and sector coordinating council membership lists, and limited technical cybersecurity expertise. Our past work describing other DHS functions has highlighted the importance of maintaining accurate and up-to-date contact information for the sharing of information. See, GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, [GAO-17-163](#) (Washington, D.C.: Feb. 1, 2017). SRMA officials said they expected CISA to possibly address this challenge if it established consistent communication mechanisms in response to the FY21 NDAA. According to CISA officials, CISA has efforts underway to address issues related to inaccurate points of contact lists.

²⁵Some agencies that serve as SRMAs have a separate regulatory relationship with their sectors and in that role are able to require private sector owner-operators to provide certain types of information. Nevertheless, even for the sectors with regulatory agencies, participation in SRMA critical infrastructure protection activities and provision of information for such activities is voluntary.

²⁶When co-SRMAs responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

Figure 7: Sector Risk Management Agency Officials' Views about Private Sector Voluntary Participation, by Sector



Sector risk management agency

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

Source: GAO analysis of agency responses. | GAO-23-105806

Note: When co-sector risk management agencies (SRMAs) responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include that sector in the total count and noted the disagreement, as is the case with the government facilities sector in the figure above.

^aThe William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA). See 6 U.S.C. § 665d.

For over two decades, we have reported on the voluntary nature of critical infrastructure protection efforts and the inherent challenges it poses for

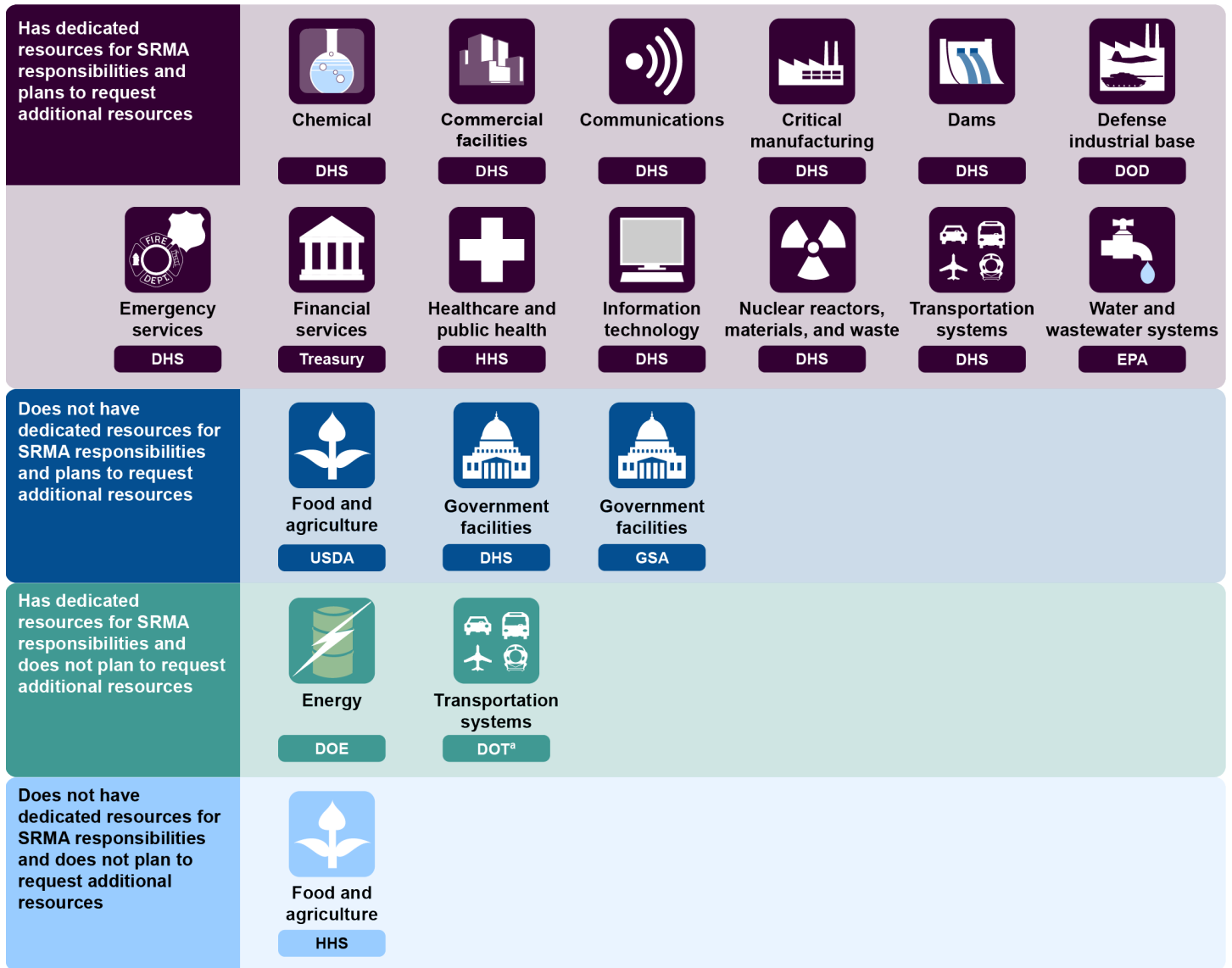
information sharing and measuring effectiveness.²⁷ For example, to help facilitate sector coordination and information sharing about physical and cybersecurity threats, we recommended in February 2018 that the departments of Agriculture, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury take steps to consult with their respective sector partners to develop methods for determining the effectiveness of cybersecurity efforts in their sectors. As of December 2022, the departments had not fully implemented these recommendations. Addressing these recommendations would present an opportunity to support SRMAs' responsibilities under the FY21 NDAA by facilitating awareness and understanding of the security-related actions within their sectors, which has been challenging to assess as a result of the voluntary nature of information sharing activities. In the absence of this information sharing, SRMAs will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation. Appendix II provides additional information about these and other recommendations aimed at addressing critical infrastructure protection challenges.

Dedicated resources. SRMA officials also stated that they face challenges because they have limited or no dedicated resources to implement their responsibilities. SRMA officials for 13 of the 16 sectors, including those with and without dedicated resources for SRMA activities, stated that they planned to request additional resources to help them implement their FY21 NDAA responsibilities (see fig. 8).²⁸

²⁷Selected products which highlight the inherent challenge of voluntary participation include: GAO, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, [GAO-01-323](#) (Washington, D.C.: Apr. 25, 2001); GAO, *Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed*, [GAO-02-918T](#) (Washington, D.C.: July 9, 2002); GAO, *Critical Infrastructure Protection: Additional Actions Are Essential For Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: Feb. 15, 2018); GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, [GAO-20-299](#) (Washington, D.C.: Feb. 25, 2020); and GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, [GAO-22-105103](#) (Washington, D.C.: Feb. 9, 2022).

²⁸In our request for information, we asked if agencies had dedicated staff and budget for SRMA activities. For the purposes of this report, we use the term resources to describe both. When the co-SRMAs responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

Figure 8: Sector Risk Management Agency (SRMA) Officials' Views about Dedicated Resources, by Sector



Sector risk management agency

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

Source: GAO analysis of agency responses. | GAO-23-105806

Note: When co-sector risk management agencies (SRMAs) responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

^aDOT officials stated that they do not currently have plans to include formal requests for dedicated staffing and budget. They have not yet made a determination, which they said may change pending the full implementation of SRMA responsibilities under the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. See 6 U.S.C. § 665d.

In particular, SRMA officials for six critical infrastructure sectors reported challenges related to dedicated resources prior to the FY21 NDAA, and stated that they generally expect them to continue. For example, SRMA officials stated that a lack of dedicated funding to support SRMA activities makes such activities a collateral duty. CISA has proposed leading an effort through the Federal Senior Leadership Council to develop standardized SRMA budget guidance on developing resource requests, as we discuss later in this report.

CISA Has Identified and Undertaken Efforts to Help SRMAs, but Does Not Have Milestones and Timelines to Complete Them

CISA has identified and undertaken some efforts that could help SRMAs implement their FY21 NDAA responsibilities. In November 2021, CISA reported on several ongoing and planned efforts to help SRMAs implement these responsibilities and to clarify federal roles and responsibilities for cybersecurity and infrastructure security actions across the federal government.²⁹ However, as of October 2022, CISA had not developed milestones and timelines to complete its efforts.

CISA Has Identified and Begun Efforts to Provide Additional Guidance to SRMAs

CISA has identified and undertaken some efforts to provide additional guidance to SRMAs, but SRMA officials for 10 sectors told us they are waiting to implement some of their FY21 NDAA responsibilities until CISA finalizes and distributes updated guidance.³⁰ For example, as a co-SRMA for the transportation sector, Department of Transportation officials stated that they will develop an approach to implementing their responsibilities

²⁹In response to the FY21 NDAA, CISA reviewed the framework for securing critical infrastructure and submitted a report to the President and congressional committees that made recommendations. According to CISA officials, they met with and collected feedback from SRMAs while preparing this report. According to CISA officials in January 2023, the President officially approved the recommendations in the 9002(b) report, and initiated the process to rewrite PPD-21. CISA, *FY 2021 National Defense Authorization Act: Section 9002(b) Report*, (Nov. 12, 2021).

³⁰Most SRMAs reported receiving routine guidance from CISA for ongoing activities.

under the FY21 NDAA when CISA provides overarching guidance to agencies.³¹

Update the 2013 National Plan and sector-specific plans. CISA officials told us the updated National Plan will clarify SRMA responsibilities in response to the FY21 NDAA. The National Plan provides the overarching national approach for critical infrastructure protection, and CISA officials stated that it will be the “cornerstone” to guide SRMAs as they implement their responsibilities. According to CISA officials, the updated National Plan will: 1) include a revised approach to critical infrastructure protection, 2) provide information on SRMA responsibilities set forth in the FY21 NDAA, 3) clarify federal roles and responsibilities for sector risk management, and 4) outline how government and industry should coordinate to identify and mitigate threats to critical infrastructure. However, as of October 2022, CISA officials told us they did not have a timeline for issuing the updated National Plan until the administration completes a review of PPD-21. The 2013 update of the National Plan responded to new policy in PPD-21, including an explicit provision that DHS update the National Plan to implement the new directive. CISA officials told us they would not make further updates to the National Plan until the review of PPD-21 is completed.

Further, CISA officials stated in October 2022 they plan to provide additional guidance to SRMAs on how they should update their sector-specific plans. CISA officials told us that the updated sector-specific plans should describe how the sector will implement the updated National Plan, along with efforts tailored to the sector’s unique characteristics. CISA officials told us they expected to issue an updated sector-specific plan template 3 to 6 months after the release of the updated National Plan for SRMAs to use in collaboration with their sector partners. Further, they told us that the sector-specific plans would likely take 1 year to develop.

Our prior work discusses the importance of updating sector-specific plans in multiple sectors, including the communications, financial services, and government facilities sectors, to address new and emerging threats to critical infrastructure, and in the case of the communications sector, to

³¹According to CISA officials, CISA conducted facilitated discussions and solicited SRMA input on the draft report required of them in the FY21 NDAA. The report identifies steps needed to implement the law’s requirements. However, CISA is still in the midst of updating guidance on FY21 NDAA implementation.

address the responsibilities outlined in the FY21 NDAA.³² In particular, we recommended that CISA work with stakeholders to update the sector-specific plans for the communications sector and of the education subsector within the government facilities sector, and recommended the Department of the Treasury update the financial sector-specific plan (see appendix II). As of December 2022, these recommendations had not been implemented, and we believe taking such actions would better position SRMAs to manage risk in their sectors.

Define maturity and effectiveness metrics. CISA officials told us in October 2022 they expect to develop a methodology and metrics to measure the maturity and effectiveness of SRMAs in implementing responsibilities outlined in the FY21 NDAA. For example, in its November 2021 report, CISA recommended that the Federal Senior Leadership Council conduct a sector-by-sector assessment of SRMA partnership participation.³³ CISA officials told us these efforts could include both standardized metrics to measure effectiveness across all sectors, and sector-specific metrics.

Of the 16 critical infrastructure sectors, only Environmental Protection Agency officials, as SRMA for the waste and wastewater systems, stated that they track and assess the effectiveness of their efforts. However, SRMA officials from nine of the sectors that do not formally track their own effectiveness reported that they collect stakeholder feedback to some degree. We have previously reported that CISA should assess the effectiveness of critical infrastructure programs and services to support the communications sector, including developing and implementing metrics. This type of assessment could help SRMAs and CISA determine which efforts are most useful or relevant in supporting critical

³²GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, [GAO-22-104462](#), (Washington, D.C.: Nov. 23, 2021); GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, [GAO-20-631](#) (Washington, D.C. Sept. 17, 2020); and 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.)

³³CISA, *FY 2021 National Defense Authorization Act: Section 9002(b) Report*, (Nov. 12, 2021).

infrastructure security and resilience.³⁴ CISA's proposal to develop a methodology to develop standard and sector-specific metrics provides an opportunity to help CISA and the other SRMAs in implementing their FY21 NDAA responsibilities by allowing them to monitor progress. According to CISA officials, the updated National Plan and sector-specific plans will outline these metrics to help evaluate SRMA preparedness and effectiveness; however, as noted above, CISA does not have a timeline for issuing the updated National Plan.

Develop standardized budget guidance. In its November 2021 report, CISA officials identified a need to develop a baseline cost estimation tool for SRMAs.³⁵ According to the report, this tool would provide SRMAs a baseline estimate of resource needs, and could be tailored to each SRMA. CISA also proposed implementing a consistent resource request process across the SRMAs, which could help address the challenges associated with their resource limitations, as previously discussed. According to CISA officials, this budget formulation tool would allow SRMAs to request sufficient resources to implement their FY21 NDAA responsibilities. For example, as co-SRMA for the food and agriculture sector, Food and Drug Administration officials within the Department of Health and Human Services stated that CISA could provide budgetary guidance to determine the recommended number of employees needed to fulfill their FY21 NDAA responsibilities. However, as of October 2022, CISA officials did not provide a timeline for when they planned to develop or disseminate this guidance.

CISA Has Identified and Started Efforts to Improve Coordination and Information Sharing with SRMAs

CISA officials told us they have two efforts underway to improve coordination and information sharing with SRMAs, and they have identified another which is still in development. SRMA officials for 11 of the 16 critical infrastructure sectors stated that CISA could improve its support of SRMAs, including coordination and information sharing with them. For example, as co-SRMAs for the government facilities sector, officials from DHS Federal Protective Service and the General Services Administration told us that CISA should provide information and guidance in a timely manner. As the SRMA for the energy sector, officials from the Department of Energy also highlighted the importance of ensuring clarity

³⁴GAO 22-104462. For example, we recommended that CISA assess the effectiveness of its support to the communications sector, including developing and implementing metrics. As of December 2022, this recommendation had not been implemented.

³⁵CISA, *FY 2021 National Defense Authorization Act: Section 9002(b) Report*, (Nov. 12, 2021).

among the roles and responsibilities of each SRMA to avoid potential confusion among industry officials. They said this is particularly important in the context of how interconnected some sectors are to others, such as the energy sector.

Create sector liaison positions. In August 2022, CISA officials told us they created liaison positions focused on fostering CISA’s relationship with SRMAs. According to CISA officials, these liaisons will help CISA respond to the responsibilities outlined in the FY21 NDAA by enhancing communication and coordination with SRMAs, triage information in response to incidents, and respond to requests for information. As of October 2022, CISA officials stated that the agency was in the process of staffing these liaison positions.

Enhance the Federal Senior Leadership Council. The Federal Senior Leadership Council provides a forum for coordination and communication among agencies with critical infrastructure responsibilities, including SRMAs. The council coordinates implementation of SRMA responsibilities as well as other initiatives related to protecting critical infrastructure. According to CISA officials, in recent years, the council has been relatively inactive and could be “reinvigorated” to exhibit sufficient collaboration and coordination to support implementation of the FY21 NDAA responsibilities.³⁶ To support these efforts, CISA officials told us the council would need to: (1) meet more frequently, (2) use multiple working groups to accomplish its new responsibilities—such as serving as a governance body for SRMAs, (3) address cross-sector issues, and (4) evaluate the list of critical infrastructure sectors.

The Federal Senior Leadership Council met in November 2022 to discuss a revised council charter, and according to CISA officials, the body will support the implementation of SRMA responsibilities outlined in the FY21 NDAA. According to CISA officials, the Federal Senior Leadership Council is intended to be one of the primary ways CISA will coordinate actions to implement the FY21 NDAA across the federal government. For example, CISA proposed that the council develop the standardized SRMA budget guidance described above. We have previously reported on the importance of centralized information sharing and coordination to

³⁶According to CISA officials, CISA also has a long-standing monthly SRMA coordination conference call to engage SRMAs.

enhancing protection of critical infrastructure.³⁷ CISA officials told us they are aware that SRMAs are generally waiting for CISA to establish collaboration and coordination functions under the Federal Senior Leadership Council before taking action. According to a summary of the November 2022 meeting, the council will first turn its attention to address SRMAs' risk assessment responsibilities outlined in the FY21 NDAA by seeking to reach consensus on a common understanding of risk assessment across the sectors. However, the summary of the meeting did not identify any milestones or timelines for conducting this work.

Develop a standardized feedback process. CISA officials told us in June 2022 that they are developing a process to conduct standardized surveys of critical infrastructure stakeholders and plan to use the results to conduct assessments. They said surveys allow them to measure the outcome of sector efforts by collecting information from partners on their intent to take action based on the information, tools, or capabilities provided to them, which they said is important due to the voluntary nature of sector partnerships. CISA's plan to develop a standardized feedback process presents an opportunity to collect information from other SRMAs, as well as critical infrastructure owners and operators on the challenges they face. For example, they could collect information on challenges inherent in the voluntary nature of sector partnerships. However, as of October 2022, CISA officials did not provide a timeline on when they would implement this feedback process.

CISA Has Not Established Milestones and Timelines to Complete Its Efforts

Although CISA has identified and started a number of efforts to help SRMAs implement their FY21 NDAA responsibilities, CISA does not have milestones and timelines to complete its efforts. According to selected characteristics from GAO's *Key Questions to Assess Agency Reform Efforts*, government reform efforts should have milestones and timelines to track implementation progress, which can also provide transparency about the progress of reforms.³⁸

³⁷GAO 20-299. In this report, we found that SRMAs felt the lack of a centralized information sharing mechanism inhibited their ability to collect and report sector-wide efforts to adopt cybersecurity measures. However, we found such mechanisms existed and made recommendations encouraging their use. As described in appendix II, these recommendations remain yet to be implemented, and we continue to believe their implementation could improve sector risk mitigation efforts.

³⁸GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, [GAO-18-427](#) (Washington, D.C.: June 13, 2018).

CISA officials said they had not established milestones and timelines to complete CISA's efforts because the agency has prioritized defining its own role as national coordinator. For example, as of October 2022, CISA officials said they were in the process of developing ways to implement CISA's new authorities under the FY21 NDAA, which requires SRMAs to carry out their responsibilities in coordination with the CISA Director and consistent with DHS strategic guidance.

Additionally, officials said their November 2021 report outlined an approach for how to address the FY21 NDAA responsibilities. However, our analysis indicates that it does not include milestones and timelines to complete its outlined efforts. For example, the report outlines some of the proposed efforts described above and states that CISA should mature its role as national coordinator for critical infrastructure. But, the proposed efforts within the report do not have associated milestones and timelines. Additionally, CISA officials told us that, as of October 2022, the National Security Council staff was reviewing CISA's report.³⁹

We recognize that CISA's efforts to address its FY21 NDAA responsibilities are linked to its efforts to mature in its role as national coordinator. However, SRMA officials for all 16 critical infrastructure sectors reported that CISA has not yet provided guidance to help the agencies implement their FY21 NDAA responsibilities. Establishing milestones and timelines, and updating them when necessary, to accomplish its efforts to support SRMAs, would help ensure CISA completes them in a timely manner.

Conclusions

Protecting critical infrastructure is a national priority, given the debilitating effects of critical infrastructure disruptions from natural, intentional, or accidental events. The FY21 NDAA expanded upon SRMA responsibilities previously outlined in PPD-21, such as information sharing, and added responsibilities related to risk assessment and emergency preparedness. SRMA officials among the 16 critical

³⁹The FY21 NDAA requires the President to review the recommendations in the report and revise, as appropriate, the designation of a critical infrastructure sector or the designation of an SRMA. It also requires the President to submit to the appropriate congressional committees and congressional leadership a report that includes an explanation of the basis for accepting or rejecting the recommendations in the report and information relating to the analysis framework, methodology, metrics, and data used to evaluate the current framework for securing critical infrastructure and develop the recommendations. 6 U.S.C. § 652a(b)(3). According to CISA officials in January 2023, the President officially approved the recommendations in the 9002(b) report, and initiated the process to rewrite PPD-21.

infrastructure sectors described actions underway to address these new responsibilities, but faced some challenges.

As the national coordinator for critical infrastructure and SRMA for eight of the 16 critical infrastructure sectors, CISA is responsible for implementing its own new SRMA responsibilities while also helping all SRMAs implement their responsibilities. While CISA identified efforts that include opportunities to address challenges SRMAs face, CISA has not established milestones and timelines to complete all of these important tasks. Doing so would help ensure CISA completes its ongoing and planned efforts in a timely manner, and would improve CISA's accountability and transparency as it continues to contribute to the federal protection of critical infrastructure. This is particularly important to ensure timely updates of necessary guidance and to improve coordination and information sharing with SRMAs.

Recommendation for Executive Action

The Director of CISA should establish milestones and timelines for its efforts to provide guidance and improve coordination and information sharing that would help SRMAs implement their FY21 NDAA responsibilities, and ensure the milestones and timelines are updated through completion. (Recommendation 1)

Agency Comments

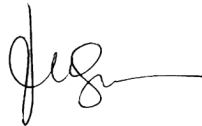
We provided a draft of this report to the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; and to the Environmental Protection Agency and the General Services Administration for review and comment. We received and incorporated technical comments from the Departments of Health and Human Services, Homeland Security, the Treasury, and the Environmental Protection Agency, as appropriate.

In its written comments, which are reproduced in appendix III, DHS concurred with our recommendation to establish milestones and timelines for its efforts to provide guidance and improve coordination and information sharing that would help SRMAs implement their FY21 NDAA responsibilities, and ensure the milestones and timelines for efforts CISA identifies are updated through completion. Specifically, DHS agreed with the importance of having a coordinated plan, including milestones and timelines, to help SRMAs implement their FY21 NDAA responsibilities.

The Department of the Treasury also provided written comments, which are reproduced in appendix IV.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; and the Administrators of the Environmental Protection Agency and the General Services Administration. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Tina Won Sherman at (202) 512-8461 or shermant@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

A handwritten signature in black ink, appearing to read 'Tina Won Sherman', with a long horizontal flourish extending to the right.

Tina Won Sherman
Director, Homeland Security and Justice

Appendix I: Additional Information on the Challenges Sector Risk Management Agencies Reported

We requested and obtained written responses to a standard set of questions from the nine sector risk management agencies (SRMAs) responsible for all 16 critical infrastructure sectors. The question set included asking for SRMA officials' perspectives about challenges they faced previously, or expected to face, in implementing their responsibilities. The most frequently cited challenges SRMA officials reported in implementing their responsibilities included limited authority because of the voluntary nature of private sector participation in SRMA activities and having limited or no dedicated resources for SRMA responsibilities.

Below, we provide examples of how the voluntary nature of private sector participation in SRMA activities affects certain sectors and reasons why some SRMAs will request additional resources.

Voluntary participation. As SRMA for the water and wastewater systems sector, Environmental Protection Agency officials said the water security program operates on a voluntary basis, with no statutory mandates that specifically require utilities to implement water security and resiliency measures to mitigate risk. As a result, officials believed sector visibility and information is lacking. As SRMAs for the government facilities and financial services sectors, respectively, officials from the General Services Administration and the Treasury described that voluntary stakeholder participation in sector programs affects their ability to collect information, and General Services Administration officials also stated that it affects sector assessments and evaluations.

As we reported in September 2020, Treasury officials, in response to recommendations aimed at improving the agency's ability to track progress and measure effectiveness of certain risk mitigation activities, told us their ability to collect that information is limited. Specifically, the department officials stated that some financial services sector entities would need legal assurance that information shared with the Treasury would not be released to other entities and that further information requests might be seen as another layer of regulatory compliance that would undermine trust in the Treasury.¹ As described in appendix II, these recommendations have not yet been implemented, and we

¹In commenting on a draft of this report in January 2023, Treasury officials said that while these challenges remain, the agency plans to take steps to engage collaboratively with the financial services sector to discuss the development of metrics on sector risk mitigation efforts and for determining the level and type of adoption of cybersecurity guidance.

**Appendix I: Additional Information on the
Challenges Sector Risk Management Agencies
Reported**

continue to believe their implementation could improve sector risk mitigation efforts.









Additionally, as the SRMA for eight sectors, Cybersecurity and Infrastructure Security Agency (CISA) officials stated that the voluntary nature of the partnership framework that they and other SRMAs foster means that SRMAs and private-sector partners do not always share the same priorities when it comes to participation in sector evaluation processes and data collection efforts. They believed that having a two-way flow of information contributes to a more complete and comprehensive understanding of shared threats.

Dedicated resources. Figure 9 below describes plans from SRMAs to request resources to help fulfill their SRMA responsibilities outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.²

²⁶ U.S.C. § 665d.

Appendix I: Additional Information on the Challenges Sector Risk Management Agencies Reported

Figure 9: Examples of Sector Risk Management Agency Officials' Views on Requests for Dedicated Resources, by Sector

Sector and sector risk management agency	Plans to request dedicated resources for Sector Risk Management Agency responsibilities
 <p>Defense industrial base Department of Defense</p>	<p>Reported that it plans to request additional resources for vulnerability analysts, cyber threat and intelligence analysts, engineers, cyber forensic examiners, developers, liaison and support staff, and assessment activities.</p>
 <p>Food and agriculture Department of Agriculture</p>	<p>Reported that it intends to request Sector Risk Management Agency support for fiscal year 2023 or fiscal year 2024.</p>
 <p>Financial services Department of the Treasury</p>	<p>Reported that it intends to request six additional full-time equivalent positions and \$5.0 million in fiscal year 2024.</p>
 <p>Government facilities Department of Homeland Security</p>	<p>Reported that it intends to request dedicated staffing for responsibilities for both physical and cybersecurity support once the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance to assess its needs.</p>
 <p>Government facilities General Services Administration</p>	<p>Reported that it intends to request dedicated staffing for both physical and cybersecurity responsibilities once it determines the level of support needed as CISA has not shared what changes will be made. It also was not certain as to how co-Sector Risk Management Agencies would request funding for what it see as a CISA-led program.</p>
 <p>Healthcare and public health Department of Health and Human Services</p>	<p>Reported that it continues to submit requests for additional support of Sector Risk Management Agency responsibilities through the annual appropriations process. For fiscal year 2024, it requested an increase in funding of \$6.5 million and an additional five full-time equivalent positions.</p>
 <p>Transportation systems Department of Homeland Security</p>	<p>Reported that the Sector Risk Management Agency responsibilities were initially more limited and less formalized, but as the role has evolved, it has created a need for dedicated staffing to support the responsibilities outline in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.</p>
 <p>Water and wastewater systems Environmental Protection Agency</p>	<p>Reported that the Office of Water requested an increase of over \$3.9 million and six full-time equivalent positions to enhance cybersecurity incident preparation, response, recovery, information sharing, and intelligence for water utilities to protect infrastructure.</p>

Source: GAO analysis of agency responses. | GAO-23-105806

Note: Agencies provided information about plans to request dedicated resources to address the expanded responsibilities in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. See 6 U.S.C. § 665d.

As the SRMA for eight sectors, CISA officials stated that they believed the resource levels provided for in the agency's current baseline for SRMA

**Appendix I: Additional Information on the
Challenges Sector Risk Management Agencies
Reported**

activities, plus increases provided for in the fiscal year 2022 enacted budget, are sufficient to fulfill the newly codified SRMA roles and responsibilities. However, CISA officials reported plans to work with Office of Management and Budget to evaluate options for annualizing the increased amount received in fiscal year 2022 for the SRMA function in future budget submissions. If they do not receive the requested increase in funding, CISA officials stated that they would evaluate options to request required staff and funding in future budget years.

Appendix II: GAO Recommendations That Could Help Agencies Address FY21 NDAA

We have a large body of work examining aspects of critical infrastructure protection and have made over 80 recommendations to sector risk management agencies (SRMAs) relevant to the responsibilities outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA).¹ As of December 2022, agencies had yet to implement 58 of these recommendations. If addressed, these recommendations have the opportunity to help agencies carry out their SRMA responsibilities delineated in the FY21 NDAA. Below are selected examples of these recommendations relevant to SRMAs' implementation of their NDAA responsibilities.

To identify these recommendations, we reviewed our prior work issued since 2013, when Presidential Policy Directive-21 and the 2013 National Plan were issued, because the responsibilities outlined in those documents are also largely reflected in the FY21 NDAA. Specifically, we reviewed reports that addressed three main categories of activities outlined in the FY21 NDAA:

- Risk, including sector risk management and assessing sector risk;
- Coordination, including sector coordination and information sharing regarding physical security and cybersecurity threats; and
- Preparedness and Response, including incident management support and contributions to emergency preparedness efforts.

We identified 19 reports, in which we made a total of 88 relevant recommendations, 27 of which have been implemented. We present below the reports with recommendations not yet implemented that were relevant to the three categories above to identify actions SRMAs could take to help address the FY21 NDAA responsibilities. We also vetted the list of reports and recommendations with internal subject matter experts.

Addressing Risk. Table 3 includes recommendations not yet implemented that address supporting sector risk management and assessing sector risk.

¹See 6 U.S.C. § 665d.

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Table 3: Recommendations from GAO Reports Not Yet Implemented Addressing Risk

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>The majority of sector risk management agencies (SRMAs) had not developed metrics to measure and report on the effectiveness of all of their cyber risk mitigation activities or their sectors' cybersecurity posture.</p>	<p>SRMAs should collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities.</p> <p>Status: The departments of Health and Human Services and Agriculture did not comment on or implement this recommendation. The department of the Treasury also did not implement this recommendation, but this recommendation was superseded by GAO-20-631 described below. Finally, the Environmental Protection Agency generally agreed with the recommendation and took steps to address it, but those steps were not finalized and did not show sufficient evidence that the efforts would address the recommendation.</p>	<p>Addressing the intent of these recommendations will be important for monitoring the progress of the programs SRMAs establish and carry out pursuant to their National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) responsibilities to assist critical infrastructure owners and operators within their designated sector to manage risk.</p>	<p>Multiple</p>	<p>Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress, GAO-16-79, (Washington, D.C., Nov. 19, 2015)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>The Transportation Security Administration (TSA) had not updated its risk assessment methodology since 2014 to reflect current threats to the pipeline industry and did not fully document data sources, assumptions, and uncertainties.</p>	<p>TSA should identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with the National Infrastructure Protection Plan and DHS critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems.</p> <p>TSA should also take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool, after completing recommended enhancements.</p> <p>Status: TSA officials initially agreed to both of these recommendations, but in 2022 requested they be closed as not implemented because TSA believes implementing these recommendations will not provide significant security-related benefit.</p>	<p>Addressing these recommendations would improve TSA's efforts to address its risk assessment responsibilities in the FY21 NDAA, such as by enhancing its risk calculations, and would provide TSA with increased assurance that the agency accurately and comprehensively ranks relative risk among pipeline systems.</p>	<p>Transportation Systems</p>	<p>Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management, GAO-19-48, (Washington, D.C., Dec. 18, 2018)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>Executive branch strategy documents on confronting cyber threats did not address the specific risks and challenges facing the electric grid and did not include key characteristics of a national strategy. As the SRMA, the Department of Energy (DOE) had not fully analyzed the cybersecurity risks and challenges to the grid. The Federal Energy Regulatory Commission (FERC) had not ensured that its approved grid cybersecurity standards fully address leading federal guidance for improving critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework. In addition, FERC had not evaluated the risk of a coordinated cyberattack on geographically distributed targets in approving the threshold for which grid cyber systems must comply with requirements in the full set of grid cybersecurity standards.</p>	<p>DOE should develop a plan aimed at implementing the federal cybersecurity strategy for the electric grid and ensure that the plan addresses the key characteristics of a national strategy, including a full assessment of cybersecurity risks to the grid.</p> <p>FERC should determine whether to direct North American Electric Reliability Corporation (NERC) to adopt any changes to its cybersecurity standards to ensure those standards more fully address the NIST Cybersecurity framework and address current and projected risks.</p> <p>FERC should (1) evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and, (2) based on the results of that evaluation, determine whether to direct NERC to make any changes to the threshold for mandatory compliance with requirements in the full set of cybersecurity standards.</p> <p>Status: DOE and FERC agreed with our recommendations, but actions taken to address them are still ongoing.</p>	<p>Addressing this recommendation could help DOE implement its FY21 NDAA responsibilities regarding risk assessment and help decision makers in allocating resources to address risks and challenges.</p> <p>Addressing the recommendations to FERC would also support the FY21 NDAA risk management responsibilities for the energy sector.</p>	Energy	<p>Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, GAO-19-332, (Washington, D.C., Aug. 26, 2019)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>The Cybersecurity and Infrastructure Security Agency (CISA) had not developed plans for how it would address challenges, such as concerns about incident response, identified in reviews of the agency's 2018 election security assistance.</p>	<p>CISA should document how the agency intends to address challenges identified in its prior election assistance efforts.</p> <p>Status: CISA agreed with the recommendation and has taken steps towards implementing it, but CISA has not documented steps intended to fully address challenges that could persist and impact future elections.</p>	<p>Addressing this recommendation would support CISA's FY21 NDAA responsibilities to coordinate with nonfederal entities by helping to protect election infrastructure, identify threats, and coordinate and provide accurate threat information that addresses the needs of the election infrastructure community.</p>	<p>Election Infrastructure Subsector of the Government Facilities Sector</p>	<p>Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections, GAO-20-267, (Washington, D.C., Feb. 06, 2020)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>Treasury had not prioritized, tracked, or measured the progress of the financial services sector's efforts against sector goals for enhancing security and resilience.</p> <p>The financial services sector-specific plan did not include metrics we had previously recommended to measure the progress of the risk mitigation efforts the sector is performing.</p>	<p>Treasury, in coordination with the Department of Homeland Security and others, should track the content and progress of sector wide cyber risk mitigation efforts, and prioritize their completion according to sector goals and priorities in the sector-specific plan, which should be updated to include such metrics and information on how the sector's ongoing and planned risk mitigation efforts will meet sector goals and requirements.</p> <p>Status: Treasury stated that it generally agreed with our two recommendations, but expressed caution about its level of authority to implement them because its ability to track, monitor, and to both devise and measure progress toward metrics on sector risk mitigation efforts is limited. In particular, Treasury stated it cannot require that financial regulators or sector firms provide it with data on efforts that are underway or information on how those efforts reduce risks. Treasury also stated that it was waiting for the National Plan update before updating the sector-specific plan. In January 2023, Treasury officials said the agency plans to engage collaboratively with sector partners to mitigate cyber risk.</p>	<p>Addressing these recommendations would help the Treasury better manage sector risks, as called for in the FY21 NDAA, by determining the effectiveness of its efforts.</p>	<p>Financial Services</p>	<p>Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts, GAO-20-631, (Washington, D.C., Sept. 17, 2020)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>The Department of Energy’s (DOE) plans did not fully address risks to the grid’s distribution systems, such as addressing distribution systems’ vulnerabilities related to supply chains.</p>	<p>The Secretary of Energy, in coordination with DHS, states, and industry, should more fully address risks to the grid’s distribution systems from cyberattacks—including the potential impact of such attacks—in DOE’s plans to implement the national cybersecurity strategy for the grid.</p> <p>Status: DOE agreed with our recommendation and took steps to address it. To fully address our recommendation, DOE should more fully address risks to the grid’s distribution systems from cyberattacks in its plans to implement the national cybersecurity strategy for the grid.</p>	<p>Addressing this recommendation to help its state and industry partners improve and effectively prioritize cybersecurity by more fully addressing risks to the grid’s distribution systems in its updated plans would help DOE fulfill its FY21 NDAA responsibilities to identify and prioritize sector risks.</p>	Energy	Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems, GAO-21-81 , (Washington, D.C., Mar. 18, 2021)
<p>The sector-specific plan for the Education subsector, last issued in 2010, was out-of-date and did not reflect current risks and operational circumstances affecting the subsector.</p> <p>The Department of Education had not determined whether sector-specific guidance is needed for K-12 schools to help protect against cyber threats.</p>	<p>The Secretary of Education should initiate a meeting with the Director of CISA to determine how to update its sector-specific plan (SSP) for the Education subsector. The plan should assess and prioritize federal actions to assist K-12 schools in protecting themselves from cyberattacks. The Secretary should also determine if the Education subsector needs additional guidance.</p> <p>Status: The Secretary of Education agreed with our recommendations and in 2022, reported that the department held an initial meeting with CISA to discuss updating the Education Facilities Subsector sector-specific plan. Education has not discussed the need for sector-specific guidance because it was taking other steps that they thought were necessary before determining the need for guidance.</p>	<p>Addressing the recommendations would help the department support sector risk management, as called for in the FY21 NDAA.</p>	Education Facilities Subsector of the Government Facilities Sector	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)

Source: GAO. | GAO-23-105806

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Addressing Coordination. Table 4 includes recommendations not yet implemented that address sector coordination and facilitating the sharing of information regarding physical security and cybersecurity threats.

Table 4: Recommendations from GAO Reports Not Yet Implemented Addressing Coordination

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
None of the sector risk management agencies (SRMAs) had measured the cybersecurity framework's implementation by entities within their respective sectors, due in large part to a lack of available data regarding adoption across the respective sectors.	<p>The Secretaries of Agriculture, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury should take steps to consult with respective sector partner(s), such as the sector coordinating council, Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.</p> <p>Status: While the above listed agencies generally agreed with the recommendation and took some steps to collect feedback from sector partners, none have fully developed methods to provide a comprehensive understanding of the framework's adoption.</p>	Addressing these recommendations presents an opportunity to support SRMAs' responsibilities under the National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) by facilitating awareness and understanding of the security-related actions within their sectors. In the absence of this information sharing, SRMAs will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation.	Multiple	Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption, GAO-18-211 , (Washington, D.C., Feb. 15, 2018)

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
The Environmental Protection Agency (EPA) had not assessed how they could organize a network of technical assistance providers to effectively provide the assistance that utilities needed to enhance their resilience to climate change.	EPA should identify technical assistance providers and engage them in a network to help water and wastewater utilities incorporate climate resilience into their projects. Status: EPA neither agreed nor disagreed with the recommendation and stated that participation of the water sector and of other federal agencies in helping these utilities is voluntary and not something the agency can enforce. Steps taken by the agency to date do not fully address the intent of the recommendation to develop a network to help the many drinking water and wastewater utilities across the country incorporate climate information into their resilience planning.	Addressing this recommendation could further promote the exchange of information called for in the FY21 NDAA by helping drinking water and wastewater utilities consider climate resilience in the planning and design of projects on an ongoing basis.	Water and Wastewater Systems	Water Infrastructure: Technical Assistance and Climate Resilience Planning Could Help Utilities Prepare for Potential Climate Change Impacts, GAO-20-24 , (Washington, D.C., Jan. 16, 2020)
Most of the nine agencies with a lead role in protecting the 16 critical infrastructure sectors, referred to as SRMAs, had not developed methods to determine the level and type of adoption of the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, as we previously recommended. As a result, the SRMAs had not collected and reported sector-wide improvements.	The Secretaries of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury should take steps to consult with respective sector partner(s) to collect and report on improvements gained from using the NIST cybersecurity framework. Status: The agencies reported varying stages of implementation, but have not fully addressed the recommendation.	Addressing these recommendations by collecting and reporting on improvements could help support SRMA efforts to implement their information sharing and reporting responsibilities under the FY21 NDAA.	Multiple	Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements, GAO-20-299 , (Washington, D.C., Feb. 25, 2020)

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
The Chemical Facility Anti-Terrorism Standards program did not fully address 3 of 4 key training practices for its cybersecurity training for inspectors or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance.	We made 5 recommendations related to training and workforce, including to fully incorporate key training practices and to identify workforce cybersecurity needs. Status: DHS agreed with our recommendations and has ongoing work intended to address them.	Addressing these recommendations to fully equip inspectors with the skills needed to perform cybersecurity assessments at chemical facilities and incorporating cybersecurity needs into its workforce planning processes could help DHS implement key sector coordination and risk assessment responsibilities as outlined in the FY21 NDAA.	Chemical	Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities, GAO-20-453 , (Washington, D.C., May 14, 2020)
The Department of Health and Human Services (HHS) did not describe coordination among two entities that are critical to the department's cybersecurity information sharing with the sector. HHS also had multiple mechanisms to facilitate collaboration with HHS and with the sector, but not all collaborative groups followed leading practices for collaboration identified by GAO.	We made seven recommendations to HHS to improve its collaboration and coordination within the department and the sector—six of which remain yet to be implemented. Status: HHS concurred with the six recommendations and described various actions to address them, but none of the six have been fully implemented.	Addressing the recommendations will strengthen HHS's ability to carry out the collaboration practices identified in the FY21 NDAA and can help ensure that HHS is improving cybersecurity within the department and sector.	Healthcare and Public Health	Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration, GAO-21-403 , (Washington, D.C., June 28, 2021)
The Department of Defense (DOD) did not develop performance measures to benchmark and to track overall program performance for the three grant programs it administers that support community coordination with local installations on climate change and extreme weather.	We made three recommendations related to developing performance measures for DOD's community grant programs that support community coordination with local installations on climate change and extreme weather. Status: DOD concurred with these recommendations, and informed GAO of ongoing actions to address them in August 2022. We will continue to monitor DOD's progress.	Addressing these recommendations can help DOD determine the operational effectiveness of its efforts and support collaboration among sector partners, a key element of the FY21 NDAA responsibilities.	Defense Industrial Base	Climate Resilience: DOD Coordinates with Communities, but Needs to Assess the Performance of Related Grant Programs, GAO-21-46 , (Washington, D.C., Dec. 10, 2020)

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>Federal Aviation Administration (FAA) had not established a tracking mechanism for monitoring progress on cybersecurity issues that were raised in coordination meetings.</p> <p>FAA did not have a staff training program specific to avionics cybersecurity, and few of the agency's certification engineers have received cybersecurity training.</p>	<p>We made six recommendations to FAA to strengthen its avionics cybersecurity oversight program.</p> <p>Status: FAA concurred with five out of six GAO recommendations, including the two related to the deficiencies discussed here. FAA described various actions to address them, but these recommendations have not been fully implemented.</p>	<p>Addressing these recommendations can further enhance the Transportation Systems sector SRMAs efforts to carry out their responsibilities to provide specialized expertise and support sector coordination, as called for in the FY21 NDAA.</p>	<p>Aviation Subsector of the Transportation Systems sector</p>	<p>Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks, GAO-21-86, (Washington, D.C., Oct. 09, 2020)</p>
<p>Stakeholders internal and external to Cybersecurity and Infrastructure Security Agency (CISA) questioned the relevance and usefulness of the National Critical Infrastructure Prioritization Program, designed to identify a list of systems and assets that, if destroyed or disrupted, would cause national or regional catastrophic effects.</p> <p>Additionally, stakeholders GAO interviewed did not understand how the framework related to prioritizing infrastructure, how it affected planning and operations, or where their particular organizations fell within it.</p> <p>Stakeholders also reported needing more regionally specific information to address critical infrastructure threats.</p>	<p>We made six recommendations to help improve CISA's critical infrastructure prioritization activities, including three that address coordination with stakeholders.</p> <p>Status: DHS concurred with these recommendations, and we will continue to monitor the agency's progress addressing them.</p>	<p>Addressing these recommendations could help ensure that the critical infrastructure community is fully engaged in implementing CISA's new prioritization framework and could help CISA and its partners in future infrastructure protection efforts, including those initiated as a result of the FY21 NDAA.</p>	<p>Multiple</p>	<p>Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing, GAO-22-104279, (Washington, D.C., Mar. 1, 2022)</p>

Source: GAO. | GAO-23-105806

Addressing Emergency Preparedness and Response. Table 5 includes recommendations not yet implemented that address supporting incident management and contributing to emergency preparedness efforts.

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Table 5: Recommendations from GAO Reports Not Yet Implemented Addressing Emergency Preparedness and Response

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>TSA had not revised the 2010 <i>Pipeline Security and Incident Recovery Protocol Plan</i> to reflect changes in federal laws or policies since the plan was issued in 2010.</p> <p>Specific to incident management, the plan states that it is to be consistent with other DHS response and incident command system procedures, but the current versions of that guidance were issued years after TSA's 2010 plan.</p>	<p>TSA should periodically review, and as appropriate, update the 2010 <i>Pipeline Security and Incident Recovery Protocol Plan</i> to ensure the plan reflects relevant changes in pipeline security threats, technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems.</p> <p>Status: TSA concurred and anticipated completion of the updated Protocol Plan by June 30, 2023.</p>	<p>Addressing this recommendation could help TSA implement the incident response and emergency preparedness responsibilities outlined in the National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) and help ensure pipeline stakeholders understand federal agencies' roles and responsibilities in preparing for, responding to, or supporting pipeline operators to restore service after a pipeline-related physical or cyber incident.</p>	Transportation Systems	<p>Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment, GAO-19-426, (Washington, D.C., June 05, 2019)</p>
<p>The Federal Communications Commission (FCC) obtained limited public input and had not publicly communicated the Hurricane Recovery Task Force's actions or findings related to Hurricane Maria following the 2017 Atlantic hurricane season.</p>	<p>FCC should enhance the transparency and accountability of FCC's operations by publicly reporting on the actions and findings of its Hurricane Recovery Task Force and determine if any changes in policy are needed to ensure FCC has transparent operations for any future disaster-related task forces.</p> <p>Status: FCC actions to address this recommendation remain ongoing.</p>	<p>Addressing this recommendation could provide accountability and transparency and help FCC assist DHS (as the Sector Risk Management Agency for the Communication Sector) implement its FY21 NDAA emergency preparedness responsibilities and could aid future disaster preparation.</p>	Communications	<p>Telecommunications: FCC Assisted in Hurricane Maria Network Restoration, but a Clarified Disaster Response Role and Enhanced Communication Are Needed, GAO-21-297, (Washington, D.C., Apr. 29, 2021)</p>

**Appendix II: GAO Recommendations That
Could Help Agencies Address FY21 NDAA**

Key deficiencies reported related to recommendation(s)	Summary of recommendation(s) and status	Why it matters	Applicable sector	GAO report
<p>The Department of Energy (DOE) did not have an overall strategy to guide its efforts to address climate change as a risk to the energy infrastructure, which includes the grid.</p>	<p>DOE should develop and implement a department-wide strategy to coordinate its efforts that defines goals and measures progress to enhance the resilience of the electricity grid to the risks of climate change.</p> <p>Status: DOE agreed and planned to update its existing grid resiliency strategy to address our recommendation.</p>	<p>Addressing this recommendation to develop and implement a department-wide strategy that defines goals and measures progress could help prioritize DOE’s climate resilience efforts to ensure that resources are targeted effectively, which in turn could help DOE fulfill its FY21 NDAA emergency preparedness responsibilities.</p>	Energy	<p>Electricity Grid Resilience: Climate Change Is Expected to Have Far-reaching Effects and DOE and FERC Should Take Actions, GAO-21-346, (Washington, D.C., Mar. 5, 2021)</p>
<p>CISA had not completed an assessment of its capabilities to perform as the federal coordinator for Emergency Support Function #2 (Communications) or assessed its effectiveness.</p> <p>Additionally, CISA had not updated its 2015 Communications Sector-Specific Plan and acknowledged that certain elements of the plan were out of date. For example, CISA had identified new and emerging threats and risks since 2015.</p>	<p>We recommended that CISA assess the effectiveness of its security and resilience support efforts; complete a capability assessment for Emergency Support Function #2; and revise the Communications Sector-Specific Plan.</p> <p>Status: CISA concurred with our recommendations and said the Communications Sector-Specific Plan would be completed by the end of March 2023 and that between that and the updated National Plan, goals would be updated against which CISA could measure effectiveness. Additionally, CISA reported that it has updated and expanded the list of Emergency Support Function #2 capabilities and initiated an on-going capability gap analysis.</p>	<p>Addressing these recommendations to develop metrics to indicate the effectiveness of security and resilience activities and the extent to which these activities are reducing risks could better position CISA to address emergency preparedness responsibilities outlined in the FY21 NDAA.</p> <p>Further, by updating the Sector-Specific Plan that addresses new and emerging threats and risks and by assessing Emergency Support Function #2 capabilities, CISA will be better positioned to ensure preparedness for future incidents, in line with its FY21 NDAA responsibilities.</p>	Communications	<p>Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector, GAO-22-104462, (Washington, D.C., Nov. 23, 2021)</p>

Source: GAO. | GAO-23-105806

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

January 14, 2023

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

Re: Management Response to Draft Report GAO-23-105806, "CRITICAL INFRASTRUCTURE PROTECTION: Timeframes to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities"

Dear Ms. Won Sherman:

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

DHS is pleased to note GAO's positive recognition of Cybersecurity and Infrastructure Security Agency (CISA) efforts to help sector risk management agencies implement their statutory responsibilities, including on-going efforts to develop and strengthen relationships with industry and government by meeting with Sector Coordinating Councils and issuing advisories and analysis reports to partners. CISA remains committed to fulfilling its role as Sector Risk Management Agency (SRMA), as defined in DHS's 2013 National Infrastructure Protection Plan (National Plan)¹ and clarified in Section 9002 of the January 2021 National Defense Authorization Act (NDAA)². Accordingly, CISA will continue working with partners across the sectors to sustain and strengthen collaborative security and resilience efforts.

The draft report contained one recommendation, with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted

¹ <https://www.cisa.gov/national-infrastructure-protection-plan>

² <https://www.cisa.gov/section-9002b-report>

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

technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2023.01.14 14:19:58 -05'00'

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

Enclosure

**Enclosure: Management Response to Recommendation
Contained in GAO-23-105806**

GAO recommended that the Director of CISA:

Recommendation 1: Establish milestones and timelines for its efforts to provide guidance and improve coordination and information sharing that would help SRMAs implement their FY21 NDAA responsibilities, and ensure those milestones and timelines are updated through completing of the efforts CISA identifies.

Response: Concur. CISA agrees with the importance of having a coordinated plan, including milestones and timelines, to provide guidance regarding coordination and information sharing that would help SRMAs implement their FY21 NDAA responsibilities. However, it is important to note that in a letter to Congress dated November 7, 2022³, President Joseph R. Biden Jr. requested an update to Presidential Policy Directive 21 (PPD-21), “Critical Infrastructure Security and Resilience,” issued February 2013. This effort is being led by the Homeland and Critical Infrastructure Resilience Interagency Policy Committee, which is currently reviewing PPD-21 to determine what changes are needed. Although there is currently no estimated completion date for this review, the PPD-21 update is likely to:

- (1) clarify and scope the list of SRMA responsibilities;
- (2) assess what is defined as critical infrastructure;
- (3) change the specific agencies responsible for mitigating and responding to risk in each critical infrastructure sector; and
- (4) modify how agencies serving as SRMA will interact with CISA in its effort to coordinate the broader national SRMA partnership framework.

While it is likely that GAO’s recommendation will be overcome by issuance of the updated PPD-21, CISA’s Stakeholder Engagement Division will continue its efforts to improve coordination and information sharing with all sector partners, to include the reinstatement of its leadership councils. The Stakeholder Engagement Division has already taken action through the reinstatement of its leadership councils, including the reinvigoration of the Federal Senior Leadership Council (FSLC), which kicked off on November 9, 2022. The FSLC will begin implementing the actions requested in President Biden’s letter, including (1) developing a shared process and template for sector risk management, and (2) redefining and updating critical infrastructure sector and SRMA structures and designations. CISA is committed to keeping GAO apprised of outcomes from FSLC meetings and will provide an update by July 31, 2023. Estimated Completion Date: September 30, 2025.

³ <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure/>

Appendix IV: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 19, 2023

Tina Won Sherman
Director, Homeland Security and Justice
Government Accountability Office

Dear Ms. Sherman:

Thank you for the opportunity to review the Government Accountability Office's (GAO) draft report entitled *Critical Infrastructure Protection: Timeframes to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities* (the Draft Report). The U.S. Department of the Treasury (Treasury) values GAO's analysis and has provided technical comments under separate cover.

The Draft Report reviews the effectiveness of sector risk management agencies (SRMAs) in carrying out the responsibilities outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA). Treasury is the SRMA for the Financial Services sector. The Draft Report contains a recommendation for the Director of the Cybersecurity & Infrastructure Security Agency. The Draft Report also reviews prior GAO recommendations related to SRMAs and identifies recommendations that, according to the Draft Report, if implemented may further help SRMAs carry out the responsibilities in the FY21 NDAA. Treasury is providing updates with respect to certain of those recommendations.

As a preliminary matter, Treasury agrees with GAO's objective for SRMAs to further implement their FY21 NDAA responsibilities. Indeed, Treasury already has taken steps to improve collaboration with the sector. In November 2022, Treasury realigned staff to create a new SRMA liaison division of OCCIP to focus exclusively on SRMA responsibilities and collaboration. The division will be supported by two teams: one focusing on intelligence and information sharing with the sector and the other focusing on sector risk and resilience.

As discussed in Appendix I of the Draft Report, the voluntary nature of private sector participation in SRMA activities affects Treasury's ability to implement certain recommendations. Notwithstanding these limitations, consistent with GAO's recommendations, and to improve sector risk mitigation efforts, Treasury plans to take steps to engage collaboratively with the Financial Services sector to discuss the development of metrics on sector risk mitigation efforts and for determining the level and type of framework adoption regarding use of the NIST cybersecurity framework.

Treasury appreciates GAO's continued work assessing implementation of the FY21 NDAA. Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

**Appendix IV: Comments from the Department
of the Treasury**



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Sincerely,

Todd Conklin
Deputy Assistant Secretary
Office of Cybersecurity and Critical Infrastructure
Protection
U.S. Department of the Treasury

1/19/2023

X Todd Conklin

Todd Conklin
Deputy Assistant Secretary
Signed by: Milad Maleki

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Ben Atwater (Assistant Director); Susanna Kuebler (Analyst-in-Charge); Nasreen Badat; Ben Crossley; Michele Fejfar; Mike Gilmore; Tracey King; Amelia Koby; Steve Komadina; Joshua Leiling; Jan Montgomery; and Janet Temko-Blinder made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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

