United States Government Accountability Office

Testimony

Before the Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, March 23, 2023

CRITICAL INFRASTRUCTURE PROTECTION

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

Statement of Tina Won Sherman, Director,
Homeland Security and Justice

GAO-23-106720

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on Sector Risk Management Agencies (SRMAs)—departments or agencies, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise to a sector. My testimony today summarizes the findings from our February 2023 report entitled *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*.[1] That report examined new responsibilities for SRMAs and the Department of Homeland Security's role in coordinating SRMA activities.[2] [3]

Events have demonstrated how disruption or destruction of the nation's critical infrastructure could have debilitating effects. In particular, the 2021 cyberattack on the Colonial Pipeline disrupted the nation's largest fuel pipeline, and an extreme weather event in Texas caused widespread power and water outages.[4] Such events also illustrate how the nation's critical infrastructure assets and systems are often interconnected with critical infrastructure in other sectors 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

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

[2]6 U.S.C. § 665d.

[3]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 outlined these new SRMA responsibilities.

[4]In 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.

critical infrastructure risks.[5] 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 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, SRMAs are responsible for leading, facilitating, or supporting the security and resilience programs and associated activities within their designated critical infrastructure sector.[6] 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) includes a provision for GAO to report on the effectiveness of SRMAs in carrying out responsibilities set forth in the act. Our February 2023 report and my statement today addresses (1) how the FY21 NDAA changed sector risk management agency responsibilities, and the actions these agencies reported taking to address them; and (2) the extent to which CISA identified and undertook efforts to help sector risk management agencies implement their responsibilities set forth in the FY21 NDAA.

To address these objectives, we analyzed the FY21 NDAA and relevant policy directives, collected written responses from SRMAs for all 16 sectors using a standardized information collection tool, reviewed other

[5]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a), 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.

[6]6 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.

DHS documents, and interviewed CISA officials.[7] Additional information about our scope and methodology can be found in our February 2023 report. Our work was performed in accordance with generally accepted government auditing standards.

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

The FY21 NDAA expanded SRMA responsibilities previously outlined in Presidential Policy Directive-21 (PPD-21) and added risk assessment and emergency preparedness as responsibilities not previously included in the directive for SRMAs.[8] 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 information sharing responsibilities found in PPD-21 by adding specific activities for SRMAs to carry out within these areas. For example, the FY21 NDAA requires SRMAs to conduct sector coordination activities, including serving as the 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.

[7]Three critical infrastructure sectors have co-SRMAs. 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.

[8]CISA 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 Response 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 Infrastructure Protection Plan, the critical infrastructure sectors and SRMAs 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).

Expanded responsibilities. In response to the expanded responsibilities required by the FY21 NDAA described above, some SRMAs reported having actions underway to address these responsibilities. 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. For example, as SRMA in the healthcare and public health sector, Department of Health and Human Services officials 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.

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, representing the energy sector and water and wastewater systems sector respectively, reported that they already address the responsibilities outlined in the FY21 NDAA.

Finally, as an 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.

Added responsibilities. To address the added risk assessment and emergency preparedness responsibilities required by the FY21 NDAA, 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. For example, as SRMA in the communications sectors, DHS officials reported plans to develop and maintain a communications risk register that includes cybersecurity risks to emergency communications infrastructure. SRMA officials for 15 of the

16 critical infrastructure sectors also stated that they had conducted risk assessment activities prior to their inclusion in the FY21 NDAA.[9]

With regard to emergency preparedness responsibilities, 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. For example, as SRMA in the financial services sector, Department of the Treasury officials reported enhancing a tabletop exercise program, developing a functional exercise platform to improve cybersecurity exercises, and refining incident management and crisis communication toolkits. 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.

Implementation challenges. 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. According to SRMA officials, these challenges pre-dated the enactment of the FY21 NDAA. Additional 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.[10]

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. 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

[9]As 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.

[10]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.

existed prior to the FY21 NDAA and they generally expected them to continue.

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.

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.[11] In addition, CISA officials described various efforts to help SRMAs implement their FY21 NDAA responsibilities, including:

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.[12] CISA officials told us in March 2022 that these efforts could include both standardized metrics to measure effectiveness across all sectors, and sector-specific metrics.

Develop standardized budget guidance. In its November 2021 report, CISA officials identified a need to develop a baseline cost estimation tool for SRMAs.[13] According to the report, this tool would provide SRMAs a baseline estimate of resource needs, and could be tailored to each

[11]In 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).

[12]CISA, *Section 9002(b) Report*, 42.

[13]CISA, *Section 9002(b) Report*, 5.

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.

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, triaging information in response to incidents, and responding to requests for information.

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, 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.

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.

Update the 2013 National Plan and sector-specific plans. CISA officials told us in March 2022 that the updated National Infrastructure Protection Plan (National Plan) will clarify SRMA responsibilities in response to the FY21 NDAA. The National Plan is a key guidance document that provides the overarching national approach for critical infrastructure protection. CISA officials stated that the National Plan 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. 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.

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.[14]

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.

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 had not yet provided guidance to help the agencies implement their FY21 NDAA responsibilities. Establishing milestones and timelines, and updating them when necessary, to

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

accomplish its efforts to support SRMAs, would help ensure CISA completes them in a timely manner.

We recommended, and DHS concurred, that the Director of CISA 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.[15] As of March 2023, the agency has not yet implemented the recommendation. CISA officials stated that the Administration's Homeland and Critical Infrastructure Resilience Interagency Policy Committee is in the process of updating PPD-21. Once it is completed, CISA will work to establish the milestones and timelines needed to develop guidance on improving coordination and information sharing.

However, as of March 2023, CISA had not developed milestones and timelines to complete its efforts. CISA officials stated that they could not provide a specific timeline for issuing the updated National Plan until the Administration completes a review of PPD-21. CISA officials stated that the Federal Senior Leadership Council has started the Sector Analysis Working Group, which is an interagency consensus-based group that will recommend a new sector designation structure and corresponding SRMA designations. CISA officials reiterated that they plan to issue guidance on improving coordination and information sharing.

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

[15]GAO-23-105806. GAO has a large body of work examining aspects of critical infrastructure protection and has made over 80 recommendations to SRMAs relevant to the responsibilities outlined in the FY21 NDAA. These recommendations involved sector risk management and assessing sector risk, sector coordination and facilitating the sharing of information regarding physical security and cybersecurity threats, and incident management and contributing to emergency preparedness efforts. As of December 2022, agencies had yet to implement 58 of these recommendations. For more information on these recommendations, see appendix II in GAO-23-105806.

GAO Contacts and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Tina Won Sherman, Director, Homeland Security and Justice, 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 statement. GAO staff who made key contributions to this testimony are Ben Atwater and Christopher Ferencik (Assistant Directors); Steve Komadina (Analyst-in-Charge); Michele Fejfar; Mike Gilmore; Tracey King; Margaret Ullengren; Haley Wall; and Candice Wright.

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