United States Government Accountability Office

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, April 6, 2022

CRITICAL INFRASTRUCTURE PROTECTION

DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure

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

GAO Highlights

Highlights of GAO-22-105973, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Committee on Homeland Security, House of Representatives

April 6, 2022

CRITICAL INFRASTRUCTURE PROTECTION

DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure

Why GAO Did This Study

The nation's critical infrastructure consists of physical and cyber assets and systems that are vital to the United States. Their incapacity or destruction could have a debilitating impact on security, national public health and safety, or national economic security. Critical infrastructure provides the essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Protecting this infrastructure is a national security priority.

GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting (1) cyber critical infrastructure in 2003 and (2) the privacy of personally identifiable information in 2015.

This statement discusses DHS's efforts to address critical infrastructure security. For this testimony, GAO relied on selected products it issued from September 2018 to March 2022, including GAO-21-236-and GAO-22-104279.

What GAO Recommends

GAO has made various recommendations to strengthen critical infrastructure security efforts, with which DHS has agreed. DHS has implemented or described planned actions to address these recommendations.

What GAO Found

To improve critical infrastructure security, key actions Department of Homeland Security (DHS) needs to take include (1) strengthening the federal role in protecting the cybersecurity of critical infrastructure and (2) improving priority setting efforts.

Strengthen the federal role in protecting the cybersecurity of critical infrastructure. Pursuant to legislation enacted in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS was charged with responsibility for enhancing the security of the nation's critical infrastructure in the face of both physical and cyber threats. In March 2021, GAO reported that DHS needed to complete key activities related to the transformation of CISA. This includes finalizing the agency's mission-essential functions and completing workforce planning activities. GAO also reported that DHS needed to address challenges identified by selected critical infrastructure stakeholders, including having consistent stakeholder involvement in the development of related guidance. Accordingly, GAO made 11 recommendations to DHS, which the department intends to implement by end of 2022.

Improve priority setting efforts. Through the National Critical Infrastructure Prioritization Program, CISA is to identify a list of systems and assets that, if destroyed or disrupted, would cause national or regional catastrophic effects. Consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, CISA annually updates and prioritizes the list. The program's list is used to inform the awarding of preparedness grants to states. However, in March 2022, GAO reported that nine of 12 CISA officials and all 10 of the infrastructure stakeholders GAO interviewed questioned the relevance and usefulness of the program. For example, stakeholders questioned the current relevance of the criteria used to add critical infrastructure to the Prioritization Program list. In 2019, CISA published a set of 55 national critical functions of the government and private sector considered vital to the security, economy, and public health and safety of the nation (see figure). However, most of the federal and nonfederal critical infrastructure stakeholders that GAO interviewed reported being generally uninvolved with, unaware of, or without an understanding of the goals of the framework for its critical functions. GAO made recommendations to DHS in its March 2022 report to address these concerns, such as ensuring stakeholders are fully engaged in the framework's implementation, and DHS agreed with the recommendations.

Examples of Critical Infrastructure

Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsevv/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-105973

View GAO-22-105973. For more information, contact Tina Won Sherman at (202) 512-8461 or ShermanT@gao.gov.

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee:

Thank you for the opportunity to contribute to today's discussion on federal perspectives to secure the nation's critical infrastructure.[1] As you know, the nation's critical infrastructure consists of physical and cyber assets and systems that are vital to the United States. Their incapacity or destruction could have a debilitating impact on security, national economic security, or national public health and safety.[2] Critical infrastructure provides the essential functions—such as supplying water, generating energy, and producing food—that underpin American society. Protecting this infrastructure is a national security priority.

We have long stressed the urgent need for effective cybersecurity to protect critical infrastructure, as underscored by increasingly sophisticated threats and frequent cyber incidents.[3] Recent events—including the ransomware attack that led to a shutdown of a major U.S. fuel pipeline, cyber threat actors who obtained unauthorized access to a U.S. water treatment facility in an attempt to increase the amount of a caustic chemical that is used as part of the water treatment process, and a cyberattack campaign again U.S. government agencies and other entities—have illustrated that the nation's critical infrastructure continues to face growing cyber threats.[4] Because the majority of critical infrastructure is owned and operated by the private sector, it is vital that

[1]The term "critical infrastructure," as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e).

[2]42 U.S.C. § 5195c(e).

[3]See, for example, GAO, *Cybersecurity and Information Technology: Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas*, GAO-21-105325 (Washington, D.C.: July 28, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[4]For more information regarding such recent events, see GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks*, GAO-21-594T (Washington, D.C.: May 25, 2021). Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

the public and private sectors work together to protect these assets and systems.

My remarks today will focus on DHS's efforts to strengthen the federal role in protecting the cybersecurity of critical infrastructure and improving its priority-setting efforts. This statement is based on the results of our prior work, which includes the reports and testimonies that we cite throughout this statement, issued from September 2018 to March 2022. Detailed information about the scope and methodology for our prior work can be found in the products cited throughout this statement.

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

Background

Information systems supporting federal agencies and our nation's critical infrastructure—such as transportation systems, communications, education, energy, and financial services—are inherently at risk. Compounding the risk, systems and networks used by federal agencies and our nation's critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet. Examples of critical infrastructure are shown in figure 1.

The Department of Homeland Security (DHS) coordinates the overall federal effort for national critical infrastructure protection.[5] This effort spans across the 16 federally designated sectors and prioritizing available resources to the most critical infrastructure can enhance our nation's security, increase resiliency, and reduce risk.[6] Our prior work has cited DHS actions to identify and assess risk to critical infrastructure. For

[5]The Homeland Security Act of 2002 created DHS and gave the agency responsibilities for coordinating national critical infrastructure protection efforts. See generally Pub. L. No. 107-296, tit. II, 115 Stat. 2135, 2145.

[6]Federal policies identify 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

example, we reported in March 2022 on DHS's Cybersecurity and Infrastructure Security Agency's (CISA) programs to prioritize assets and systems for protection efforts.[7] Specifically, we evaluated the National Critical Infrastructure Prioritization Program (NCIPP), which, consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, annually prioritizes critical infrastructure based on the consequences associated with the disruption or destruction of those assets.[8] The program's list is used to inform the awarding of preparedness grants to states. We also examined CISA's National Critical Functions framework, which consists of 55 National Critical Functions, which are the functions of government and nongovernmental entities 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. Our prior findings on both the NCIPP and National Critical Functions framework are discussed later in this statement.

Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsevv/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-105973

[7]GAO, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing*, GAO-22-104279 (Washington, D.C.: Mar. 1, 2022)

[8]Originally developed in 2006, the NCIPP identifies critical infrastructure that would result in national-level consequences if disrupted or destroyed, resulting in classified lists of specific assets, clusters, and systems. The NCIPP annually prioritizes critical infrastructure based on the consequences associated with the disruption or destruction of those assets. To conduct this work, CISA coordinates a voluntary effort with states and other partners to identify, prioritize, and categorize high-priority critical infrastructure.

GAO Has Previously Identified Four Major Cybersecurity Challenges Facing the Nation

To underscore the importance of this issue, we have designated information security as a government-wide high-risk area since 1997.[9] In 2003, we added the protection of critical infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.[10]

In our high-risk updates from September 2018 and March 2021, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government faces.[11] These challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.

Federal Law and Policy Establish Requirements for Critical Infrastructure

Federal law and policy establish roles and responsibilities for the protection of critical infrastructure, discussed below in chronological order.

- **Presidential Policy Directive 21.** In February 2013, the White House issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, to specify critical infrastructure responsibilities.[12] Among other things, the order designated nine federal sector-specific agencies with lead roles in protecting critical infrastructure sectors. The lead agencies coordinate federally sponsored activities within their respective sectors. The policy also directed DHS to coordinate with lead agencies to develop a description of functional relationships

[9]GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: Feb. 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[10]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015) and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: Jan. 2003).

[11]GAO-21-288 and GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

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

across the federal government related to critical infrastructure security and resilience. The policy further provided that DHS, in coordination with lead agencies, to conduct an analysis and recommend options for improving public-private partnership effectiveness.

- **Executive Order 13636.** In February 2013, the White House issued Improving Critical Infrastructure Cybersecurity, Executive Order 13636, which called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing.[13] To do so, the order established mechanisms for promoting engagement between federal and private organizations. Further, the order directed DHS, with help from the lead agencies, to identify, annually review, and update a list of critical infrastructure sectors for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework.** Executive Order 13636 directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes.[14] Further, the order directed the lead agencies, in consultation with DHS and other interested agencies, to coordinate with critical infrastructure partners to review the cybersecurity framework. The agencies, if necessary, should develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

  In response to the order, in February 2014, NIST first published its framework—a voluntary, flexible, performance-based framework of cybersecurity standards and procedures. The framework, which was updated in April 2018, outlines a risk-based approach to managing cybersecurity that is composed of three major parts: a framework core, profiles, and implementation tiers.[15] The framework core

[13]Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

[14]The Cybersecurity Enhancement Act of 2014 authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure. 15 U.S.C. § 272(c)(15). *The Framework for Improving Critical Infrastructure Cybersecurity* represents that voluntary set of standards.

[15]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 2018).

provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes.

- **Cybersecurity and Infrastructure Security Agency Act of 2018.** The November 2018 act established CISA,[16] within DHS, and gave it responsibility to coordinate a national effort to secure and protect against critical infrastructure risks. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.
- **William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.** The act established roles and responsibilities for lead agencies, known as sector risk management agencies, in protecting the 16 critical infrastructure agencies.[17] According to the act, among other things, the lead agencies are required to (1) coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) support sector risk management, in coordination with CISA; (3) assess sector risk, in coordination with CISA; (4) coordinate the sector, including by serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; and (5) support incident management, including supporting CISA, upon request, in asset response activities.

  The act also established the Office of the National Cyber Director within the Executive Office of the President.[18] Among other responsibilities, the Director is to serve as the principal advisor to the White House on cybersecurity policy and strategy, including coordination of implementation of national cyber policy and strategy.

  In June 2021, the Senate confirmed a Director to lead this new office. In October 2021, the National Cyber Director issued a strategic intent statement, outlining a vision for the Director's office and the high-level lines of efforts it intends to focus on, including national and federal

[16]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169, (Nov. 16, 2018) (codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[17]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 states that the term "sector risk management agency" replaces the term "sector-specific agency" in the Homeland Security Act of 2002. The act amends the Homeland Security Act of 2002 and sets out sector risk management agency responsibilities within this critical infrastructure framework. Pub. L. No. 116-283, § 9002, 134 Stat. 3388, 4768.

[18]Pub. L. No. 116-283, § 1752, 134 Stat. at 4144 (codified at 6 U.S.C. § 1500).

cybersecurity; budget review and assessment; and planning and incident response, among others.[19]

Executive Order 14028. In May 2021, the President issued, Improving the Nation's Cybersecurity, Executive Order 14028, that was prompted, in part, by malicious cyber campaigns that threaten the public and private sectors.[20]

DHS Actions Urgently Needed to Protect Critical Infrastructure

Over the last several decades, we have emphasized the urgent need for the federal government to improve its ability to protect against cyber and other threats to our nation's critical infrastructure. In our recent work, we emphasized the need for the federal government to address major cybersecurity challenges through critical actions. These actions include the need for DHS to strengthen its role in protecting the cybersecurity of critical infrastructure. In addition, as we reported in March 2022, DHS's CISA should take actions to improve its priority setting efforts for the protection of critical infrastructure.[21]

DHS Needs to Strengthen Its Role in Protecting the Cybersecurity of Critical Infrastructure

The federal government has been challenged in working with the private sector to protect critical infrastructure. We have made recommendations aimed at strengthening DHS's role in critical infrastructure cybersecurity, including by (1) enhancing the capabilities and services of CISA and (2) ensuring that federal agencies with sector-specific responsibilities are providing their sector partners with effective guidance and support.

DHS Needs to Complete CISA Transformation Activities

The importance of clear cybersecurity leadership extends beyond the White House to other key executive branch agencies, including DHS. Federal legislation enacted in November 2018 established CISA within the department to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on

[19]The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, D.C.: Oct. 28, 2021).

[20]Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021).

[21]GAO-22-104279.

cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency.[22]

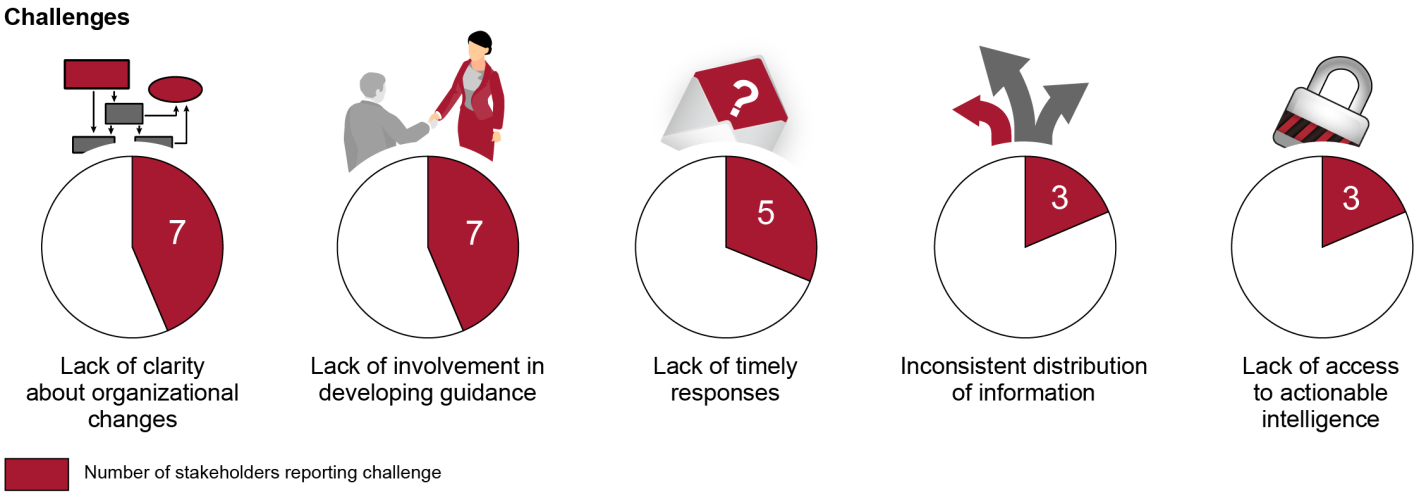
To implement the statutory requirements, CISA leadership launched an organizational transformation initiative. In March 2021, we reported that CISA had completed the first two of the three phases of its organizational transformation initiative.[23] Specifically, we noted DHS had not fully implemented its phase three transformation, which included finalizing the agency's mission-essential functions and completing workforce-planning activities by December 2020.

We also found that of 10 selected key practices for effective agency reforms we previously identified, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. Further, we reported on a number of challenges that selected government and private sector stakeholders had noted when coordinating with CISA, including a lack of clarity surrounding its organizational changes and the lack of stakeholder involvement in developing guidance. Although CISA had activities under way to mitigate some of these challenges, it had not developed strategies to, among other things, clarify changes to its organizational structure. Figure 2 below describes the coordination challenges identified by private-sector stakeholders.

[22]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2,132 Stat. 4168, 4169, (codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[23]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).

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



Source: GAO analysis of stakeholder interviews. | GAO-22-105973

To address these weaknesses, we made 11 recommendations to DHS. The department concurred with our recommendations and, as of September 2021, reported that it intends to fully implement them by the end of calendar year 2022. Implementing these recommendations will better position CISA to ensure the success of its reorganization efforts and carry out its mission to lead national efforts to identify and respond to cyber and other risks to our nation's infrastructure.

Sector Risk Management Agencies Need to Ensure Effective Guidance and Support

Since 2010, we have made about 80 recommendations for various federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the NIST framework of voluntary cyber standards and correct sector-specific weaknesses. Specifically, we found that most sector risk management agencies were not collecting and reporting on improvements in the protection of critical infrastructure as a result of using the framework across the sectors.[24] We concluded that collecting and reporting on these improvements would help the sectors understand the extent to which sectors are better protecting their critical infrastructure from cyber threats.

[24]GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Apr. 9, 2020).

To address these issues, we made 10 recommendations—one to NIST on establishing time frames for completing selected programs—and nine to the lead agencies, to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. However, as of November 2021, none of the recommendations had been implemented. Until the lead agencies collect and report on improvements gained from adopting the framework, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructure from threats will be largely unknown. We reiterated these recommendations in a February 2022 report.[25]

We have also frequently reported on the need for lead agencies to enhance the cybersecurity of their related critical infrastructure sectors and subsectors—such as transportation systems, communications, energy, education, and financial services.[26]

CISA Should Improve its Priority Setting Efforts

CISA and Critical Infrastructure Stakeholders Do Not Find the NCIPP Useful

In our March 2022 report, CISA and other critical infrastructure stakeholders we spoke with told us that the NCIPP's results were of little use. In addition, the stakeholders raised concerns with the program,

[25]GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance,* GAO-22-105103 (Washington, D.C.: Feb. 9, 2022).

[26]GAO-21-288. See also GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, GAO-21-105263 (Washington, D.C.: July 27, 2021); GAO, *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices,* GAO-20-404 (Washington, D.C.: Apr. 3, 2020); GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, GAO-20-104462 (Washington, D.C.: Nov. 23, 2021); AO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019); GAO, *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021); 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); and 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).

which included the relevance of the program's criteria given the current threat environment, limited state participation, and lack of use among critical infrastructure stakeholders.[27]

Relevance of NCIPP criteria, given current threat environment. We reported in March 2022 that CISA and other stakeholders questioned the present-day relevance of the criteria for adding critical infrastructure to the NCIPP list. To be included on the NCIPP's Level 1 list (its highest consequence list), an asset's destruction or disruption must meet minimum specified consequence thresholds for at least two of the following four categories: economic loss, fatalities, mass evacuation length, and degradation of national security.[28]

Senior officials with CISA, as well as other federal, state, and private sector officials we spoke with said that the consequence thresholds for these criteria did not reflect the current threat environment, which focuses more on cyberattacks and extreme weather events. The threat environment also focuses on vulnerabilities or attacks that can affect multiple entities within a short period. In this scenario, the consequences related to a single asset, entity, system, or cluster may not reach NCIPP thresholds, but the aggregate impacts may be nationally significant, according to CISA officials.

Limited state participation. As part of the NCIPP process, we found in our March 2022 report that state homeland security agencies identify relevant critical infrastructure—both public and private—and nominate those assets for inclusion on the NCIPP list.[29] However, CISA data showed that since fiscal year 2017, no more than 14 states (of 56 states

[27]GAO-22-104279.

[28]CISA coordinates a voluntary effort with states and other partners to identify, prioritize, and categorize high-priority critical infrastructure as either Level 1 or Level 2 based on the possible consequences to the nation in terms of our factors—fatalities, economic loss, mass evacuation length, and degradation of national security. According to DHS, the overwhelming majority of the assets and systems identified through the NCIPP are categorized as Level 2. Only a small subset of assets meet the Level 1 consequence threshold—those whose loss or damage could result in major national or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001, attacks. The precise consequence thresholds for inclusion on the NCIPP list are information that DHS has designated as "for official use only." We did not include the specific thresholds in this report so that we could publically present the results of our work.

[29]GAO-22-104279.

and territories) provided new nominations or updates to the program in any given fiscal year.

Lack of use among critical infrastructure stakeholders. Critical infrastructure stakeholders, including Protective Security Advisors (PSAs) and Cybersecurity Advisor (CSAs),[30] we interviewed for our March 2022 report also questioned the NCIPP's usefulness.[31] These stakeholders noted that the data were not accurate, relevant, consistent, or reflective of infrastructure risk. For example:

- **PSAs and CSAs.** Three of the 12 PSAs and CSAs we spoke with reported using the NCIPP list to a limited degree when planning annual outreach to some facilities. However, these same officials (as well as the other nine we spoke with) all questioned the list's accuracy and relevance. For example, one CSA said that the current NCIPP list was missing key assets that needed protection because the current criteria to be included on the list were outdated.
- **Sector Risk Management Agencies.** None of the four Sector Risk Management Agency officials we contacted reported regularly using the NCIPP list.[32] Sector Risk Management Agency officials raised a number of issues with the results, leading them to not rely on the list for risk management purposes. For example, officials from one Sector Risk Management Agency said their department had a copy of the list, but it was generally not something they referred to regularly or used in

[30]CISA offers government (federal, state, local, tribal, and territorial), private sector, and other critical infrastructure stakeholders a suite of programs and services to identify and mitigate risks to infrastructure security. These include infrastructure and cybersecurity services, some of which are carried out by CISA's PSAs and CSAs. PSAs are operators with expertise in physical security protection, and CSAs are cybersecurity specialists responsible for helping to bolster owners' and operators' cybersecurity capabilities. Both types of advisors use their respective assessment tools to work with critical infrastructure stakeholders to help make critical infrastructure more resilient. CSAs and PSAs operate across CISA's 10 regions. CSAs and PSAs we interviewed were from Regions 2, 3, 4, 5, 7, and 8. We also interviewed the CISA Regional Coordinator from Region 10 for contextual information on the regional coordinator role; however, this interview is not included in our overall total number of regional stakeholder interviews, which include only the PSAs and CSAs.

[31]GAO-22-104279.

[32]Sector Risk Management Agencies we interviewed were the Department of Energy (energy sector), Environmental Protection Agency (water sector), and CISA (both the critical manufacturing and IT sectors).

their efforts. Officials felt that the types of infrastructure on the list were not consistent across regions.

- **State homeland security agencies.** Only one of the six state homeland security agencies we contacted reported regularly using the NCIPP list.[33] State homeland security agency officials questioned the list's accuracy, and most said that they did not use the list to inform risk communication or influence decisions.

Given the evolving risk landscape and CISA and the critical infrastructure community's recognition of the NCIPP's limitations, we made two recommendations to CISA regarding NCIPP: (1) that the agency improve its NCIPP process to better reflect current threats and (2) the agency should seek input from states that have not provided recent updates on identifying critical infrastructure. DHS concurred with the recommendations and described initial actions under way or planned in response to our report, with completion expected by September 2023.

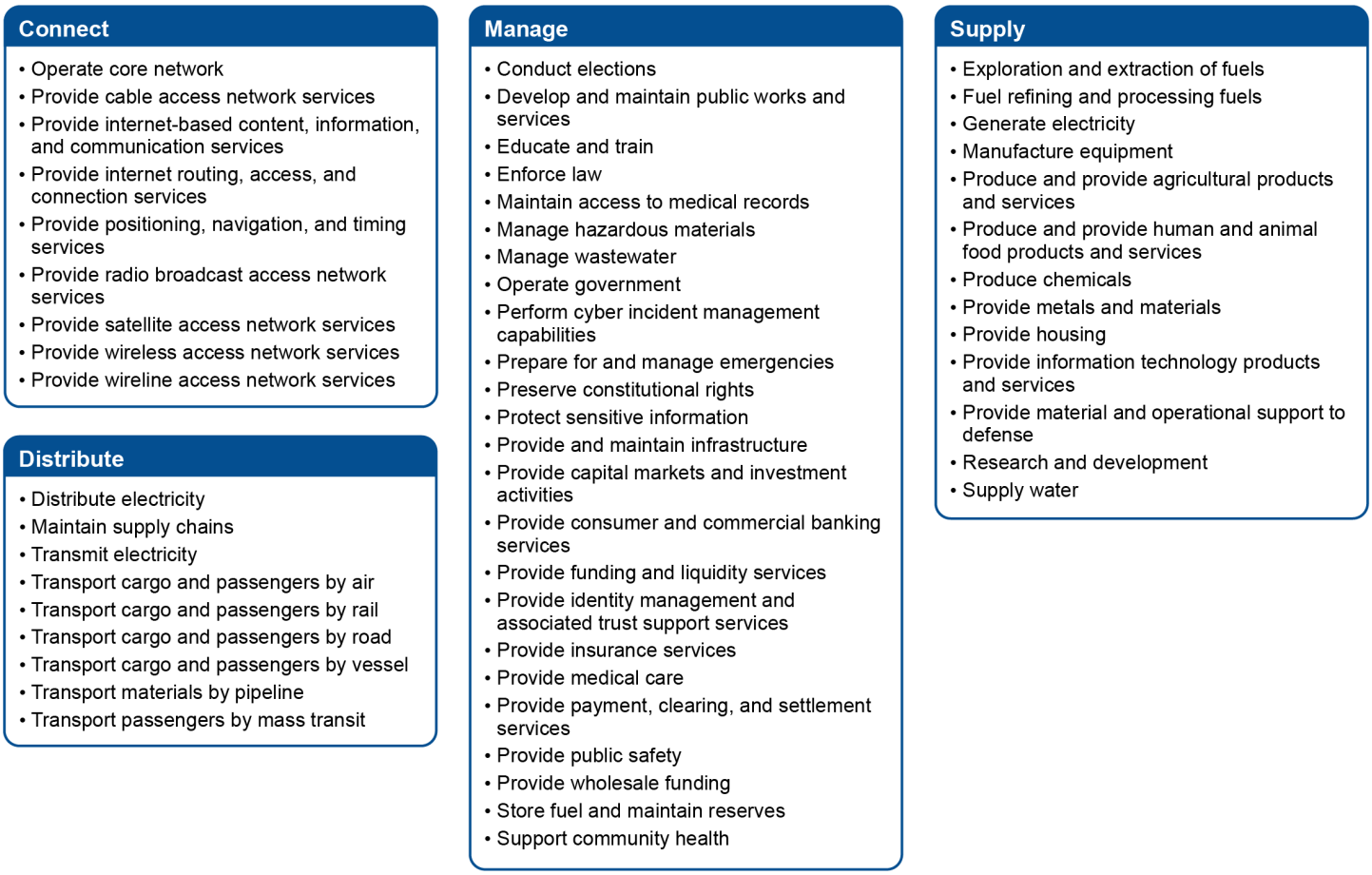
Limited Understanding of National Critical Functions Framework May Pose Challenges

We reported in March 2022 that CISA's National Risk Management Center published a set of 55 critical functions in spring 2019 as part of its new National Critical Functions framework.[34] According to CISA officials, since 9/11, the complexity and interdependency of critical infrastructure has expanded significantly. While the NCIPP has historically focused on protecting physical assets within the context of the 16 critical infrastructure sectors, primarily from acts of terrorism, the framework reflects a shift in risk management. The shift emphasizes resilience—maintaining and restoring the nation's essential services and customary conveniences—along with hazards and threats that are increasingly cross-cutting in nature, particularly around cybersecurity and natural disasters. The complete list of functions is shown in figure 3.

[33]One state homeland security official said that while data on the NCIPP was problematic, his state did refer to the NCIPP each year to inform the state's grant allocation methodology.

[34]GAO-22-104279.

Figure 3: Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions



Source: GAO analysis of CISA information. | GAO-22-105973

Seven of 25 critical infrastructure stakeholders we met with were aware of and supportive of CISA's new direction and had positive feedback on the National Critical Functions; however, most of the federal and nonfederal critical infrastructure stakeholders we interviewed reported being generally uninvolved with, unaware of, or not understanding the goals of the framework. Specifically, stakeholders did not understand how the framework related to prioritizing infrastructure, how it affected planning and operations, or where their particular organizations fell within the framework.

For example, eight of the 25 officials we interviewed said that communication from CISA headquarters regarding the National Critical

Functions framework needed improvement. Industry officials from one of the four sectors we met with said that their sector's members were trying to cooperate with CISA and provide data when CISA requested it but said that the requests were often broad or their goals unclear. Officials from one state homeland security agency said that CISA often shares complex and academic presentations about sophisticated risk modeling and visualizations; however, officials said they felt those presentations were too complicated and, therefore, they did not know how they were supposed to use the information.

Five of six CISA regional CSAs—who are responsible for reducing cybersecurity risks to the nation's critical infrastructure—were also not using or did not understand how the National Critical Functions would affect their stakeholders, despite some of the functions having a cyber and IT focus. For example, one advisor said that they and their stakeholders—organizations for which he provides cybersecurity assessments—are bombarded with information. The advisor stated that they have not had time to understand the National Critical Functions framework, which they believed was more focused on physical security, rather than cybersecurity. The PSA and CSA in one region said that there was no prioritization within the 55 critical functions, making everything equally critical. Accordingly, the officials said they did not have a clear sense of what they—or DHS broadly—should prioritize. In response, CISA officials stated that stakeholders with local operational responsibilities were the least likely to be familiar with the National Critical Functions. These functions were conceived to improve the analysis and management of cross-sector and national risks. Still, CISA officials acknowledged the need to improve connection between the National Critical Functions framework and local and operational risk management activities and communications.

As we stated in our March 2022 report, helping to ensure that stakeholders understand the goals of the framework and are involved in its implementation could aid CISA in its future infrastructure protection efforts.[35] We therefore recommended that CISA ensure that stakeholders are fully engaged in the implementation of the National Critical Functions framework. DHS concurred with the recommendation and described initial actions under way or planned in response to our report, with estimated completion by October 2022.

[35]GAO-22-104279.

In summary, cyberattacks, physical attacks, and other threats facing the nation's critical infrastructure require an effective and coordinated public-private response. CISA has undertaken a wide range of efforts to identify and prioritize nationally significant critical infrastructure. However, as our previously reported findings and recommendations indicate, urgent action is needed and CISA should take steps to improve and further these efforts. By taking steps to ensure that is process for identifying and prioritizing critical infrastructure accounts for current threats and meets the needs of all states, CISA and its partners could have a more relevant and useful understanding of critical infrastructure risk.

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

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 included Kevin Walsh (Director), Ben Atwater (Assistant Director), Eric Hauswirth, Susan Hsu, Stephen Komadina, Susannah Kuebler, Tracey King, Kush Malhotra, Jan Montgomery, and Umesh Thakkar.

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