



March 2022

CRITICAL INFRASTRUCTURE PROTECTION

CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing

GAO Highlights

Highlights of [GAO-22-104279](#), a report to congressional requesters

Why GAO Did This Study

The risk environment for critical infrastructure ranges from extreme weather events to physical and cybersecurity attacks. The majority of critical infrastructure is owned and operated by the private sector, making it vital that the federal government work with the private sector, along with state, local, tribal, and territorial partners. CISA is the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts.

GAO was asked to review CISA's critical infrastructure prioritization activities. This report examines (1) the extent to which the National Critical Infrastructure Prioritization Program currently identifies and prioritizes nationally significant critical infrastructure, (2) CISA's development of the National Critical Functions framework, and (3) key services and information that CISA provides to mitigate critical infrastructure risks.

GAO analyzed agency documentation and conducted interviews with critical infrastructure stakeholders representing the energy, water and wastewater systems, critical manufacturing, and information technology sectors; six of 10 CISA regions; and six states to understand the need for any improvements to CISA's efforts, among other things. GAO selected these six states based on population size and the amounts of grant awards received from DHS's State Homeland Security Program.

View [GAO-22-104279](#). For more information, contact Tina Won Sherman at (202) 512-8461 or shermant@gao.gov.

March 2022

CRITICAL INFRASTRUCTURE PROTECTION

CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing

What GAO Found

Through the National Critical Infrastructure Prioritization Program, the Cybersecurity and Infrastructure Security Agency (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, the program works to annually update and prioritize the list. The program's list is used to inform the awarding of preparedness grants to states. However, 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 identified cyberattacks as among the most prevalent threats they faced but said that the program's list was not reflective of this threat. Further, according to CISA data, since fiscal year 2017, no more than 14 states (of 56 states and territories) provided updates to the program in any given fiscal year. Ensuring that its process for determining priorities reflects current threats, such as cyberattacks, and incorporates input from additional states would give CISA greater assurance that it and stakeholders are focused on the highest priorities.

In 2019, CISA published a set of 55 critical functions of government and the private sector considered vital to the security, economy, and public health and safety of the nation. According to CISA officials, this new National Critical Functions framework is intended to better assess how failures in key systems, assets, components, and technologies may cascade across the 16 critical infrastructure sectors. Examples of critical functions are shown below in CISA's four broad categories of "connect" (nine of the 55 functions), "distribute" (nine), "manage" (24), and "supply" (13).

Examples of Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions

Connect	Distribute	Manage	Supply
<ul style="list-style-type: none">• Provide positioning, navigation, and timing services• Provide satellite access network services• Provide wireless access network services	<ul style="list-style-type: none">• Distribute electricity• Maintain supply chains• Transport materials by pipeline	<ul style="list-style-type: none">• Manage wastewater• Perform cyber incident management capabilities• Protect sensitive information	<ul style="list-style-type: none">• Manufacture equipment• Produce and provide human and animal food products and services• Supply water

Source: GAO analysis of CISA information. | [GAO-22-104279](#)

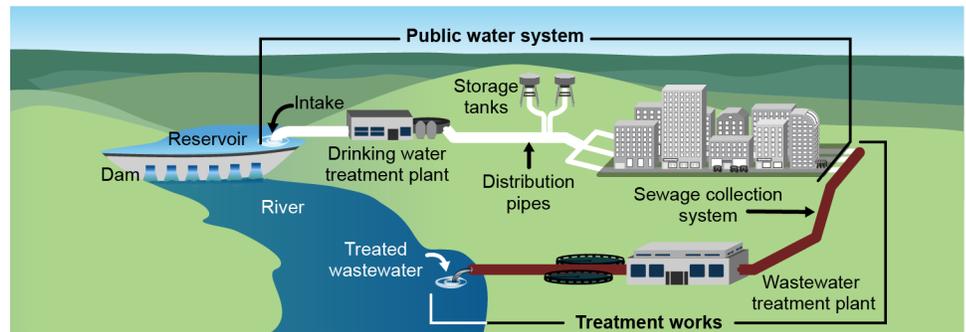
CISA is currently carrying out a process to break down each of the 55 national critical functions (such as "supply water") into systems (such as "public water systems") and assets (including infrastructure such as "water treatment plants"), as illustrated below.

What GAO Recommends

GAO recommends that CISA take the following six actions and DHS concurred:

- improve its process for identifying critical infrastructure priorities to better reflect current threats;
- seek input from states that have not provided recent updates on identifying critical infrastructure;
- involve stakeholders in the development of the National Critical Functions framework;
- document goals and strategies for the National Critical Functions framework;
- improve efforts to coordinate cybersecurity services; and
- share regionally specific threat information.

Examples of Critical Infrastructure Systems and Assets That Support the National Critical Function “Supply Water”



Source: GAO (graphic) and U.S. Environmental Protection Agency and Department of Homeland Security (information). | GAO-22-104279

CISA plans to integrate the National Critical Functions framework into broader prioritization and risk management efforts, and has already used it to inform key agency actions. For example, CISA used the framework to analyze the impact of COVID-19 on critical infrastructure. Although CISA initiated the functions framework in 2019, most of the federal and nonfederal critical infrastructure stakeholders that GAO 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 it. In response, CISA officials stated that stakeholders with local operational responsibilities were the least likely to be familiar with the National Critical Functions, which were intended 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. In addition, CISA lacks an available documented framework plan with goals and strategies that describe what it intends to achieve and how. Without such a documented plan, stakeholders' questions regarding the framework will likely persist.

CISA offers physical and cybersecurity assessments to critical infrastructure partners, but the agency's 2020 reorganization resulted in challenges in communicating and coordinating the delivery of some cybersecurity services. According to regional staff, their ability to effectively coordinate the cybersecurity services that CISA headquarters delivered was impaired because of staff placement following the reorganization. Specifically, staff conducting outreach and offering a suite of cybersecurity assessments to critical infrastructure stakeholders are located in regional offices, while CISA offers additional cyber assessment services using staff from a different division—the Cybersecurity Division—which operates out of headquarters. Addressing these communication and coordination challenges can improve CISA's cybersecurity support.

CISA analyzes and shares threat information related to critical infrastructure; however, stakeholders reported needing more regionally specific information to address those threats. For instance, selected stakeholders that GAO spoke to said that CISA's threat information helped them to understand the broader threat landscape, such as threats to election security and COVID-19 response efforts. Almost half (12 of 25) of the stakeholders reported needing additional information related to the threats specific to their regions and local infrastructure. Specifically, stakeholders told us that organizations in their regions were primarily concerned with active shooters, chemical spills, or biological attacks and, thus, needed information that was applicable to those threats.

View [GAO-22-104279](#). For more information, contact Tina Won Sherman at (202) 512-8461 or shermant@gao.gov.

Contents

Letter		1
	Background	7
	CISA and Critical Infrastructure Stakeholders Do Not Find the NCIPP Useful	16
	Limited Understanding of National Critical Functions Framework May Pose Challenges	25
	CISA Cyber Services and Threat Information Sharing Lack Regional Focus	33
	Conclusions	41
	Recommendations for Executive Action	42
	Agency Comments and Our Evaluation	43
Appendix I	Critical Infrastructure Sectors and Their Sector Risk Management Agencies	47
Appendix II	Examples of Selected Department of Homeland Security Critical Infrastructure Prioritization Processes	48
Appendix III	Comments from the Department of Homeland Security	49
Appendix IV	GAO Contacts and Staff Acknowledgments	54
Tables		
	Table 1: States Providing New Nominations and Updates to the National Critical Infrastructure Prioritization Program, by Fiscal Year (FY)	18
	Table 2: Examples of National Critical Functions Affected by the 2021 Colonial Pipeline Company Cyberattack	30
	Table 3: Examples of Cybersecurity and Infrastructure Security Agency (CISA) Security Assessments and Numbers of Assessments Conducted in Fiscal Year (FY) 2020	34
	Table 4: Cybersecurity and Information Security Agency (CISA) Intelligence and Threat Information Sharing	39

Table 5: Selected Department of Homeland Security (DHS) Critical Infrastructure Identification Processes and Results	48
---	----

Figures

Figure 1: Examples of Critical Infrastructure	7
Figure 2: Selected Critical Infrastructure Sectors and Their Sector Risk Management Agencies	8
Figure 3: Cybersecurity and Infrastructure Security Agency (CISA) Select Divisions and Responsibilities	10
Figure 4: Cybersecurity and Infrastructure Security Agency (CISA) Regions and Regional Office Locations	12
Figure 5: Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions	15
Figure 6: Examples of Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions	26
Figure 7: Examples of Critical Infrastructure Systems and Assets That Support the National Critical Function “Supply Water”	27
Figure 8: Cybersecurity and Infrastructure Security Agency (CISA) Selected Activities for the National Critical Functions Framework	28
Figure 9: Critical Infrastructure Sectors and Their Sector Risk Management Agencies	47

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
CSA	Cybersecurity Advisor
DHS	Department of Homeland Security
DOE	Department of Energy
FEM	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
GCC	Government Coordinating Council
GPRAMA	GPRA Modernization Act of 2010
IT	Information Technology
NCIPP	National Critical Infrastructure Prioritization Program
PSA	Protective Security Advisor
SCC	Sector Coordinating Council

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.



March 1, 2022

Congressional Requesters

The nation's critical infrastructure consists of physical and cyber assets and systems that are so vital to the United States that their incapacity or destruction could have a debilitating impact on national security, public health and safety, or the economy.¹ 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.

The risk environment for critical infrastructure ranges from natural hazards to cyberattacks, including acts of terrorism and insider threats from witting or unwitting employees. Companies that own or operate critical infrastructure have increasingly sought to gain efficiencies by connecting their physical and cyber systems, and the convergence between these assets and systems creates new opportunities for potential attackers.

For instance, the 2021 cyberattack on the Colonial Pipeline Company—which led to the temporary disruption of gasoline and other petroleum product delivery across much of the southeast United States—illustrated how the nation's critical infrastructure assets and systems are often interconnected with other systems and the internet, making them more vulnerable to attack. Because the majority of critical infrastructure is owned and operated by the private sector, it is vital that the public and private sectors work together to protect these assets and systems.

The Department of Homeland Security (DHS) coordinates the overall federal effort for national critical infrastructure protection and has stated that prioritizing available resources to the most critical infrastructure can enhance our nation's security, increase resiliency, and reduce risk.² As part of its responsibilities, DHS conducts critical infrastructure risk assessments and integrates relevant information and analyses to identify

¹42 U.S.C. § 5195c(e).

²The 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.

priorities for protective measures. DHS and other federal agencies; state, local, tribal, and territorial agencies and authorities; and the private sector may implement these measures. The Cybersecurity and Infrastructure Security Agency Act of 2018 established the Cybersecurity and Infrastructure Security Agency (CISA) as an operational component agency within DHS.³ As the lead federal agency responsible for coordinating the national effort to understand and manage risk to critical infrastructure, CISA has a critical responsibility to effectively coordinate and consult with its federal, state, local, territorial, tribal, and private sector partners.

Our prior work has identified DHS actions to identify and assess risk to critical infrastructure. For example, we reported in 2013 that DHS changed the National Critical Infrastructure Prioritization Program (NCIPP) list of the nation's highest-priority critical infrastructure to make the list entirely consequence based—that is, based on the effects that an event would have on public health and safety, the national economy, or other areas. However, DHS had not identified the impact of those changes on users nor validated its approach. We recommended that DHS commission an external peer review of its approach, which DHS did.⁴

In 2014, we reported that DHS offices and components conducted or required thousands of critical infrastructure vulnerability assessments, but that DHS needed to enhance the integration and coordination of these efforts.⁵ DHS implemented five of the six recommendations in our report, including our recommendation to better coordinate vulnerability assessments within DHS and other critical infrastructure partners. In October 2017, we also reported that DHS assesses each of the three elements of risk—threat, vulnerability, and consequence—for the sectors

³Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2, 132 Stat. 4168 (codified as amended at 6 U.S.C. § 652). Since its establishment, CISA has been reorganizing offices and functions previously organized under the department's National Protection and Programs Directorate and aligning 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).

⁴GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, [GAO-13-296](#) (Washington, D.C.: Mar. 25, 2013).

⁵GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, [GAO-14-507](#) (Washington, D.C.: Sept. 15, 2014).

we reviewed and that these assessments helped infrastructure owners and operators take action to improve security and mitigate risks.⁶

You asked us to review CISA's efforts to identify and prioritize critical infrastructure. This report addresses

1. the extent to which CISA's National Critical Infrastructure Prioritization Program identifies nationally significant critical infrastructure and what changes to the program, if any, are needed;
2. CISA's development of and stakeholders' perspectives on the National Critical Functions framework; and
3. what key services and information CISA provides to mitigate critical infrastructure risks, and the extent to which the services and information meet stakeholder needs.

Our review addresses these questions with a focus on two of CISA's methodologies for identifying nationally significant critical infrastructure – the NCIPP and the National Critical Functions framework. We selected the NCIPP because it is a long-standing asset-based critical infrastructure prioritization model with direct ties to FEMA's multi-billion dollar Homeland Security Grant Programs. We selected the NCF framework because it represents CISA's new approach to risk analysis and critical infrastructure prioritization.

For all three questions, we focused our review on four critical infrastructure sectors—energy, water and wastewater systems (water), critical manufacturing, and information technology (IT). To select these sectors, we reviewed CISA's *Guide to Critical Infrastructure Security and Resilience* and DHS's *Sector Risk Snapshots* and determined that these four sectors and their associated functions were strongly represented among CISA's list of National Critical Functions. CISA defines these as functions of 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. CISA has also designated two of the four sectors (energy and water) as "lifeline sectors" or "lifeline functions," meaning that their reliable operations are so critical that a

⁶GAO, *Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning*, [GAO-18-62](#) (Washington, D.C.: Oct. 30, 2017).

disruption or loss of one of these functions would directly affect the security and resilience of critical infrastructure within and across numerous sectors.⁷ The information we gathered is not generalizable to all 16 critical infrastructure sectors but does provide insight into how DHS identifies and prioritizes critical infrastructure and the key services and information that CISA provides to mitigate risks as part of all three objectives.⁸ From these four sectors, we met with officials from the federal Sector Risk Management Agency. This agency is a federal department or agency designated by law or presidential directive with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in an all hazards environment in coordination with DHS.⁹ Specifically, we met with officials from the Department of Energy (energy sector); Environmental Protection Agency (water sector); and CISA (for both critical manufacturing and IT sectors). We met with other relevant federal agencies, including the Federal Energy Regulatory Commission (FERC), on the basis of its role in the energy sector; and the Federal Emergency Management Agency (FEMA), on the basis of its use of CISA risk information and support of critical infrastructure stakeholders.¹⁰

In addition to the four Sector Risk Management Agency officials noted above, to address all three questions we interviewed a sample of federal and nonfederal critical infrastructure stakeholders. For each selected sector, we met with officials from a relevant sector coordinating council or industry association, which included owner-operators of critical assets and members of their respective trade associations. We interviewed one

⁷The four lifeline functions are transportation, water, energy, and communications.

⁸The 16 critical infrastructure sectors are 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.

⁹See 6 U.S.C. § 651(5). Sector Risk Management Agency responsibilities include the requirements to conduct sector specific risk assessments, coordinate with the department on national risk assessments, and provide the Director of CISA with critical infrastructure information on an annual basis. See 6 U.S.C. § 665d.

¹⁰FERC is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FEMA, within DHS, is part of a larger team of federal agencies; state, local, tribal, and territorial governments; and nongovernmental stakeholders that share responsibility for emergency management and national preparedness.

CISA Protective Security Advisor (PSA) and one Cybersecurity Advisor (CSA) from each of the six out of 10 CISA regions we selected, for a total of 12 interviews.¹¹ Our selected regions covered 31 states, two U.S. territories, and the District of Columbia, and are home to an estimated 70 percent of the U.S. population, as of July 1, 2019. These regions were selected to represent diversity in state population size, critical infrastructure (e.g., unique clusters of energy production, food production, manufacturing, etc.), and geography (e.g., coastal, interior). The results of our interviews with PSAs and CSAs are not generalizable; however, they represent more than half of CISA's regions and provide useful insights on critical infrastructure prioritization efforts. Last, we interviewed state homeland security agency officials from five states—Colorado, Florida, Illinois, Texas, and Washington—and obtained written responses to our questions from California. We selected a mix of large- and medium-sized states with the highest levels of criticality within their respective CISA regions, based on their populations and the amount of grant awards received from FEMA's State Homeland Security Program.¹² Though the information we obtained is not generalizable to all states, it provided a range of state perspectives. Further, our state selection complemented our CISA regional selection, ensuring that we were able to interview officials from states outside our selection of CISA regions and, thus, to broaden the range of national views we obtained.

To evaluate the extent to which CISA's NCIPP identifies nationally significant critical infrastructure and whether changes to the program were needed, we obtained and analyzed infrastructure counts from NCIPP lists finalized for fiscal years 2017 through May 2021. We used those lists to determine the total number of high-priority (Level 1 and Level 2) assets by state and the change in distribution of high-priority assets from year to year. We used these data to determine the extent to which states provided updates to the program and the extent to which the number of assets on the lists has changed over time. We reviewed documentation, including CISA's guidance for nominating assets to the

¹¹CSAs 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.

¹²DHS uses the population of each state, among other data, to allocate State Homeland Security Program and Urban Areas Security Initiative program grant funds - states with larger populations represent a greater degree of criticality and receive higher amounts of funding.

NCIPP list, and discussed quality assurance procedures with CISA officials. We determined that the data were sufficiently reliable to describe the number of states that submitted data for the NCIPP list. Last, we interviewed officials from a sample of federal and nonfederal critical infrastructure stakeholders, identified above, to discuss their roles in the NCIPP.

To describe CISA's development of the National Critical Functions framework, we obtained and reviewed documentation on CISA's processes for developing the National Critical Functions framework, including documentation of CISA's outreach to the critical infrastructure community. We compared these efforts with criteria set forth in the 2013 National Infrastructure Protection Plan (National Plan).¹³ Last, we interviewed officials from a sample of federal and nonfederal critical infrastructure stakeholders, identified above, to discuss their roles in critical infrastructure identification and prioritization and their views on CISA's current efforts.

To evaluate the key services and information that CISA provides to mitigate risks to critical infrastructure, and the extent to which this support has met stakeholder needs, we examined DHS policies and guidance related to administering critical infrastructure security services and obtained information from CISA officials to determine how they prioritize providing services and outreach. In addition, we reviewed prior GAO reports and DHS Office of Inspector General reports to identify any challenges that CISA has faced in providing security services and critical infrastructure information. We interviewed critical infrastructure stakeholders, as described above, to gather views on CISA support. We also met with officials from CISA's National Risk Management Center, Integrated Operations Division, and the Cybersecurity Division to understand their processes for coordinating and providing security services and information to the regions. Additionally, we compared CISA's efforts to support critical infrastructure stakeholders with

¹³Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, D.C.: December 2006). DHS updated the 2006 National Plan in January 2009 to include greater emphasis on resiliency; and *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). DHS updated the 2009 *National Infrastructure Protection Plan* in December 2013 to emphasize the integration of physical and cybersecurity into the risk management framework: *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

applicable coordination criteria in the National Plan and relevant statutory provisions.¹⁴

We conducted this performance audit from September 2020 to February 2022 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

Critical Infrastructure, Sectors, and Agency Partnerships

The nation's critical infrastructure (examples of which are shown in fig. 1) refers to the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of them would have a debilitating impact on U.S. security, economic stability, public health or safety, or any combination of these factors.¹⁵

Figure 1: Examples of Critical Infrastructure



Source: (L to R) anekoho/stock.adobe.com, Sergiy Serdyuk/stock.adobe.com, yelantsev/stock.adobe.com, Federico Rostagno/stock.adobe.com. | GAO-22-104279

Federal law and policy establish roles and responsibilities for protecting critical infrastructure. Presidential Policy Directive 21 and federal law describe Sector Risk Management Agencies (formerly known as Sector-Specific Agencies) in the public sector as the federal departments or agencies, designated by law or presidential directive, that are responsible

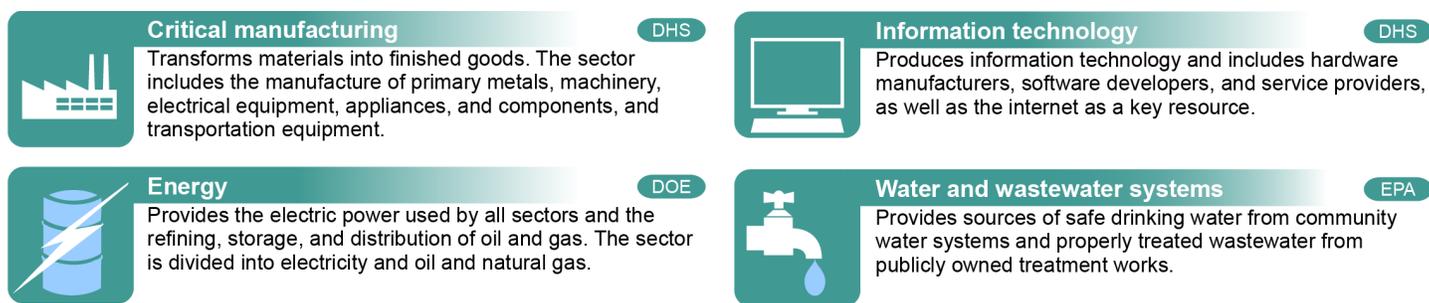
¹⁴Department of Homeland Security, *2013 National Infrastructure Protection Plan*.

¹⁵42 U.S.C. § 5195c(e).

for providing institutional knowledge and specialized expertise.¹⁶ The Sector Risk Management Agencies are to lead, facilitate, and support the security and resilience programs and associated activities of their designated critical infrastructure sectors in an all hazards environment in coordination with DHS, among other duties.

The directive identified 16 critical infrastructure sectors and designated the nine associated Sector Risk Management Agencies, which are listed in appendix 1. Figure 2 lists the four sectors we reviewed for this report and their respective Sector Risk Management Agencies.

Figure 2: Selected Critical Infrastructure Sectors and Their Sector Risk Management Agencies



Sector-specific agency

DOE Department of Energy **DHS** Department of Homeland Security **EPA** Environmental Protection Agency

Sources: GAO analysis of Presidential Policy Directive-21 and Department of Homeland Security, 2013 *National Infrastructure Protection Plan*; Art Explosion (clip art). | GAO-22-104279

As part of the partnership structure, each sector has a government coordinating council, consisting of representatives from various levels of government, and a sector coordinating council (SCC), consisting of owner-operators of critical assets and members of relevant trade associations. The National Plan describes the voluntary partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. It provides a framework for

¹⁶The White House, Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: February 2013). 6 U.S.C. § 651(5). After enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Sector-Specific Agencies became known as Sector Risk Management Agencies. Pub. L. No. 116-283, § 9002(a)(7).

developing and implementing a coordinated national effort to protect critical infrastructure within the 16 critical infrastructure sectors.¹⁷

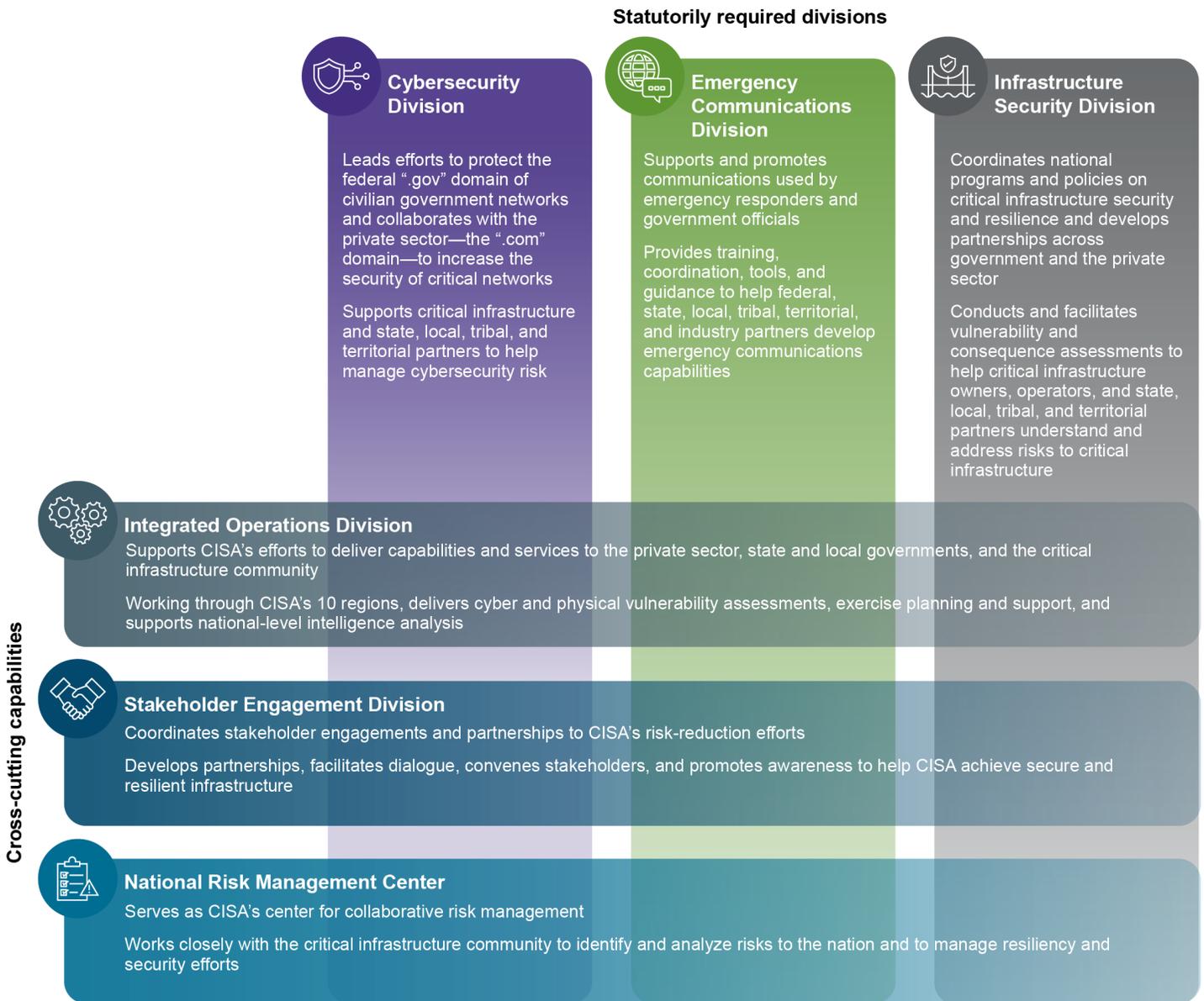
CISA Organizational Structure

Since the passage of the Cybersecurity and Infrastructure Security Agency Act of 2018 and an ongoing reorganization effort, CISA has developed an organizational structure that includes three statutorily defined divisions, as well as 10 regional offices.¹⁸ Under this structure, each CISA regional office works with the organizations in its geographic area to deliver resources and services. Multiple divisions and offices within CISA headquarters carry out the agency's critical infrastructure protection programs, as described below in figure 3.

¹⁷Department of Homeland Security, *National Infrastructure Protection Plan*. DHS updated the 2006 *National Infrastructure Protection Plan* in January 2009 to include greater emphasis on resiliency: *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency*. DHS updated the 2009 *National Infrastructure Protection Plan* in December 2013 to emphasize the integration of physical and cybersecurity into the risk management framework: *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience*. CISA officials reported that, as of November 2021, the National Plan was in the process of being updated and will include references to the National Critical Functions.

¹⁸[GAO-21-236](#).

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

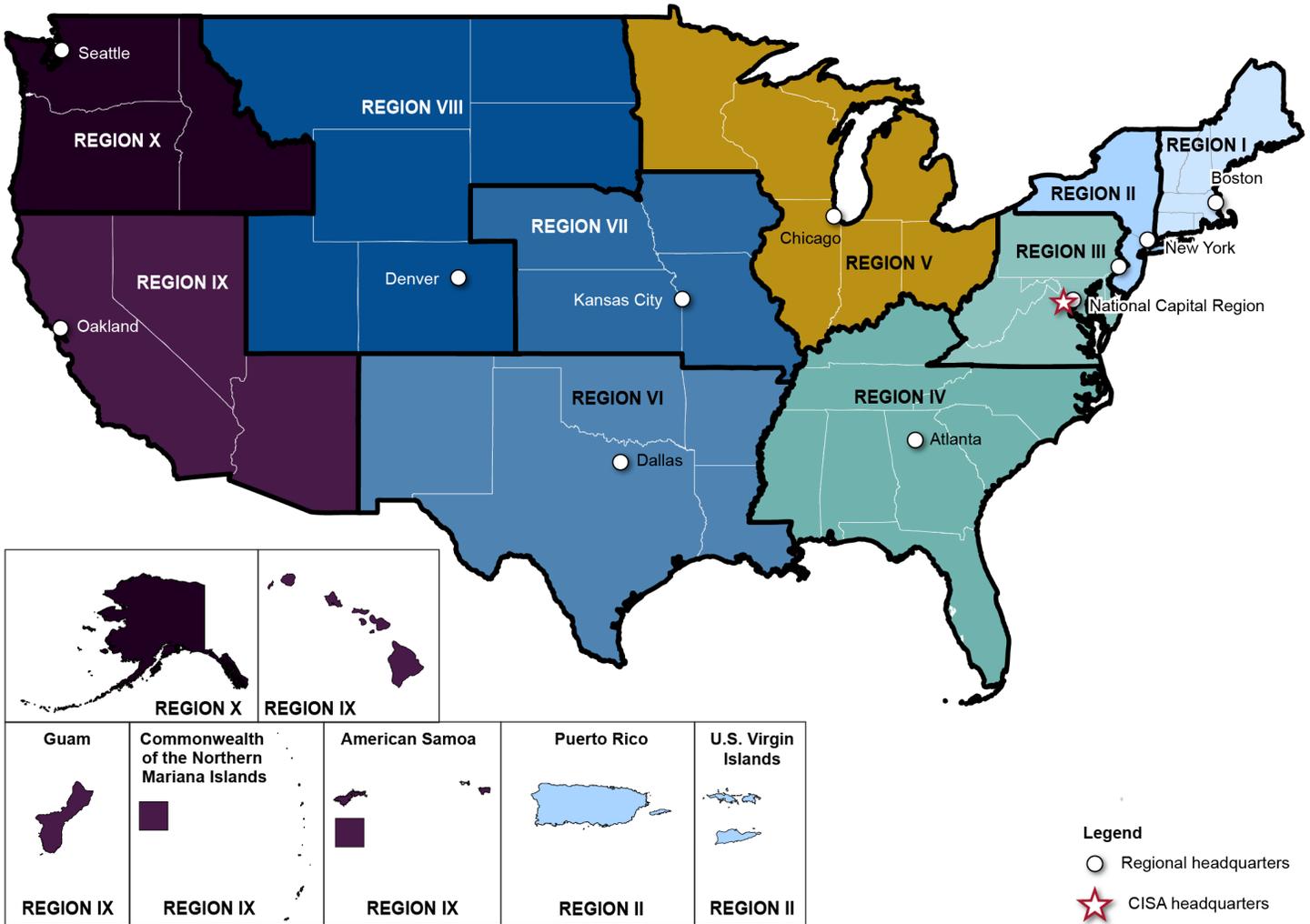


Sources: Department of Homeland Security, CISA. | GAO-22-104279

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.

For fiscal year 2020, the PSA program expended approximately \$38.5 million and had 127 staff, and the CSA program expended approximately \$21 million and had around 67 staff, according to CISA. PSAs and CSAs operate across all 50 states and U.S. territories, as illustrated in figure 4.

Figure 4: Cybersecurity and Infrastructure Security Agency (CISA) Regions and Regional Office Locations



Source: GAO analysis of CISA documentation. | GAO-22-104279

DHS and CISA Methods for Identifying and Prioritizing Critical Infrastructure

DHS and CISA use various processes to identify critical infrastructure, and these processes generally result in prioritized lists of infrastructure (e.g., bridges, power plants), information systems (e.g., federal IT systems or databases), or entities (e.g., private companies), technology elements and IT products and services. According to CISA officials, these lists are developed to support different risk management activities, such as understanding what needs to be prioritized for cybersecurity services following an incident. Different executive orders have required CISA to

identify the critical entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security and to identify critical infrastructure systems, networks, and assets most affected by an electromagnetic pulse event or attack.¹⁹ Examples of CISA critical infrastructure identification processes are listed in appendix II.

CISA also manages a national-level, multisector critical infrastructure identification effort—NCIPP. 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.²⁰ The NCIPP annually prioritizes critical infrastructure based on the consequences associated with the disruption or destruction of those assets.²¹ To conduct this work, 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

¹⁹Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013); Exec. Order No. 13,865, 84 Fed. Reg. 12,041 (Mar. 29, 2019).

²⁰According to NCIPP guidance, clusters or systems of critical infrastructure consist of two or more associated or interconnected assets or nodes that can be disrupted through a single event, resulting in regional or national consequences that meet the NCIPP criteria thresholds. An asset is a single facility with a fixed location that functions as a single entity (although it can contain multiple buildings or structures) and meets the NCIPP criteria by itself. A node is a single facility, similar to an asset, that does not meet the NCIPP criteria individually but does meet the criteria when grouped with other nodes or assets in a cluster or system. According to DHS, It recognized the need to identify clusters of critical infrastructure in 2008 after Hurricanes Gustav and Ike damaged a group of refineries that resulted in a nationally significant supply disruption of certain petrochemicals used across a wide range of industries.

²¹The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) amended Title II of the Homeland Security Act of 2002, requiring the Secretary of Homeland Security to establish and maintain a national database of systems and assets that the Secretary, in consultation with appropriate homeland security officials of the states, determine to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any state, or any local government, or as otherwise determined appropriate for inclusion by the Secretary. In addition, the 9/11 Commission Act required the Secretary of Homeland Security to establish and maintain a single prioritized list of systems and assets included in the national database that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects. The 9/11 Commission Act also required that DHS report annually to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on any significant challenges in compiling the database or list and, if appropriate, the extent to which the database or list has been used to allocate federal funds to prevent, reduce, mitigate, or respond to acts of terrorism. See 6 U.S.C. § 664.

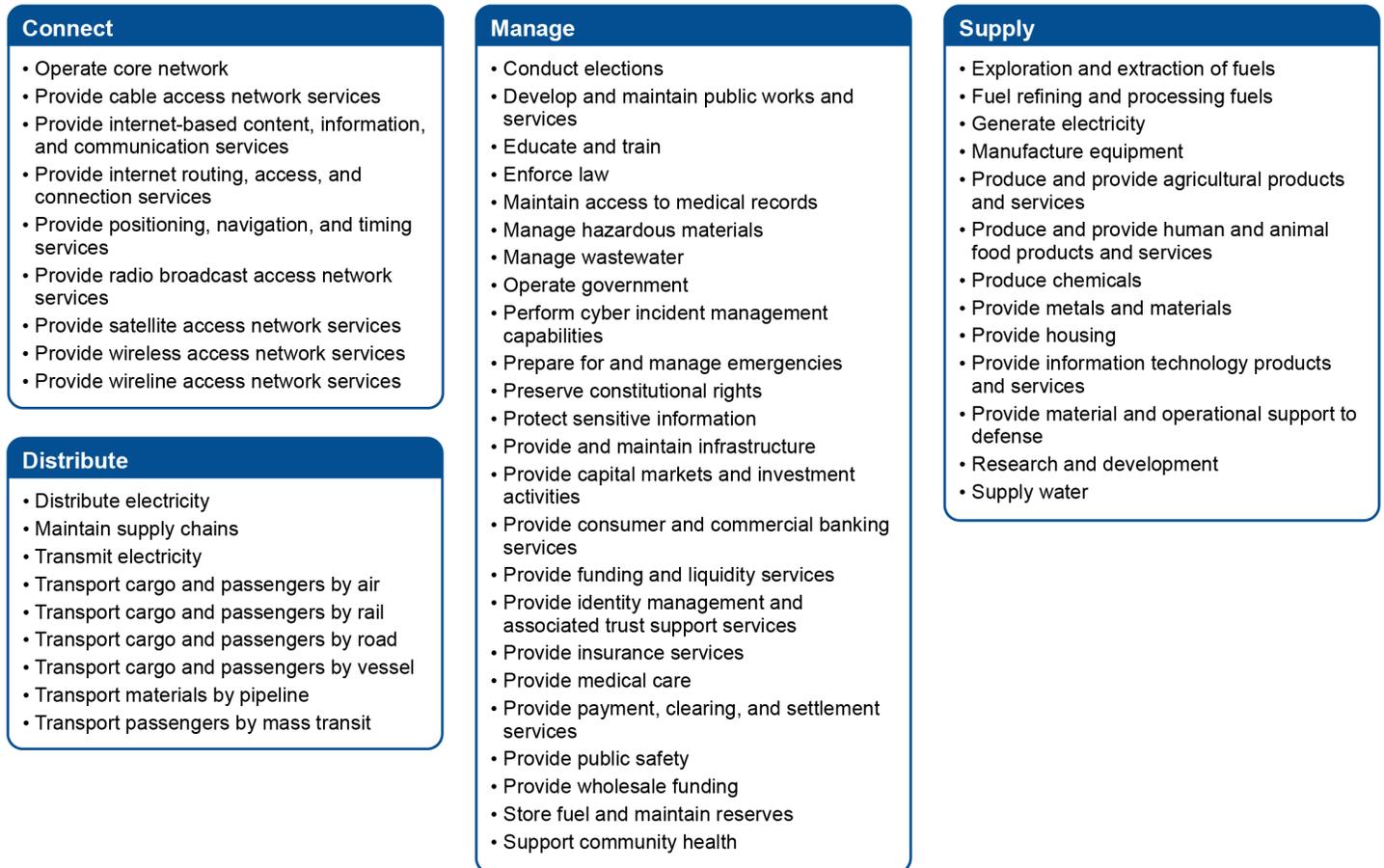
four factors—fatalities, economic loss, mass evacuation length, and degradation of national security. According to DHS, the overwhelming majority of the assets and systems identified through the NCIPP are categorized as Level 2. Only a small subset of assets meet the Level 1 consequence threshold—those 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.

National Critical Functions Framework

In 2019, CISA published its initial set 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. According to CISA, the National Critical Functions framework will be used to better assess how failures in key systems, assets, components, and technologies may cascade across the 16 critical infrastructure sectors and impact the nation. The framework is also intended to enable a richer understanding of how various entities, assets and technologies—such as electric facilities, banks, communications hubs, and managed service providers—come together to support critical functions.

The National Critical Functions includes government and nongovernmental functions such as “distribute electricity,” “provide medical care,” and “produce and provide agricultural products and services.” The complete list of functions is shown in figure 5.

Figure 5: Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions



Source: GAO analysis of CISA information. | GAO-22-104279

CISA and Critical Infrastructure Stakeholders Do Not Find the NCIPP Useful

CISA and Critical Infrastructure Stakeholders Expressed Concerns about the NCIPP's Relevance and Usefulness

The NCIPP serves as a prioritized list of systems and assets that the Secretary of Homeland Security has determined would cause national or regional catastrophic effects if they were to be destroyed or disrupted; however, CISA and other critical infrastructure stakeholders we spoke with reported that the program's results are presently of little use and raised concerns with the program.²² These concerns included the relevance of the program's criteria given the current threat environment, limited state participation, and lack of use among critical infrastructure stakeholders.

²²The 9/11 Commission Act required the Secretary of Homeland Security to establish and maintain a single prioritized list of systems and assets in a national database that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects. See 6 U.S.C. § 664.

Critical Infrastructure Threat: Cyberattacks

Cyberattacks are designed to damage or disrupt critical infrastructure that delivers vital services, such as electricity or financial services.

Cyber-attackers can target information technology, such as the software that underpins business functions.

Cyber-attackers can also target operational technology, such as control systems designed to operate physical processes like petroleum transportation.



Sources: The President's National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017); stock.adobe.com/christian42 (photo). | GAO-22-104279

Relevance of NCIPP criteria, given current threat environment. CISA and other stakeholders questioned the present-day relevance of the criteria for adding 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.²³

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 threat environment today, 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.

Twenty of the 25 critical infrastructure stakeholders we met with said that cyberattacks (including ransomware attacks) from inside actors, foreign adversaries, and others were among the most prevalent threats that they faced. Officials reported experiencing cyberattacks on hospitals, education systems, water treatment facilities, government agencies, and private companies. IT sector stakeholders we met with said that cyberattacks were increasing in frequency, sophistication, and scale. Homeland security officials from one state agency noted that the threat of cyberattacks touched every critical infrastructure sector in their state. For instance, a 2018 ransomware attack on a state agency was severe enough for officials to designate it as a statewide disaster—a designation usually reserved for a major fire or flood.

In addition to citing cyberattacks, critical infrastructure stakeholders cited extreme weather events (e.g., more severe and frequent flooding, fires, and hurricanes) as another major threat that they faced. Thirteen of the 25 federal and nonfederal critical infrastructure partners we met with identified extreme weather events as a major threat, with several stakeholders noting that weather events, such as hurricanes and floods, can affect multiple critical infrastructure sectors.

²³The 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.

Critical Infrastructure Threat: Extreme Weather Events

More frequent and intense extreme weather and other risks associated with climate change can affect critical infrastructure, including electricity generation, transmission, and distribution.

For example, in February 2021, extreme cold weather that spread from the Canadian border as far south as Texas caused record winter demand for electricity and left about 4.5 million customers in Texas without power, along with about 376,000 customers in Louisiana and Oklahoma.



Sources: GAO; Federal Emergency Management Agency (photo). | GAO-22-104279

We have previously reported that in 2018 alone, 14 separate billion-dollar weather and climate disaster events occurred across the United States, with total costs of at least \$91 billion, including the loss of public and private property.²⁴ However, officials representing the water sector said that the NCIPP list was not useful when preparing for a major 2017 hurricane because it did not account for the interdependencies of certain infrastructure. Specifically, officials said the NCIPP list did not consider how high-risk assets (such as a major hospital) were critically dependent on assets that were not represented on the NCIPP list (such as a water system, because if the hurricane were to disrupt the water system, the hospital would need to be evacuated). Given these limitations, the official said that the water sector generally disregarded the NCIPP list.

Limited state participation. As part of the NCIPP process, state homeland security agencies identify relevant critical infrastructure—both public and private—and nominate those assets for inclusion on the NCIPP list. However, CISA data showed that since fiscal year 2017, no more than 14 states (of 56 states and territories) provided new nominations or updates to the program in any given fiscal year, as shown below in table 1.

Table 1: States Providing New Nominations and Updates to the National Critical Infrastructure Prioritization Program, by Fiscal Year (FY)

States	FY 2017	FY 2018	FY 2019	FY 2020 ^a	FY 2021
1. Arkansas	—	—	—	—	•
2. Arizona	—	—	—	—	•
3. California	•	•	•	—	•
4. Colorado	—	—	•	•	—
5. Florida	•	—	—	—	—
6. Georgia	—	—	—	—	•

²⁴GAO, *Climate Resilience: A Strategic Investment Approach for High-Priority Projects Could Help Target Federal Resources*, [GAO-20-127](#) (Washington, D.C.: Oct. 23, 2019). The rising number of natural disasters and increasing reliance on the federal government for assistance is a key source of federal fiscal exposure and, in 2013, we added “Limiting the Federal Government’s Fiscal Exposure by Better Managing Climate Change Risks” as an area on our high-risk list—a list of federal programs and operations at risk of fraud, waste, abuse, and mismanagement or that need transformation to address economy, efficiency, or effectiveness challenges. See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

States	FY 2017	FY 2018	FY 2019	FY 2020 ^a	FY 2021
7. Iowa	•	—	•	—	—
8. Idaho	—	—	—	—	•
9. Illinois	•	—	—	—	—
10. Indiana	•	—	—	—	—
11. Louisiana	•	•	•	—	•
12. Massachusetts	•	—	—	—	—
13. Michigan	—	—	•	—	—
14. Nevada	•	•	•	—	•
15. New Mexico	—	—	—	—	•
16. New Jersey	—	•	—	—	—
17. New York	—	—	—	—	•
18. Oregon	—	—	—	—	•
19. Pennsylvania	—	—	—	—	•
20. Rhode Island	—	—	•	—	—
21. South Dakota	—	—	•	—	—
22. Texas	•	•	•	—	•
23. Virginia	•	•	•	—	—
24. Washington	—	—	—	—	•
25. Wisconsin	—	—	•	—	•
States by fiscal year	10	6	11	1	14

Legend:

• = the state submitted updated data or new infrastructure.

— = the state or territory did not submit updated data or new infrastructure. States and territories that did not submit updated data or new infrastructure from fiscal years 2017 through 2021 were Alabama, Alaska, Connecticut, Delaware, Hawaii, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, North Carolina, North Dakota, Ohio, Oklahoma, South Carolina, Tennessee, Utah, Vermont, West Virginia, and Wyoming. U.S. territories that did not submit updated data or new infrastructure were American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands.

Source: Department of Homeland Security (DHS). | GAO-22-104279

^aDHS did not request updates to the National Critical Infrastructure Prioritization Program for fiscal year 2020 because the agency performed the year's update on a compressed schedule based on leadership direction at the time.

When states do not submit data or corrections to the NCIPP list, CISA staff perform some independent validation. CISA officials said that they annually check whether they need to remove any infrastructure on the NCIPP list by consulting a national-level data set for critical infrastructure. CISA officials then ask their regional staff to validate and verify corrections or new nominations to the list. Officials said that CISA regional staff—namely PSAs—work closely with state homeland security

agencies and infrastructure owners and operators and were, therefore, well-positioned to validate the NCIPP lists each year.

However, one PSA we spoke with said that CISA sent the list with a 2-week deadline to validate the infrastructure on it—a time line the PSA felt was not possible to meet, given the dozens of assets on the list. Furthermore, the PSA felt it was actually impossible to validate the NCIPP list because every asset's consequence estimates were subjective and, in the PSA's words, "a total guess." The PSA reported not seeing how CISA could normalize and validate these estimates and, therefore, reported having little confidence in the resulting lists of infrastructure.²⁵

Lack of use among critical infrastructure stakeholders. Critical infrastructure stakeholders we interviewed questioned the NCIPP's usefulness, noting that the data were not accurate, relevant, consistent, or reflective of infrastructure risk. Only four of the officials we met with reported using the NCIPP list in their infrastructure protection efforts. 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.²⁶

Sector Risk Management Agencies. None of the four Sector Risk Management Agency officials we contacted reported regularly using the NCIPP list. Sector Risk Management Agency officials raised a number of issues with the results, leading them to not rely on the list

²⁵CISA headquarters officials clarified that Regional Staff are not required to validate the consequence estimates in the submissions, rather they are to confirm that the assets or nodes in their areas of responsibility are operating under similar conditions as when they were put on the list.

²⁶We interviewed CISA PSAs and CSAs (i.e., CISA regional staff who advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators and offer cybersecurity services) from CISA Regions 2, 3, 4, 5, 7, 8. These regions cover 32 states, two U.S. territories, and the District of Columbia and are home to an estimated nearly 70 percent of the U.S. population, as of July 1, 2019.

for risk management purposes.²⁷ 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 their efforts. Officials felt that the types of infrastructure on the list were not consistent across regions.

Additionally, officials from another Sector Risk Management Agency said that the agency did not use the NCIPP list or rely on it for any purpose. Officials said that large infrastructure systems within their sector that served large metropolitan areas already knew their risk, which they assessed regularly, as a matter of course.

State homeland security agencies. Only one of the six state homeland security agencies we contacted reported regularly using the NCIPP list.²⁸ 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. Officials from three of six state agencies said that there were assets on the list that were not critical to their states.²⁹ Some state officials also said that the infrastructure on the list seemed inconsistent from state to state and that the criteria for adding assets were highly subjective, making the list generally unreliable, in their view.

Similar views were provided to us in 2013 by the State, Local, Tribal, and Territorial Government Coordinating Council. Council leadership said that the NCIPP process was burdensome and not reflective of the infrastructure risk in their areas of responsibility. The council Chair added that providing data to the NCIPP was an arduous process requiring a huge number of hours that took away from work that was more essential. Additionally, some state governments cited the burden of developing technical information for NCIPP submissions.³⁰

²⁷Sector 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).

²⁸One 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.

²⁹State Homeland Security Agency officials we interviewed were from Colorado, Florida, Illinois, Texas, and Washington. California provided written responses to questions about this topic, so we are reporting their responses here; however, California is not included in the 25 total stakeholders we discuss in the rest of this report. CISA officials noted that if a state identifies a facility it believes should not be on the list, it should provide that information to CISA during the annual data call.

³⁰[GAO-13-296](#).

For example, some states said that they lacked expertise to develop scenarios and model complex infrastructure systems with sufficient fidelity to assess likely consequences of failure or disruption.

CISA Officials Stated the NCIPP Provided Value Initially but Acknowledged It Now Has Limitations

CISA officials stated that while the NCIPP provided a number of benefits that supported the protection and prioritization of critical infrastructure, some limitations with the program exist. In terms of benefits, CISA officials stated that the NCIPP provided broad awareness of critical infrastructure that it did not have prior to the program and that DHS had integrated the program's lessons learned throughout its operations. For instance, a senior CISA official said that the NCIPP has generated a large body of knowledge of what would happen to specific assets in the event of a major failure, and this knowledge has informed CISA's thinking on a number of issues. The NCIPP was also useful in providing DHS and its partners with ways to think about prioritizing assets in certain situations. CISA officials also said that some states are highly engaged in the NCIPP because they receive federal grant funding under FEMA's Homeland Security Program.³¹ Specifically, FEMA uses counts of NCIPP assets as a way to capture infrastructure risk as an element of the Terrorism Risk Methodology Model, which it uses to calculate the relative risk order of the 56 states and territories. CISA officials stated that states and metropolitan areas are incentivized by the FEMA's grant program methodology to ensure the most comprehensive capture of infrastructure within their locations, often submitting nominations for assets and systems that are on the borderline of current criteria. CISA officials stated that in their review of new nominations, CISA staff have identified infrastructure assets that are no longer operational, but were not identified by state officials.

In addition, a senior CISA official said that they incorporated the NCIPP's prioritized-asset approach to looking at infrastructure risk to help inform

³¹FEMA provides preparedness grants to state, local, tribal, and territorial governments to help prepare for, prevent, protect against, respond to, recover from, and mitigate terrorist attacks or other disasters. State Homeland Security Program grants are awarded to the nation's 56 states and territories. Grant allocations have been based, in part, on FEMA's risk-based grant assessment model, with states deemed to be at higher risk receiving higher awards than those deemed at lower risk.

incident management and response efforts.³² Specifically, during an approaching hurricane, CISA staff query the NCIPP to identify vulnerable infrastructure within the geographic path of the hurricane. Once identified, the potentially affected assets may be included in an “Infrastructure of Concern” list and then shared with CISA regional staff in the area so that they can monitor the status of the assets during the emergency. CISA officials told us that while the “Infrastructure of Concern” data set is primarily used to compile lists of assets threatened by hurricanes, they are in the process of developing prioritization schemas and filtration formulas to apply to other hazards and threats across all 10 of CISA’s regions.

A senior CISA official said that ranked-asset approaches to risk are now largely built into DHS’s and its partners’ operational models. Therefore, the official believed that CISA’s and states’ time and other resources would be better directed to other efforts. Further, the official added that CISA and its federal and state partners were not finding any new or significant critical infrastructure through the NCIPP that they did not already know about or that they would not have identified through other means.

Our analysis of CISA data supports the lack of new assets on the list. As of May 2021, there were 1,404 assets on the NCIPP list—88 Level 1 assets and 1,316 Level 2 assets. This represents a net change of 38 assets since fiscal year 2018—five additional Level 1 assets and 33 additional Level 2 assets. Over this same period, states nominated 421 assets to the NCIPP’s lists. However, CISA did not approve most of these nominations for various reasons, mostly technical in nature, such as needing additional documentation of economic consequences or the estimated length of time for evacuations, or needing additional support that estimated fatalities would be “prompt.”

A CISA official added that halting its current NCIPP work could allow CISA to work with its state and local partners to understand and prioritize infrastructure in their areas of responsibility that is most important to them (a focus that officials said is missing in the NCIPP, which prioritizes only very high consequence assets in certain scenarios). For example, the

³²DHS produces Infrastructure of Concern lists to identify critical infrastructure and key resources in response to terrorist attacks, natural hazards, and other events. The information supports the activities of the department and informs the strategies of federal, state, local, and private sector partners to deter, prevent, preempt, and respond to terrorist attacks and other disruptions to infrastructure.

current NCIPP criteria allow for a single-incident cyber scenario but not a prolonged or cascading scenario—an event that is much more likely in today’s threat environment. In other words, the NCIPP is focused on simple scenarios where a threat or hazard impacts a single asset, system or cluster. Cyberattacks, however, often involve multiple entities and locations being impacted over a period of time where no one asset may meet the NCIPP thresholds.

CISA officials acknowledged other challenges when looking at attack scenarios through the eyes of the asset-and-geography framework of the NCIPP. For example, CISA officials said that a large transformer—a critical component of the bulk electricity transmission grid—may have a vulnerability that an attacker could exploit, but the failure of that single transformer may not meet the NCIPP’s consequence thresholds (nor may it have widespread impact based on how the grid is designed and operated). However, if an attacker were able to exploit multiple transformers simultaneously, due to a common vulnerability or attack, the consequences could be higher and lead to repercussions that have regional or national-level impacts. The importance of such assets in terms of scalable attacks or cascading failures is not captured through the current NCIPP nomination process.

Despite these challenges, CISA officials said they felt that the agency was limited in its ability to make changes to its NCIPP list because of the statutory requirement to maintain it and because FEMA uses NCIPP data in its Homeland Security Program grant assessment model. NCIPP infrastructure counts are included in FEMA’s model, but FEMA officials told us that the NCIPP counts are not strongly correlated with a grant applicant’s risk score and that much of the funding awarded through the State Homeland Security Program—one of the programs within the Homeland Security Grant Program—was subject to statutory minimums, thus limiting the amount of funding that could be awarded based on the risk model.³³ FEMA officials said that they, too, would like to use a different, more relevant source of information in the grant model to better represent critical infrastructure vulnerability. FEMA officials said that they planned to update how the model accounts for infrastructure risk, but this

³³NCIPP activity is a small percentage of the current State Homeland Security Program grant formula (approximately 10 percent), but CISA officials noted that nominating assets to the NCIPP list is one of the few opportunities that state, local, tribal, and territorial stakeholders have to influence their risk ranking within the current grant formula.

will take time, as FEMA needs to collaborate with CISA to analyze the best enhancements and to conduct substantial outreach to state partners.

A supplemental tool to the 2013 National Plan states that a sound approach to critical infrastructure risk management includes identifying the assets, systems, and networks that contribute to critical functionality, including analyzing infrastructure dependencies and interdependencies.³⁴ The National Plan supplemental tool also states that critical infrastructure partners (which include federal partners; critical infrastructure owners and operators; and state, local, tribal, and territorial partners) should work together to ensure that the critical infrastructure inventory data structure is accurate, current, and secure. Given the evolving risk landscape and CISA, FEMA, and the critical infrastructure community's recognition of the NCIPP's limitations, helping to ensure that CISA's process for identifying and prioritizing critical infrastructure both accounts for current threats and incorporates stakeholder input could provide CISA and its partners with a more relevant and useful understanding of critical infrastructure risk.

Limited Understanding of National Critical Functions Framework May Pose Challenges

The National Critical Functions Framework Marks a Shift in DHS's Critical Infrastructure Identification and Prioritization

In spring 2019, CISA's National Risk Management Center published a set of 55 critical functions as part of its new National Critical Functions framework. 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 that 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. Figure 6 lists examples of National Critical Functions in four broad categories: “connect” (nine of the 55

³⁴Department of Homeland Security, *2013 National Infrastructure Protection Plan, Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*.

functions), “distribute” (nine of the 55 functions), “manage” (24 of the 55 functions), and “supply” (13 of the 55 functions).

Figure 6: Examples of Cybersecurity and Infrastructure Security Agency (CISA) National Critical Functions

Connect	Distribute	Manage	Supply
<ul style="list-style-type: none"> • Provide positioning, navigation, and timing services • Provide satellite access network services • Provide wireless access network services 	<ul style="list-style-type: none"> • Distribute electricity • Maintain supply chains • Transport materials by pipeline 	<ul style="list-style-type: none"> • Manage wastewater • Perform cyber incident management capabilities • Protect sensitive information 	<ul style="list-style-type: none"> • Manufacture equipment • Produce and provide human and animal food products and services • Supply water

Source: GAO analysis of CISA information. | GAO-22-104279

At the time of our review, CISA was still early in its efforts to fully develop and apply the National Critical Functions, including linking critical functions to their relevant Sector Risk Management Agencies. CISA National Risk Management Center officials noted that some functions, such as “supply water” and “manage wastewater,” have a logical lead organization (i.e., the Environmental Protection Agency). However, many critical functions are highly distributed across multiple (or even all) critical infrastructure sectors. For example, all sectors protect sensitive information, 10 sectors provide public safety, and 14 sectors manage hazardous materials.

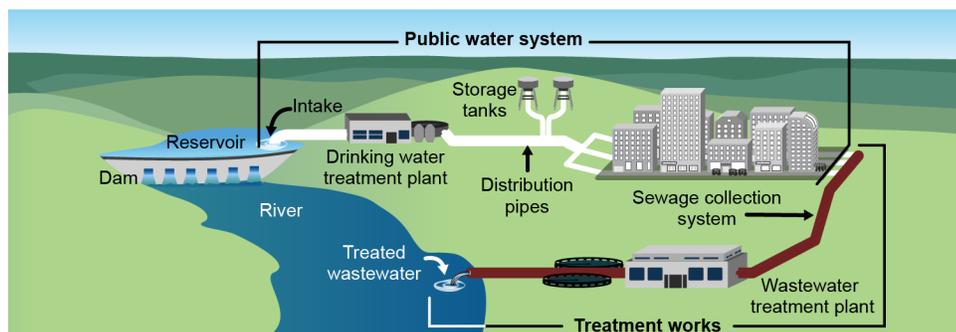
CISA National Risk Management Center officials said this new framework marks a substantial shift in DHS’s thinking on risk and that it will take time to fully understand the interdependencies across the 16 sectors and to integrate the framework into key strategic documents and policies (such as the National Plan or DHS’s Risk Management Framework). CISA reported having such work underway, including updating the National Plan to include the National Critical Functions.³⁵

CISA also plans to use the 55 functions to identify the critical infrastructure that supports those functions through a multistep process. Each function is being broken down into its related subfunctions, then into systems and assets needed to carry out the subfunctions, and ultimately into assets that support these systems. For instance, CISA is currently

³⁵In June 2021, CISA officials reported that they were chartering a National Critical Functions Implementation Steering Group made up of representatives from across CISA. The group will manage and coordinate efforts to institutionalize the National Critical Functions framework as CISA’s approach to infrastructure identification and prioritization.

breaking down each function (such as “supply water”) into systems (such as public water systems) and assets (including infrastructure such as water treatment plants), as illustrated below in figure 7.

Figure 7: Examples of Critical Infrastructure Systems and Assets That Support the National Critical Function “Supply Water”



Source: GAO (graphic) and U.S. Environmental Protection Agency and Department of Homeland Security (information). | GAO-22-104279

CISA is also developing the foundational requirements for what it calls the Risk Architecture Tool—an interactive tool for analysts and decision makers that CISA intends to use to provide a visual representation of the networks between the critical functions. CISA officials reported that version 1 of the Risk Architecture Tool was completed in October 2021 and that a second version of the tool was being developed in early fiscal year 2022. Developing version 1 of the tool included breaking down all 55 National Critical Functions into subfunctions, as illustrated below in figure 8.

CISA Has Used the National Critical Functions Framework to Support Critical Infrastructure Protection Efforts

Despite being early in its development, the National Critical Functions framework has informed key CISA efforts over the last 2 years, according to CISA officials. This has included analyzing Coronavirus Disease 2019's (COVID-19) impacts and providing national-level responses to the pandemic, including developing guidance on essential workers and providing technical support to vaccine manufacturers.³⁶

CISA has also used the National Critical Functions framework to assess the cross-sector and national-level impacts of other events, such as the 2021 cyberattack on the Colonial Pipeline Company, to provide decision makers with foresight into the impact on critical infrastructure. For example, in May 2021, CISA published a National Critical Functions assessment, which identified broad impacts from the cyberattack across multiple sectors and select National Critical Functions. The assessment reported that some National Critical Functions were under stress from the limited availability of fuel and limited storage options as extraction and refining continued. CISA reported that a prolonged shutdown would likely have resulted in negative consequences to many critical functions, examples of which are shown in table 2.

³⁶CISA issued the critical worker guidance originally on March 19, 2020, and published four additional updates.

Table 2: Examples of National Critical Functions Affected by the 2021 Colonial Pipeline Company Cyberattack

National Critical Function	Geographic concentration	Effect	Consequence
Store fuel and maintain reserves.	National	Storage facilities along the Gulf Coast will be unable to move fuel and, therefore, unable to receive further fuel from refineries. Facilities along the East Coast will begin to empty as the reserves are drawn down.	The inability to move fuel from the Gulf Coast will result in the slowdown or shutting down of refineries in the Gulf Coast until there is storage capacity for refined products. Reserves along the East Coast that would be available for other emergencies will no longer be available.
Transport materials by pipeline.	National	Markets in the Southeast and, to a lesser extent, the mid-Atlantic, are dependent on the Colonial Pipeline for petroleum products. The Plantation Pipeline, which parallels part of the Colonial Pipeline, is currently understood to be operating at or near capacity. Colonial has restored operations on some branch lines, moving fuel to inland markets.	Other pipelines, such as the Buckeye and Plantation pipelines, will be under pressure to operate at capacity. Demand for fuel trucks, barges, and vessels will increase dramatically, resulting in price increases. Fuel truck availability will likely become extremely limited, due to demand outstripping supply and the current shortage of qualified drivers.
Maintain supply chains.	Regional	Supply chains typically rely on vehicles running on fossil fuels to move raw or finished products. Disruptions to movement by air, road, and rail can result in disruptions of these supply chains until fuel availability is restored or alternative transportation is set up.	Disruptions to supply chains could quickly cascade to the supply chains of other entities across the country reliant upon goods or services from the affected areas.

Source: Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. | GAO-22-104279

Beyond CISA, an October 2021 report by the Bipartisan Commission on Biodefense referenced the National Critical Function of providing medical care, noting that it required the efforts of the Health Care and Public Health sector, as well as the contributions of 10 other critical infrastructure sectors.³⁷ The report noted that responding to a biological

³⁷In addition to the Healthcare and Public Health Sector, the following critical infrastructure sectors also contributed to the effective execution of the National Critical Function to provide medical care: Chemical; Communications; Critical Manufacturing; Emergency Services; Energy; Food and Agriculture; IT; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater. See: Bipartisan Commission on Biodefense, *Insidious Scourge: Critical Infrastructure at Biological Risk* (Washington, D.C.: October 2021).

event required multiple sectors to execute National Critical Functions together and that a biological event could affect sectors in different ways and to varying extents, making it challenging to coordinate an efficient response. Moreover, CISA officials told us that some of the sectors, such as oil and natural gas, and transportation, also manage hazardous materials and do so using similar technologies and equipment. Officials said that the National Critical Functions framework has also been useful in helping stakeholders understand risk management across both physical and cyberspace risks because, while many stakeholders have come to understand what they need to do to mitigate physical threats, many do not have the visibility, expertise, and resources to mitigate cyber risks in the current threat environment.

Most Stakeholders Were Unclear on National Critical Functions Framework Goals

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 risks to the nation's critical cyber 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 and 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, which 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.

CISA's National Risk Management Center officials said that their office solicited broad stakeholder input to identify the critical functions but that further defining the functions and institutionalizing the framework was intentionally designed to be headquarters focused. However, a 2020 update on CISA's efforts to break down the critical functions emphasized the importance of stakeholder input, noting the need to broaden the stakeholder community involved in critical infrastructure risk management by better engaging nontraditional groups.³⁸ Additionally, DHS's National Plan states that partnerships enable more effective and efficient risk management. CISA's July 2020 update to the National Critical Functions framework stated that nearly 40 percent of the 55 functions were local in nature, meaning that any disruption to the function would not necessarily scale to larger geographic areas. This focus further emphasizes the need for stakeholder engagement and buy-in to account for local perspectives. Helping to ensure that stakeholders understand the goals of the framework and are fully engaged in implementing it could aid the agency in its future infrastructure protection efforts.

In addition to a need for stakeholder engagement, CISA does not have an available documented plan for the National Critical Functions framework that includes clear goals and strategies to describe what the framework is intended to achieve, and how. While CISA's Strategic Intent from 2019 references the importance of protecting the National Critical Functions, it

³⁸In addition to the Healthcare and Public Health Sector, the following critical infrastructure sectors also contributed to the effective execution of the National Critical Function to provide medical care: Chemical; Communications; Critical Manufacturing; Emergency Services; Energy; Food and Agriculture; IT; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater. See: Bipartisan Commission on Biodefense, *Insidious Scourge: Critical Infrastructure at Biological Risk* (Washington, D.C.: October 2021).

does not outline the goals and strategies for the framework and how they are to be achieved.³⁹ The Government Performance and Results Act of 1993 (GPRA), as updated by the GPRA Modernization Act of 2010 (GPRAMA), includes principles for agencies to focus on the performance and results of programs by putting elements of a strategy and plan in place, such as (1) establishing measurable goals and related measures and (2) developing strategies and plans for achieving results. Although GPRAMA applies to the department or agency level, in our prior work we have reported that these provisions can serve as leading practices for strategic planning at lower levels within federal agencies, such as planning for individual divisions, programs, or initiatives.⁴⁰ Outlining the goals and strategies for the National Critical Functions framework is critical for determining whether CISA has a clear sense of how it will assess progress toward achieving its intended results. Without such a documented plan, stakeholders will likely continue to raise similar questions about it.

CISA Cyber Services and Threat Information Sharing Lack Regional Focus

CISA Provides Vulnerability Assessments, but Regional Outreach for Cybersecurity Services Is Not Fully Communicated or Coordinated

CISA offers physical and cybersecurity assessments to identify vulnerabilities, support national risk management efforts, and build critical infrastructure stakeholder resiliency and partnerships; however, stakeholders we met with identified the need for better coordination between headquarters and the regions in delivering cybersecurity services. CISA provides a broad range of services to critical infrastructure owners and operators, including webinars, training, tabletop exercises, and technical tools and assessments, many of which it offers in an online services catalog. The catalog provides information on services across all of CISA's mission areas that are available to federal government; state, local, tribal, and territorial governments; private industry; academia;

³⁹See Cybersecurity and Infrastructure Security Agency, *CISA Strategic Intent* (August 2019).

⁴⁰See GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs*, [GAO-18-562](#) (Washington, D.C.: Aug. 22, 2018); and *Environmental Justice: EPA Needs to Take Additional Actions to Help Ensure Effective Implementation*, [GAO-12-77](#) (Washington, D.C.: Oct. 6, 2011).

nongovernmental and nonprofit organizations; and general public stakeholders.

CISA’s regional PSAs and CSAs are responsible for providing many of CISA’s infrastructure security and cybersecurity assessments for industry and private sector stakeholders, and CISA headquarters is responsible for providing cyber services. Examples of these assessments and services are described in table 3.

Table 3: Examples of Cybersecurity and Infrastructure Security Agency (CISA) Security Assessments and Numbers of Assessments Conducted in Fiscal Year (FY) 2020

Assessment	Description and level	Who conducts them	Number conducted in FY 2020
Infrastructure security assessments			
Security Assessment at First Entry	Assesses current security posture and identifies options for facility owners and operators to mitigate relevant threats Foundational	Regional Protective Security Advisors (PSA)	550
Infrastructure Survey Tool	Web-based assessment to identify and document the overall physical security and resilience of a facility Intermediate	Regional PSAs	313
Regional Resiliency Assessment Program	Cooperative assessment of specific critical infrastructure that identifies security and resilience issues that could have regionally or nationally significant consequences. Typically involves a year-long process to collect and analyze data, followed by continued technical assistance Foundational	Regional PSAs and CISA Infrastructure Security Division	12
Cybersecurity assessments			
Cyber Infrastructure Survey	Evaluates effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience of an organization’s cybersecurity ecosystem Foundational	Regional Cybersecurity Advisors (CSA)	80
Cyber Resilience Review	Interview-based assessment that evaluates an organization’s operational resilience and cybersecurity practices. Evaluates capacities and capabilities across 10 domains, including asset management, incident management, and situational awareness Advanced	Regional CSAs	112

Assessment	Description and level	Who conducts them	Number conducted in FY 2020
Cybersecurity assessments			
External Dependencies Management Assessment	Measures and reports on the ability of an organization to manage external dependencies as they relate to the supply and operation of information and communications technology. Intermediate	Regional CSAs	63
Remote penetration testing	Simulates the tactics and techniques of real-world adversaries to identify and validate a perimeter's exploitable pathways Intermediate	CISA's Cybersecurity Division	728
Web application scanning	Evaluates publically accessible websites for potential bugs and weak configurations to provide recommendations for mitigating web application security risks Foundational	CISA's Cybersecurity Division	48
Phishing campaign assessment	Provides opportunity to determine potential susceptibility of personnel to phishing attacks Foundational	CISA's Cybersecurity Division	522
Vulnerability scanning	Evaluates external network presence by scanning public, static internet protocol addresses for accessible services and vulnerabilities. Provides weekly vulnerability reports and ad hoc alerts Foundational	CISA's Cybersecurity Division	2,067
Validated architecture design reviews	Assists with architecture and design review, system configuration, log file review, and analysis of network traffic to identify anomalous communication flows Intermediate/advanced	CISA's Cybersecurity Division	357

Source: GAO analysis of CISA information. | GAO-22-104279

Note: "Foundational" refers to services and resources that are available and recommended to all users, regardless of capability. "Intermediate" are services that require users to have some experience developing and implementing security policies and procedures either on their own or through previous CISA engagements. "Advanced" are services that, because of their expansive scope and technical complexity, require preexisting capabilities and programs already in place within an organization that can be leveraged as prerequisites for receiving that service.

Critical infrastructure stakeholders had generally positive feedback on CISA information sharing but shared mixed views on CISA's delivery of assessments. Critical infrastructure stakeholders we met with—which included Sector Risk Management Agencies, SCCs and state homeland security advisors—had generally positive feedback on CISA's information-sharing efforts, including its alerts and guidance. For example, two of four SCC officials said that CISA was effective at aggregating and sharing information from disparate sources and that its

guidance presented concrete steps that agencies could take to respond to real-world events, such as cyberattacks and data breaches. Another council official said that in the past, they had to collect this type of information from multiple sources; however, CISA now provided consolidated information to the sector via email, social media feeds, and government-wide information-sharing networks. Two of four SCC members and two of six homeland security advisors had similarly positive feedback on CISA's information sharing.

Critical infrastructure stakeholders provided mixed views on CISA's physical and cybersecurity assessments; however, CISA had efforts underway to address these issues. Two state homeland security advisors told us that they relied on CISA's physical vulnerability assessments to provide insight into their states' vulnerabilities because they had limited capacity to conduct those assessments on their own. However, some SCC members and Sector Risk Management Agency officials said that CISA's physical vulnerability assessments may provide potentially misleading representations of an organization's level of security. They added that the cyber and physical vulnerability assessments varied in quality, depending upon the experience and expertise of the CSA or PSA conducting them. For example, one CISA physical security assessment—the Infrastructure Survey Tool—provides organizations with a relative ranking of their security practices compared with other similar organizations that also completed the assessment. One CSA said that in their view, assessing performance comparatively—rather than assessing an organization against a set standard—can result in an overly positive assessment of an organization's security, if all comparable organizations also have weak security practices. CISA officials said in July 2021 that they were in the process of updating their primary physical vulnerability assessment tool to address these and other concerns.

CSAs face communication and coordination challenges in delivering cybersecurity services. CSAs we met with said there is high demand for CISA's cybersecurity services, but CISA headquarters and regional CSAs have experienced challenges in communicating and coordinating how CISA will deliver some of its services. As noted above in table 3, regional CSAs offer cybersecurity assessments that can be geared toward organizations at different levels of maturity, from foundational-level reviews to highly advanced technical assessments. According to CISA officials, CISA's Cybersecurity Division offers a suite of voluntary cyber hygiene and assessment services, available upon request and with the documented consent of the company. These services include regular vulnerability scans and remote penetration tests where CISA will try to

achieve access to a company's internal systems in the same ways malicious actors would.

CSAs told us that CISA headquarters asks CSAs to promote the cyber hygiene services to regional critical infrastructure partners but noted that CISA headquarters will also promote the services directly to regional partners, resulting in communication and coordination challenges. Specifically, CISA headquarters' and regional staff did not coordinate when conducting outreach to critical infrastructure organizations. Four of six CSAs told us that headquarters staff did not coordinate with the regions when offering cybersecurity services to local organizations, which CSAs felt undermined their local relationships and lessened CISA's credibility with these organizations. For example, one CSA noted that CISA headquarters directed the regions to advertise services available out of headquarters, such as vulnerability scanning or remote penetration tests.⁴¹ However, the CSA noted that headquarters' limited resources often meant that the agency could not adequately support requests for services to local organizations, which led to frustration. CSAs said they were also unsure which organizations CISA headquarters had reached out to in the regions, which made CSA's outreach efforts more difficult. Further, CSAs reported lacking insight into CISA headquarters' scheduling and, therefore, were unable to inform organizations when they might receive services.

CISA's recent reorganization has contributed to these challenges.

One CSA told us that they lacked insight into the cybersecurity services delivered by headquarters because of their organizational placement following CISA's 2020 reorganization.⁴² Specifically, the CSA (and their counterpart PSAs) are located in regional offices, which are organized under CISA's Integrated Operations Division. CISA's cyber assessment services, however, are provided by staff within a different branch of

⁴¹Remote penetration testing focuses entirely on externally accessible systems and may incorporate scenario-based external network penetration testing, external web application testing, and phishing campaign assessments. Vulnerability scanning assesses internet-accessible systems on a continual, remote basis to identify vulnerabilities.

⁴²The Cybersecurity and Infrastructure Security Agency Act of 2018 renamed the National Protection and Programs Directorate to CISA and prescribed changes to its organizational structure. Pub. L. No. 115-278, § 2, 132 Stat. 4168 (codified as amended at 6 U.S.C. § 652). To implement these requirements and position itself to effectively carry out its mission, CISA launched an organizational transformation initiative to be carried out in three phases. We reported on CISA's progress in March 2021. See [GAO-21-236](#).

CISA—the Cybersecurity Division—which operates out of CISA headquarters.

CISA officials acknowledged that the agency experienced some unanticipated challenges delivering cybersecurity services to the regions following the agency's recent reorganization and that they had a variety of actions underway to address those challenges. These actions included establishing a shared, online cybersecurity service delivery schedule and holding frequent meetings with all levels of regional staff (including CSAs). Other actions included providing regional staff with copies of all email communications with the stakeholders in their regions (including scheduling invitations, providing meeting invitations, and sending information on when headquarters' cyber assessment team will be onsite in the region) and developing a stakeholder relationship management tool to help CISA headquarters and regional staff coordinate outreach to critical infrastructure partners.

As of November 2021, these actions were still under development and had yet to be fully implemented; therefore, we could not determine whether the actions would address the challenges we identified. The 2013 National Plan emphasizes the importance of clear and frequent communication as part of a well-functioning partnership for critical infrastructure protection. Communicating and coordinating its cybersecurity efforts among headquarters and regional staff could help CISA improve the overall effectiveness of its cybersecurity support.

**Stakeholders Reported
Needing Regionally
Specific Threat Information**

CISA analyzes and shares threat information for incidents ranging from cyberattacks to hurricanes; however, critical infrastructure stakeholders reported a need for more regionally specific threat information. CISA shares threat information through several channels, examples of which are in table 4.

Table 4: Cybersecurity and Information Security Agency (CISA) Intelligence and Threat Information Sharing

Program	Description
CISA Intelligence Subdivision	Develops, provides, and integrates all-source intelligence to inform CISA operations and activities
National Cyber Awareness System	Provides cost-free subscription-based cybersecurity threats, issues, general security topics, and other informational products that are emailed to stakeholders to improve situational awareness. Subscribers receive technical alerts, control system advisories and reports, weekly vulnerability bulletins, analyses, and tips on cybersecurity and cyber hygiene best practices.
CISA Central	CISA's primary threat information hub for sharing threats and emerging risks to U.S. critical infrastructure
Automated Indicator Sharing	Enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect participants of the Automated Indicator Sharing community and to ultimately reduce the prevalence of cyberattacks.

Source: GAO analysis of CISA threat information programs. | GAO-22-104279

Selected PSAs, CSAs, Sector Risk Management Agencies, SCC members, and state homeland security advisors we spoke to said that CISA's threat information helped them to understand the broader threat landscape, such as threats to election security and COVID-19 response efforts. However, almost half (12 of 25) of the stakeholders reported needing additional information related to the threats specific to their regions and local infrastructure.

For example, one CSA said that CISA National Risk Management Center' threat products provided a broad overview of national issues but did not provide a risk perspective tailored to the critical infrastructure organizations in the CSA's region, rendering the information less relevant to the CSA's critical infrastructure partners.⁴³ A PSA and a CSA from another region stated that CISA's focus on national issues, such as cybersecurity and election security, was necessary, but regionally specific threat information would better meet the needs of local critical infrastructure owners and operators.

Some CSAs and PSAs told us that organizations in their regions were primarily concerned with active shooters and chemical spills (accidental or intentional) and thus needed information that was applicable to those threats. For example, one PSA in a heavily agricultural region stated that an attack on a truck full of anhydrous ammonia (a common source of nitrogen fertilizer) in a major intersection was more concerning to

⁴³According to CISA, relevant threat information enables an organization to make informed and timely risk decisions regarding threats that are specific and of interest to their operations, assets, and organization.

stakeholders in their region than general descriptions of national-level threats. Another PSA said that the region would benefit from threat information that emphasized the sectors that addressed other sectors that are important to the region, such as the water, energy, and telecommunications sectors. The PSA said that an attack on any of these sectors would have cascading impacts that would affect nearly all of the region's critical infrastructure, yet the PSA said that they did not receive sufficient threat information from CISA that focused on those sectors.

State and industry officials expressed a need for more regionally specific threat information. SCC and state homeland security officials reported similar views to the PSAs and CSAs. Specifically, one SCC official told us that CISA's products were always well-researched, but CISA's threat information could be more regionally focused. For example, in some cases, the official reported learning about threats that affected their sector through media reports or via social media websites rather than from CISA and added that the critical infrastructure organizations in their sector wanted more regionally specific threat information.

State homeland security agency officials we met with echoed these concerns. For example, a homeland security advisor from one state told us that CISA provided some guidance on protecting soft targets from active shooters, such as checklists and self-assessments for schools, shopping centers, and houses of worship. Additionally, the state officials said that while CISA provided some threat information, their state needed more threat information that related to domestic violent extremism.

CISA officials agreed with the need to improve regionally specific threat information sharing but said that they faced challenges in doing so. For one, officials told us that they had limited intelligence resources dedicated to serving the regions. For example, an official from CISA's Intelligence Subdivision, an office under the Integrated Operations Division, stated that three intelligence analysts shared the responsibility of providing intelligence information to the regions, in addition to their other responsibilities. Moreover, officials told us that CISA's role as a provider of regionally specific threat information supplemented the efforts of regionally based organizations, such as Fusion Centers and Information Sharing and Analysis Centers, which CISA and other organizations relied on for threat information. CISA officials stated that these organizations were the primary generators of regionally specific threat information and characterized themselves as "information brokers" rather than the source

of such threat information.⁴⁴ CISA officials also noted that even if they were to generate more specific threat information, some organizations in the regions did not have staff with the necessary security clearances to receive the information. Even so, CISA officials agreed that finding ways to share such information was important because it would enable CISA and its critical infrastructure partners to better target resources, including CISA vulnerability assessments.

According to its 2021 budget justification submission, CISA's 10 regions are to provide a local perspective to the national risk picture by identifying, assessing, and minimizing the physical and cyber risk to critical infrastructure at the state, local, and regional levels. Additionally, the National Plan and a 2013 presidential directive have all emphasized the need for DHS to improve threat information sharing with other levels of government and the private sector to manage risks to critical infrastructure.⁴⁵ These documents frame the nation's efforts to protect critical infrastructure in both a national and a regional context. This includes sharing information about threats to jurisdictions that can enhance their ability to make informed and efficient security and resilience investments. Improving its coordination efforts with regionally based threat information organizations, such as Fusion Centers, Information Sharing and Analysis Centers, Information Sharing and Analysis Organizations, and other organizations could give CISA an opportunity to enhance information sharing with key partners and regional stakeholders, thus potentially reducing vulnerabilities to the nation's critical infrastructure.

Conclusions

Cyberattacks, multibillion-dollar environmental disasters, and other threats facing the nation's critical infrastructure require an effective and coordinated public-private response. CISA has undertaken a wide range

⁴⁴Fusion Centers are state-owned and -operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal and territorial, federal, and private sector partners. Information Sharing and Analysis Centers are member-driven organizations that deliver all-hazards threat and mitigation information to asset owners and operators. Threat information "brokering" as a service is a common cyber threat information-sharing model in which the producer ingests information from multiple sources or feeds and then shares the content with consumers that have a legal right to the information. The main purpose of a broker is to normalize or synthesize the information from multiple sources to make it easier for organizations to ingest, visualize, and to perform analytics on large data sets.

⁴⁵Department of Homeland Security, *2013 National Infrastructure Protection Plan*; Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013); and Pub. L. No. 116-283, § 9002.

of efforts to identify and prioritize nationally significant critical infrastructure but could take steps to improve and further these efforts. Helping to ensure that CISA's process for identifying and prioritizing critical infrastructure accounts for current threats and meets the needs of all states could allow CISA and its partners to have a more relevant and useful understanding of critical infrastructure risk. CISA's new National Critical Functions framework is a logical evolution from the asset-centric approach of prior DHS efforts, including the NCIPP. However, CISA has considerable work ahead to continue operationalizing this framework for all critical infrastructure prioritization. Ensuring that the critical infrastructure community is fully engaged in implementing the new framework could help CISA and its partners in future infrastructure protection efforts. Furthermore, CISA having a documented plan for the National Critical Functions framework that includes goals and strategies will help stakeholders better understand the intent of the framework and how to achieve it.

CISA also has opportunities to improve how it delivers cybersecurity services and shares threat information with the critical infrastructure community, including its regional PSAs and CSAs. CISA delivered hundreds of infrastructure security and cybersecurity services in fiscal year 2020, but better communicating and coordinating the delivery of key cybersecurity services within CISA could improve the effectiveness of these efforts. Last, CISA shares a wide range of information with the critical infrastructure community, which stakeholders reported finding valuable. Working with its partner organizations to gather and share more regionally specific threat information could help CISA's information-sharing efforts and further reduce vulnerabilities to the nation's critical infrastructure.

Recommendations for Executive Action

We are making the following six recommendations to CISA:

The Director of CISA should ensure that CISA's process for developing a prioritized list of critical infrastructure that would cause national or regional catastrophic effects if destroyed or disrupted reflects current threats. (Recommendation 1)

The Director of CISA should ensure that CISA's process for developing a prioritized list of critical infrastructure that would cause national or regional catastrophic effects if destroyed or disrupted includes input from additional states that have not provided recent nominations or updates. (Recommendation 2)

The Director of CISA should ensure that stakeholders are fully engaged in the implementation of the National Critical Functions framework.
(Recommendation 3)

The Director of CISA should document, as appropriate, goals and strategies for the National Critical Functions framework.
(Recommendation 4)

The Director of CISA should implement processes to improve communication and coordination between critical infrastructure organizations and CISA headquarters and regional staff.
(Recommendation 5)

The Director of CISA should coordinate with relevant regionally based, federal, and nonfederal partners to regularly develop and distribute regionally specific threat information to each of CISA's 10 regions.
(Recommendation 6)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, DOE, FERC, and EPA. DHS provided written comments, which are reproduced in appendix III. In its comments, DHS concurred with our recommendations and described actions planned to address them. DHS also provided technical comments, which we incorporated as appropriate. DOE, FERC, and EPA reviewed the report and did not have comments. We also provided draft excerpts of this product for review to nonfederal critical infrastructure stakeholders we interviewed for this report. One state had comments on the excerpts, which we incorporated as appropriate.

With regard to our first recommendation, that CISA ensure its process for developing a prioritized list of critical infrastructure reflects current threats, DHS stated that CISA will evaluate existing nomination thresholds within the NCIPP against current threats. CISA will use the results of the evaluation to support a comprehensive update of nomination thresholds in fiscal year 2023, in coordination with Sector Risk Management Agencies. These actions, if fully implemented, should address the intent of the recommendation.

With regard to our second recommendation, that CISA ensure its process for developing a prioritized list of critical infrastructure includes input from states that have not provided recent nominations or updates, DHS stated that CISA will reach out to states that did not submit nominations in the last three fiscal years to confirm they are aware of the program. Additionally, in the next call for nominations, CISA will ask states to affirm

that there are no new relevant assets and that no assets currently on the NCIPP list have been taken offline. These actions, if fully implemented as part of the NCIPP annual nomination process, should address the intent of the recommendation.

With regard to our third recommendation, that CISA ensure stakeholders are fully engaged in the implementation of the National Critical Functions framework, DHS listed steps taken to date to engage the private sector and government partners, such as organizing meetings and establishing a Federal Risk Management Working Group in March 2021. DHS also stated that CISA will conduct additional outreach to stakeholders through “Communities of Interest” it has identified for each National Critical Function. This action, if fully implemented, should address the intent of the recommendation.

With regard to our fourth recommendation, that CISA document goals and strategies for the National Critical Functions framework and integrate them with other efforts, DHS stated that CISA will leverage the anticipated 2022 update to the National Plan to provide clear documentation of its goals and strategies for the National Critical Functions. This action, if fully implemented, should address the intent of the recommendation.

With regard to our fifth recommendation, that CISA implement processes to improve communication and coordination between critical infrastructure organizations and CISA headquarters and regional staff, DHS stated that CISA will establish and document formal mechanisms for coordination and feedback on service delivery. This action, if fully implemented, should address the intent of the recommendation.

With regard to our sixth recommendation, that CISA coordinate with relevant partners to regularly develop and distribute regionally specific threat information to each of CISA’s 10 regions, DHS listed steps taken to date to disseminate threat information to regional partners, such as proactively providing classified briefings to key partners in some circumstances. Additionally, DHS stated that CISA is conducting a pilot program with Regions 2 and 3 to support their intelligence requirements, which is estimated to be completed in six months. To the extent the pilot program successfully distributes regionally specific threat information, and the results of the pilot program are applied to all 10 regions, these actions should address the intent of the recommendation.

We are sending copies of this report to the Secretary of Homeland Security; the Secretary of the Department of Energy; the Administrator of EPA; the Executive Director of the Federal Energy Regulatory Commission; appropriate congressional committees and other interested parties. In addition, the report is available at no charge on GAO's 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 VII.



Tina Won Sherman
Director, Homeland Security and Justice

List of Requesters

The Honorable Gary C. Peters
Chairman

The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Maggie Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kyrsten Sinema
Chair
Subcommittee on Government Operations and Border Management
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ron Johnson
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
United States Senate

The Honorable Mitt Romney
United States Senate

The Honorable Jacky Rosen
United States Senate

Appendix I: Critical Infrastructure Sectors and Their Sector Risk Management Agencies

Figure 9: Critical Infrastructure Sectors and Their Sector Risk Management Agencies



Sector-specific agency

USDA Department of Agriculture	HHS Department of Health and Human Services	TREASURY Department of the Treasury	<div style="background-color: #0070C0; width: 15px; height: 15px; display: inline-block; margin-right: 5px;"></div> Reflects the four selected sectors highlighted in this report
DOD Department of Defense	DHS Department of Homeland Security	EPA Environmental Protection Agency	
DOE Department of Energy	DOT Department of Transportation	GSA General Services Administration	

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-22-104279

Appendix II: Examples of Selected Department of Homeland Security Critical Infrastructure Prioritization Processes

The Department of Homeland Security (DHS) and its component agencies have various ways of identifying and prioritizing critical infrastructure. Cybersecurity and Infrastructure Security Agency (CISA) officials identified the following processes as examples of critical infrastructure identification and prioritization processes that are led by CISA’s National Risk Management Center (see table 5).

Table 5: Selected Department of Homeland Security (DHS) Critical Infrastructure Identification Processes and Results

Process	Description	Results
Electromagnetic Pulse	An electromagnetic pulse has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. The Electromagnetic Pulse List assesses which critical infrastructure systems, networks, and assets are most vulnerable to the effects of electromagnetic pulses.	List of critical infrastructure systems, networks, and assets most affected by an electromagnetic pulse event or attack
Infrastructure of Concern	DHS produces Infrastructure of Concern Lists to identify critical infrastructure and key resources in response to terrorist attacks, natural hazards, and other events. The information supports the activities of the department and informs the strategies of federal, state, local, and private sector partners to deter, prevent, preempt, and respond to terrorist attacks and other disruptions to infrastructure.	Prioritized list of infrastructure for significant federal response activities (such as response to fires or hurricanes)
High Value Asset	High Value Assets are federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U.S.’s national security interests, foreign relations, economy, or to the public confidence, civil liberties, or the public health and safety of the American people. The Office of Management and Budget directs agencies to “identify, categorize, and prioritize High Value Assets,” report High Value Assets to DHS annually, and ensure that appropriate protections improve High Value Asset security postures.	List of critical federal information systems and data
Section 9	Section 9 entities are critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. DHS is to use a risk-based approach to identify critical infrastructure.	List of critical infrastructure most affected by a cybersecurity incident
Information and Communication Technology () Supply Chain	Addresses the threat posed by the unrestricted acquisition or use of information and communication technology and services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries.	Assessment to identify entities, hardware, software, and services that present vulnerabilities, including an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers

Source: GAO analysis of DHS documents. | GAO-22-104279

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

February 10, 2022

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-22-104279, "CRITICAL INFRASTRUCTURE PROTECTION: CISA Should Improve Priority-Setting, Stakeholder Involvement, and Threat Information Sharing"

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.

The Department is pleased to note GAO's positive recognition of the National Critical Functions (NCF) framework, and the valuable information and services the Cybersecurity and Infrastructure Security Agency (CISA) provides to the critical infrastructure community. CISA remains committed to maturing approaches to risk identification, analysis, and management to address the complex and evolving risk landscape for critical infrastructure.

The draft report contained six recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

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: 2022.02.10 10:22:36
-05'00'

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

Attachment

**Attachment: Management Response to Recommendations
Contained in GAO-22-104279**

GAO recommended that the Director of CISA:

Recommendation 1: Ensure that its process for developing a prioritized list of critical infrastructure that would cause national or regional catastrophic effects if destroyed or disrupted reflects current threats.

Response: Concur. By August 2022, CISA's National Risk Management Center (NRMC) will complete an evaluation of existing nomination thresholds within the National Critical Infrastructure Prioritization Program (NCIPP) and the applicability of current thresholds to address current threats. Once complete, the NRMC will use this analysis as a baseline to support a more comprehensive update of nomination thresholds during Fiscal Year (FY) 2023, in coordination with Federal Interagency stakeholders (Sector Risk Management Agencies). Estimated Completion Date (ECD): September 30, 2023.

Recommendation 2: Ensure that its process for developing a prioritized list of critical infrastructure that would cause national or regional catastrophic effects if destroyed or disrupted includes input from additional states that have not provided recent nominations or updates.

Response: Concur. CISA NRMC will work with CISA Regional staff to make affirmative outreach to states who did not submit nominations in FY 2019, FY 2020, or FY 2021 to ensure these states are aware of the program and the process to submit nominations. During the next nomination data call, CISA NRMC will also provide an option for states to affirm that no new assets or nodes anticipated to reach nomination thresholds have begun operations and no assets or nodes currently on the NCIPP list have been taken offline. It is important to note that although CISA can request information from program participants, it cannot compel a response. The FY 2023 NCIPP nomination schedule has not yet been finalized, but is anticipated to begin in Spring 2022 with conclusion prior to the end of FY 2022. ECD: September 30, 2022.

Recommendation 3: Ensure that stakeholders are fully engaged in the implementation of the National Critical Functions framework.

Response: Concur. Since 2018, CISA NRMC, in collaboration with all CISA Divisions, has engaged with private sector and government partners in the development and application of the NCFs, and CISA is committed to continue, improve, and expand its engagement with stakeholders. To date, CISA has engaged through webinars, meetings with sector councils and cross-sector councils, workshops, and meetings with individual

public and private entities. In March 2021, CISA also established the Federal Risk Management Working Group through the Federal Senior Leadership Council which ensures federal partners, including Sector Risk Management Agencies, have a formal role in implementation of the NCF framework. Thus far, CISA developed 55 stakeholder linkage profiles for each NCF, as described in GAO's report, to ensure CISA understands the full range of stakeholders involved in addressing and supporting each function. Currently, CISA is using these stakeholder linkage profiles to form "Communities of Interest" for each NCF to provide input into framework development and support risk management activities. ECD: October 31, 2022.

Recommendation 4: Document, as appropriate, goals and strategies for the National Critical Functions framework, and integrate them with other efforts.

Response: Concur. CISA's Infrastructure Security Division is currently leading the review and coordination of an update to the "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," (the "National Plan"), which is anticipated to be completed during 2022. Once complete, CISA NRMC will leverage the National Plan to provide clear documentation of the goals and strategies for the NCFs. The coordination process for the National Plan will ensure that critical infrastructure stakeholders have an opportunity to refine communications, so they are clear and actionable and support robust engagement. ECD: October 31, 2022.

Recommendation 5: Implement processes to improve communication and coordination between critical infrastructure organizations and CISA headquarters and regional staff.

Response: Concur. On January 7, 2022, the CISA Director issued a memorandum titled: "Cybersecurity and Infrastructure Security Agency Operating Model Update" to update policies, and improve communication and coordination within CISA and with external stakeholders. This memorandum addresses: (1) programmatic direction; (2) service delivery; (3) incident coordination; (4) stakeholder engagement; (5) risk management; and (6) training. CISA's Assistant Director of Integrated Operations, who oversees the regional staff, will work with the other CISA Assistant Directors and Executive Assistant Directors to establish and document formal mechanisms for coordination and feedback concerning service delivery by the end of February 2022. ECD: February 28, 2022.

Recommendation 6: Coordinate with relevant regionally based, federal, and nonfederal partners to regularly develop and distribute regionally specific threat information to each of CISA's 10 regions.

Response: Concur. CISA, primarily through its Integrated Operations Division (IOD), continually works to disseminate unclassified threat products to regional partners who can take appropriate action in their areas of responsibility. In addition, depending on the

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

circumstance or emerging incident, CISA may proactively reach out to key partners and CISA regions to provide classified briefings. CISA IOD prioritizes regional-focused support to ensure threat information is provided in a timely fashion, and CISA's intelligence structure continues to mature in capacity with a focus on providing support to CISA's regions. Further, CISA continues to codify regional relationships with state and local fusion centers, the DHS Office of Intelligence and Analysis Field Operations Directorate, as well as other subject matter experts from across the intelligence community to improve collaboration. CISA is also currently in a pilot program with Regions 2 and 3 to support their intelligence requirements that will be completed in six months. ECD: July 29, 2022.

Appendix IV: GAO Contacts 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), Charlotte Gamble (Analyst-in-Charge), Michele C. Fejfar, Eric Hauswirth, Denton Herring, Tracey King, Terence Lam, Lerone Reid, and Adam Vogt made significant contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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

