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.

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
● Provide positioning, navigation, and timing services	● Distribute electricity	● Manage wastewater	● Manufacture equipment
● Provide satellite access network services	● Maintain supply chains	● Perform cyber incident management capabilities	● Produce and provide human and animal food products and services
● Provide wireless access network services	● Transport materials by pipeline	● Protect sensitive information	● 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.

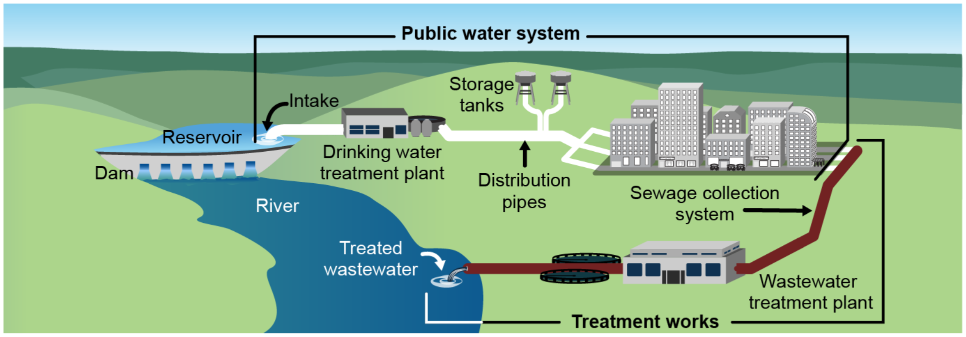
What GAO Recommends

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.

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

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.