GAO Highlights

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

Why GAO Did This Study

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

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

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

What GAO Recommends

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

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

April 6, 2022

CRITICAL INFRASTRUCTURE PROTECTION

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

What GAO Found

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

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

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

Examples of Critical Infrastructure

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