GAO Highlights

Highlights of GAO-22-105530, a testimony before the Committee on Transportation and Infrastructure, House of Representatives

December 2, 2021

CYBERSECURITY

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

Why GAO Did This Study

Federal agencies and the nation's critical infrastructure—such as transportation systems, energy, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

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.

In 2018, GAO reported that the federal government needed to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Within these four challenges are 10 actions critical to successfully dealing with the serious cybersecurity threats facing the nation (see the figure at right identifying the four challenges and 10 actions).

GAO was asked to testify on the federal government's efforts to address critical infrastructure cybersecurity. For this testimony, GAO relied on selected products it previously issued.

View GAO-22-105530. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

GAO has previously reported on major cybersecurity challenges facing the nation and the critical federal actions needed to address them (see figure).

Four Major Cybersecurity Challenges and 10 Associated Critical Actions

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government- wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis. | GAO-22-105530

To address critical infrastructure cybersecurity, key actions the federal government needs to take include (1) developing and executing a comprehensive national cyber strategy and (2) strengthening the federal role in protecting the cybersecurity of critical infrastructure.

Develop and execute a comprehensive national cyber strategy. In September 2020, GAO reported that the White House's 2018 National Cyber Strategy and related implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources. GAO also reported that it was unclear which official within the executive branch ultimately maintained responsibility for coordinating the execution of the National Cyber Strategy. Accordingly, GAO recommended that the National Security Council update the cybersecurity strategy and for Congress to consider legislation to designate a position in the White House to lead such an effort.

In January 2021, a federal statute established the Office of the National Cyber Director within the Executive Office of the President. In June 2021, the Senate confirmed a Director to lead this new office. In October 2021, the National Cyber Director issued a strategic intent statement, outlining a vision for the Director's planned high-level lines of efforts. The establishment of a National Cyber Director is an important step toward positioning the

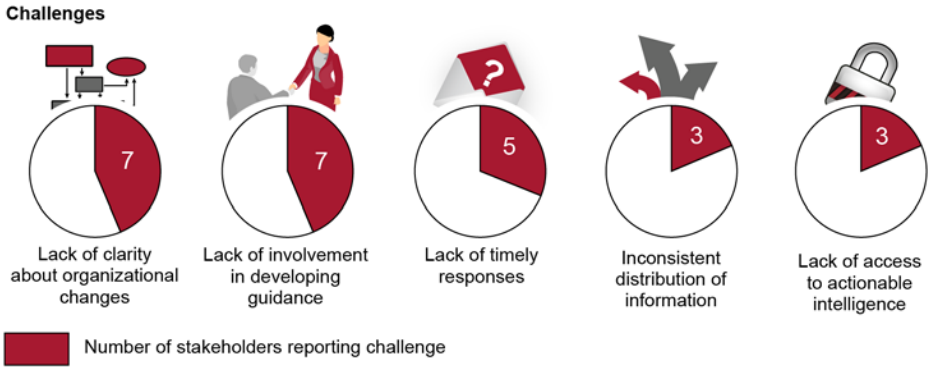
What GAO Recommends

Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of November 2021, about 900 of those recommendations were not yet implemented.

federal government to better direct activities to address the nation's cyber threats. Nevertheless, GAO's recommendation to develop and execute a comprehensive national cyber strategy is not yet fully implemented. As a result, a pressing need remains to provide a clear roadmap for addressing the cyber challenges facing the nation, including its critical infrastructure.

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 the Department of Homeland Security (DHS) was charged with responsibility for, among other things, 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, including 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 (see figure). Accordingly, GAO made 11 recommendations to DHS. As of November 2021, DHS had not yet implemented them, though it stated its intent to do so.

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



Source: GAO analysis of stakeholder interviews. | GAO-22-105530

Regarding specific critical infrastructure sectors, since 2010 GAO has made about 80 recommendations to enhance the cybersecurity of these sectors and subsectors, including within the aviation and pipeline industries. In October 2020, GAO reported that, although the Federal Aviation Administration had established a process for certification and oversight of U.S. commercial airplanes, it had not prioritized risk-based cybersecurity oversight or included periodic testing as part of its monitoring process, among other things. In July 2021, GAO testified that the Transportation Security Administration had not fully addressed pipeline cybersecurity-related weaknesses that GAO had previously identified, such as aged protocols for responding to pipeline security incidents. Until GAO's recommendations to address issues such as these are fully implemented, federal agencies will not be effectively positioned to ensure critical infrastructure sectors are adequately protected from potentially harmful cybersecurity threats.