GAO@100

Highlights

Highlights of GAO-21-288, a report to congressional addressees

March 2021

HIGH-RISK SERIES

Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, 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).

This report provides an update on the progress that the federal government has made in addressing GAO's recommendations for the four major cybersecurity challenges, as of December 2020.

View GAO-21-288. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov, or Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

GAO reiterates the importance of addressing the four major cybersecurity challenges and the 10 associated critical actions listed below.

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-21-288

As described below, although the federal government has made selected improvements, it needs to move with a greater sense of urgency commensurate with the rapidly evolving and grave threats to the country.

- **Establishing a comprehensive cybersecurity strategy and performing effective oversight**. The prior administration's September 2018 national cybersecurity strategy and the June 2019 implementation plan detail the executive branch's approach to managing the nation's cybersecurity. In September 2020 GAO reported that the national strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed. The new administration needs to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics.

  GAO also highlighted the urgent need to clearly define a central role for leading the implementation of the national strategy. Accordingly, it recommended that the Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, the Congress did so by establishing the Office of the National Cyber Director within the Executive Office of the President. Once the position is filled, the federal government will be better situated to direct activities to overcome the nation's cyber threats and challenges, and to perform effective oversight.

In performing its work, GAO generally reviewed the cybersecurity-related products it had issued since September 2018. It also assessed actions taken on prior GAO recommendations, and determined which recommendations had not yet been implemented. Further, GAO identified its relevant ongoing cybersecurity work. Finally, GAO reviewed cybersecurity findings from agency inspector general reports, and analyzed the recommendations of the U.S. Cyberspace Solarium Commission.

What GAO Recommends

Since 2010, GAO has made about 3,300 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of December 2020, more than 750 of those recommendations are not yet implemented.

GAO requested comments on a draft of this report from the Department of Homeland Security (DHS), National Security Council (NSC), and Office of Management and Budget (OMB). DHS provided technical comments, which were incorporated as appropriate. NSC staff and OMB's liaison to GAO both provided comments via email.

NSC staff stated that, as the administration charts a course for cyber policy issues, the draft offered a comprehensive review of the cybersecurity challenges facing the nation and the opportunities available to make concrete improvements. Further, NSC staff described the administration's preliminary views about the four major cybersecurity challenges identified in the report.

In its comments, OMB highlighted ongoing and planned efforts that the office is taking for two major challenges—securing federal systems and information and protecting privacy and sensitive data.

Although establishing the Cyber Director position is an essential step forward, critical risks remain on supply chains, workforce management, and emerging technologies. For example, in December 2020, GAO reported that none of the 23 agencies in its review had fully implemented key foundational practices for managing information and communications technology supply chains. It made a total of 145 recommendations to the agencies to implement such practices in their approaches to supply chain management.

- **Securing federal systems and information**. The federal government has made some progress in securing systems. Nevertheless, federal agencies continue to have numerous cybersecurity weaknesses due in large part to ineffective information security programs. Further, cyber incidents are increasingly posing a threat to government and private sector entities. The seriousness of the threat was reinforced by the December 2020 discovery of a cyberattack that has had widespread impact on government agencies, critical infrastructures, and the private sector. In 2019 GAO reported that most of the 16 agencies reviewed had incident response processes with key shortcomings thereby limiting the ability to minimize damage from attacks.
- **Protecting cyber critical infrastructure**. The nation's critical infrastructure includes both public and private systems vital to national security and other efforts including providing the essential services that underpin American society. Since 2010, GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity; for example, GAO recommended that agencies better measure the adoption of the National Institute of Standards and Technology framework of voluntary cyber standards and correct sector-specific weaknesses. However, most of these recommendations (nearly 50) have not been implemented. As a result, the risks of unprotected infrastructures being harmed are heightened.
- **Protecting privacy and sensitive data**. The federal government and private sector have struggled to protect privacy and sensitive data. Advances in technology have made it easy to correlate information about individuals and ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities. The vast number of individuals affected by various data breaches has underscored concerns that personally identifiable information is not adequately being protected. GAO's reviews of agency practices to protect sensitive data have identified weaknesses and made numerous recommendations at agencies such as the Department of Housing and Urban Development, Department of Education, and Internal Revenue Service.

  In January 2019, GAO reported that the United States did not have a comprehensive internet privacy law governing the collection, use, and sale or other disclosure of consumers' personal information. Accordingly, GAO recommended that the Congress consider developing legislation on internet privacy that, among other things, would enhance consumer protections.