U.S. GOVERNMENT ACCOUNTABILITY OFFICE

CYBERSECURITY HIGH-RISK SERIES:

Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government should do the following:

- Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace
- Mitigate global supply chain risks (e.g., installation of malicious software or hardware)
- Address cybersecurity workforce management challenges
- Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things)

Overview

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on technology systems to carry out fundamental operations and to process, maintain, and report vital information. The security of these systems and data is also vital to safeguarding individual privacy and protecting the nation's security, prosperity, and well-being.

However, risks to these essential technology systems are increasing—in particular, malicious actors are becoming more willing and capable of carrying out cyberattacks. Such attacks could result in serious harm to human safety, national security, the environment, and the economy. Agencies and critical infrastructure owners and operators must protect the confidentiality, integrity, and availability of their systems and effectively respond to cyberattacks.

We have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure. In 2015, we expanded it again to include protecting the privacy of personally identifiable information.

This is the first in a series of four reports that lay out the main cybersecurity areas the federal government should urgently address, beginning with the need for a comprehensive strategy and effective oversight.[1] We have made about 335 recommendations in public reports since 2010 with respect to this area. About 190 of these recommendations were not implemented as of December 2022. Until these are fully implemented, federal agencies will be more limited in their ability to protect private and sensitive data entrusted to them.

For more information on this report and others in this series, visit https://www.gao.gov/cybersecurity.

What actions can the federal government take to execute a more comprehensive federal cyber strategy?

The federal government needs to address missing elements in the *National Cyber Strategy* and *Implementation Plan*.

The White House's September 2018 *National Cyber Strategy* and the National Security Council's (NSC) accompanying June 2019 *Implementation Plan* detail the executive branch's approach to managing the nation's cybersecurity. In September 2020, we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies. In particular, the *National Cyber Strategy*, when combined with the *Implementation Plan*, addressed three of the six desirable characteristics of national strategies but did not include key elements for three other characteristics (see figure 1). We stressed that moving forward, the incoming administration needed to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics.

[1]In 2018, GAO reported that the federal government needed to address four major cybersecurity challenges related to (1) establishing a comprehensive cybersecurity strategy, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.

Figure 1: Extent to Which the National Cyber Strategy and Implementation Plan Addressed the Desirable Characteristics of a National Strategy

Characteristic	Extent addressed
Purpose, scope, and methodology	●
Organizational roles, responsibilities, and coordination	●
Integration and implementation	●
Problem definition and risk assessment	○
Goals, subordinate objectives, activities, and performance measures	○
Resources, investments, and risk management	○

● Addressed—The *National Cyber Strategy*, when combined with the *Implementation Plan*, fully addressed the desirable characteristics associated with this subcategory.
○ Did not fully address—The *National Cyber Strategy*, when combined with the *Implementation Plan*, did not fully address the desirable characteristics associated with this subcategory.

Source: GAO analysis of 2018 *National Cyber Strategy* and 2019 *Implementation Plan*. | GAO-23-106415

The Congress and Administration took action to establish and fill a critical cybersecurity leadership position. Specifically, in January 2021, the National Defense Authorization Act for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President. In June 2021, the Senate confirmed the first National Cyber Director to head the office and serve as the principal advisor to the President on cybersecurity policy and strategy. The Director subsequently issued a strategic statement for the office that summarized its vision, challenge, path, and urgency to improve the nation's cybersecurity. However, until the federal government fully develops and implements a comprehensive national strategy, it will not have a clear roadmap for overcoming the cyber challenges facing our nation.

- **We recommended** that the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include goals, performance measures, and resource information, among other things. As of August 2022, according to the Office of the National Cyber Director, the development of a national cybersecurity strategy by the administration is underway. The office noted that it is obtaining feedback on the strategy from many other federal entities, including the National Security Council, on this effort.

What actions can the federal government take to mitigate global supply chain risks?

Federal agencies need to fully implement all of the foundational practices for supply chain risk management.

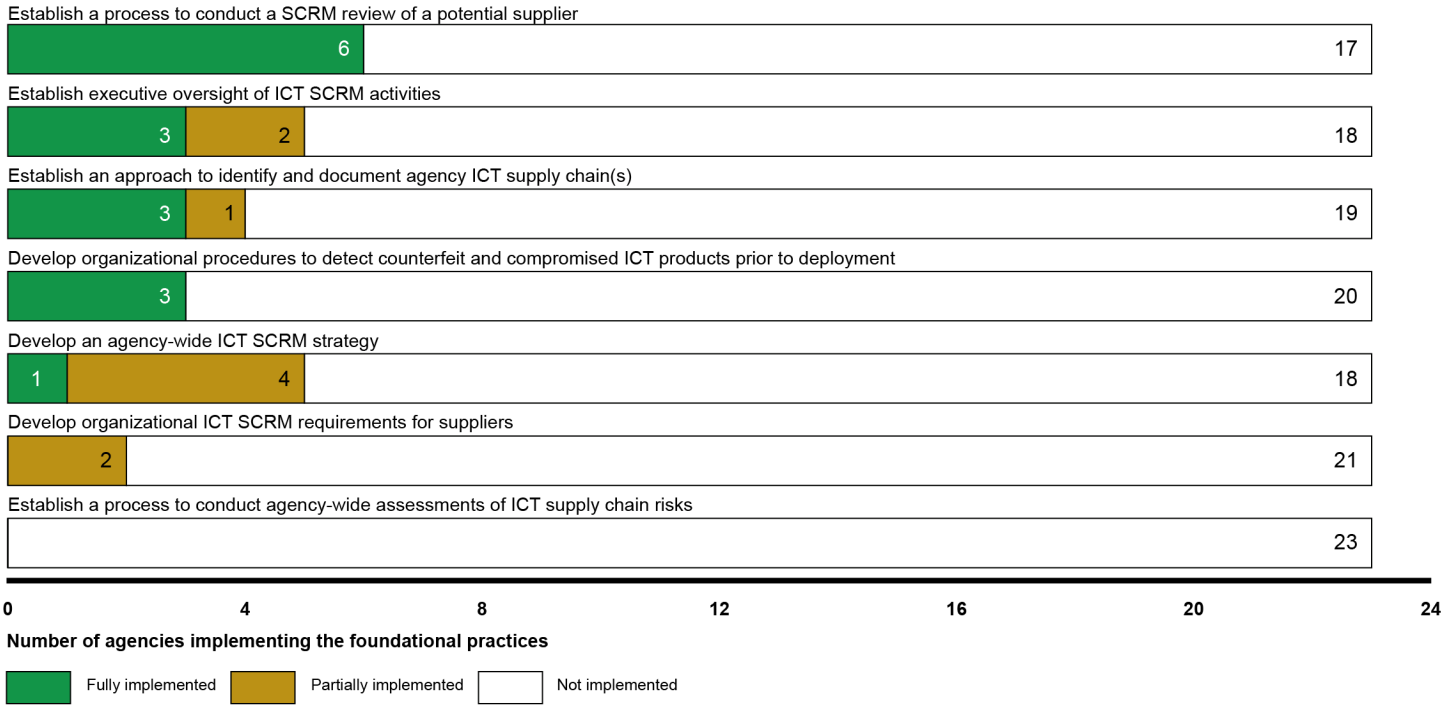
Federal agencies rely extensively on information and communications technology (ICT) products and services to carry out their operations. However, agencies face numerous ICT supply chain risks, including threats posed by counterfeiters who may exploit vulnerabilities in the supply chain. To assist agencies with effectively managing their ICT supply chain risks, the National Institute of Standards and Technology developed guidance that includes risk-based practices.

In December 2020, our review of 23 civilian agencies found that none had fully implemented all of the seven foundational practices for supply chain risk management and that 14 had not implemented any of the practices (see figure 2).[2] For example, only three out of the 23 agencies had fully developed organizational procedures to detect counterfeit and compromised ICT products prior deployment. In addition, none of the 23 agencies had established a process to conduct agency-wide assessments of ICT

[2]The 23 civilian agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. We did not include the Department of Defense because our scope was the civilian agencies.

supply chain risks. Implementing foundational practices for ICT supply chain risk management is essential to agencies addressing the risks of malicious actors disrupting mission operations, stealing intellectual property, or harming individuals.

Figure 2: Extent to Which the 23 Civilian Agencies Implemented Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Practices



Source: GAO analysis of agency data. | GAO-23-106415

- **We recommended** that the 23 agencies fully implement foundational practices in their organization-wide approaches to ICT supply chain risk management.[3] As of December 2022, 130 of our 145 recommendations were not yet implemented; none of the 23 agencies had fully implemented all recommendations addressed to them.

What actions can the federal government take to address cybersecurity workforce challenges?

The Office of Management and Budget (OMB) should develop a government-wide plan to address the cybersecurity workforce shortage.

In April 2020, we examined the extent to which OMB and lead agencies addressed key practices for effectively implementing selected government-wide reforms (see figure 3). These included reforms that prioritized solving the cybersecurity workforce shortage by identifying and closing workforce skills gaps and developing a standardized approach to hiring, training, and retaining qualified cybersecurity professionals.

[3]In the sensitive version of this report issued in October 2020, GAO-21-164SU, we made 145 recommendations to the 23 agencies.

Figure 3: Extent to Which the Government-Wide Plan to Solve the Cybersecurity Workforce Shortage Addressed Key Reform Practices

Key reform practice	Extent addressed	Summary of findings
Establishing goals and outcomes	◐	The Department of Homeland Security (DHS) established goals and outcomes for certain projects and activities, but the Office of Management and Budget (OMB) and DHS have not developed government-wide goals and outcomes.
Involving employees and key stakeholders	◐	DHS conducted outreach to employees and key stakeholders for certain projects and activities but not for the reform as a whole.
Addressing high-risk areas and long-standing management challenges	◐	OMB and DHS have acknowledged cybersecurity challenges, such as our high-risk area of protecting cyber critical infrastructure, but they have not demonstrated how the reform proposal will address these challenges.
Leadership focus and attention	◐	While a May 2019 Executive Order demonstrated high-level leadership attention, OMB and DHS have not yet established a dedicated government-wide implementation team.
Managing and monitoring	◐	While DHS has developed some agency-specific implementation plans and mechanisms to monitor progress, OMB and DHS have not developed an implementation plan with time lines, key milestones, and deliverables for the reform proposal as a whole.
Strategic workforce planning	◐	DHS developed its cybersecurity workforce strategy as required by the Cybersecurity Workforce Assessment Act. OMB and DHS have not developed a government-wide cybersecurity strategic workforce plan.
Employee engagement	○	OMB and DHS have not yet demonstrated how they are monitoring, sustaining, and strengthening employee engagement of affected cybersecurity professionals across the federal government.

◐ Partially addressed—OMB and DHS addressed a practice with significant gaps in their coverage of the actions associated with this subcategory.
○ Not addressed—OMB and DHS did not address this practice or demonstrate coverage of associated actions with this subcategory.

Source: GAO analysis of agencies' plans. | GAO-23-106415

We found that OMB and the Department of Homeland Security (DHS) partially addressed most of the key practices associated with effective reforms through their efforts to implement several projects, such as training employees to fill vacant cybersecurity positions and streamlining hiring processes. However, OMB and DHS had not established a dedicated implementation team or a government-wide implementation plan, among other practices. Without these practices in place, OMB and DHS will likely be unable to make significant progress towards solving the cybersecurity workforce shortage.

- **We recommended** several actions aimed at addressing continuing cybersecurity workforce challenges. These recommendations focused on developing a government-wide workforce plan and related supporting practices such as establishing a leadership team and crafting an implementation plan. Government-wide leadership responsibility for cyber workforce issues transitioned in 2022 from OMB and DHS to the Office of the National Cyber Director. Since the transition, the Director has committed to developing a national strategy that addresses cyber training and education, digital awareness, and the cyber workforce. This commitment is consistent with the current Administration's management agenda, which states that the Administration must identify and address critical skills gaps across the federal IT and cybersecurity workforce. We will continue monitoring efforts to develop the strategy.

What actions can the federal government take to ensure the security of emerging technologies?

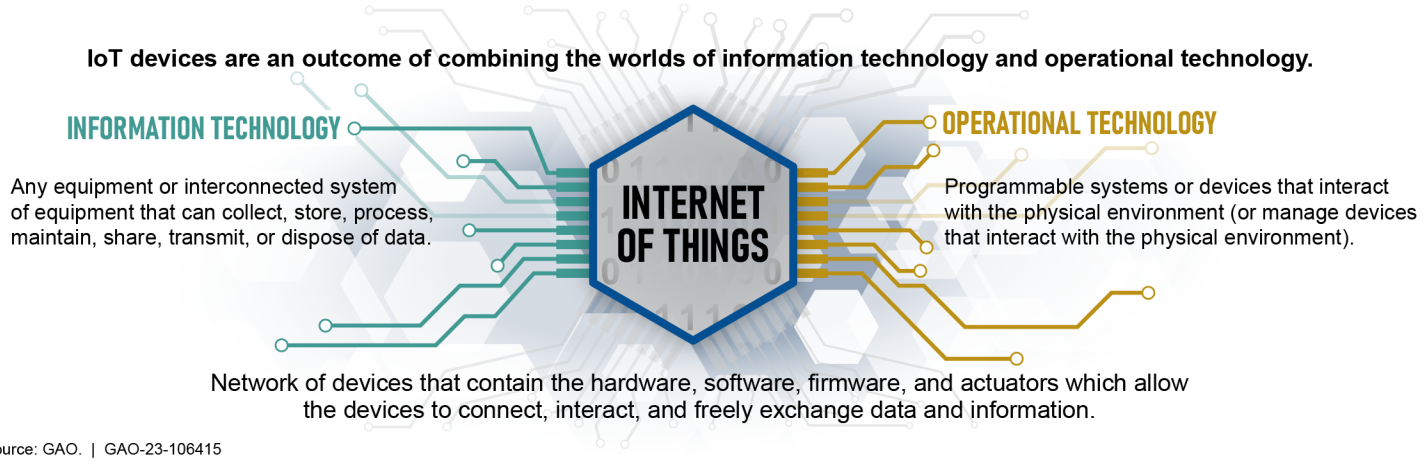
Federal agencies need to take action to better secure internet-connected devices.

The nation's critical infrastructure sectors rely on electronic systems, including Internet of Things (IoT) and operational technology (OT) devices and systems (see figure 4).[4] In December 2022, we reported that the federal lead agencies of the reviewed critical infrastructure sectors—the Departments of Energy, Health and Human Services, Homeland Security, and Transportation—had cybersecurity initiatives underway

[4]IoT generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of "things," throughout such places as buildings, transportation infrastructure, or homes. OT are programmable systems or devices that interact with the physical environment, such as building automation systems that control machines to regulate and monitor temperature.

intended to help protect three critical infrastructure sectors with extensive use of IoT or OT devices and systems.

Figure 4: Overview of Connected IT, Internet of Things (IoT), and Operational Technology



Source: GAO. | GAO-23-106415

However, none of the lead agencies had developed metrics to assess the effectiveness of their efforts. Further, the agencies had not conducted IoT and OT cybersecurity risk assessments. While agency officials noted difficulty assessing program effectiveness when relying on voluntary information from sector entities, the success of initiatives intended to mitigate risks is unknown without attempts to measure effectiveness and assess risks of IoT and OT.

- **We recommended** that the Departments of Energy, Health and Human Services, Homeland Security, and Transportation to establish and use metrics to assess the effectiveness of sector IoT and OT cybersecurity efforts and evaluate sector IoT and OT cybersecurity risks. As of December 2022, none of these recommendations had been implemented.

Quantum computing has the potential to create major cybersecurity risks.

We reported in September 2022 that quantum technologies build on the study of the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies. Quantum computers could dramatically accelerate computation for some applications, such as machine learning and information decryption. In addition, quantum information technologies could dramatically increase capabilities beyond what is possible with classical technologies, such as having high-value applications in security and cryptography. However, quantum computing has the potential to create major cybersecurity risks. For example, a full-scale quantum computer has the potential to break standard encryption technologies, creating a major information security risk. As a result, the federal government's cybersecurity infrastructure will need to evolve to address this threat.

As artificial intelligence (AI) technologies continue to advance, federal oversight considerations will need to evolve.

In March 2021, we reported that AI might have a number of associated challenges and risks. For example, if the data used by AI are biased or become corrupted by hackers, the results could be biased or cause harm. In March 2021, the National Security Commission on Artificial Intelligence issued a report in which the commission described additional cybersecurity risks associated with AI and recommendations to address them.[5] Specifically, the commission stated that AI would enable malware to mutate into thousands of different forms, find vulnerabilities, and attack selectively. The commission added that the

[5]Section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the National Security Commission on Artificial Intelligence as an independent commission to consider the methods and means necessary to advance the development of AI, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States. Pub. L. No. 115-232, § 1051, 132 Stat. at 1962.

National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

expanding application of AI cyber capabilities would make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale. The federal government will need to take appropriate action to address these threats.

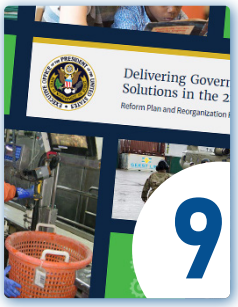
GAO's Prior Work

We have previously reported on the numerous challenges that the federal government faces and have made recommendations aimed at establishing a comprehensive cybersecurity strategy and performing effective oversight. Key reports focus on the following topics:

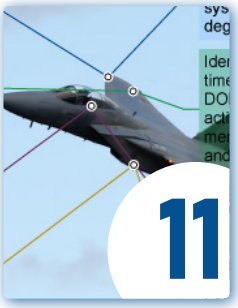
Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace

Mitigate global supply chain risks

Address cybersecurity workforce management challenges



Ensure the security of emerging technologies



Source: Images: (1, 7) VideoFlow/stock.adobe.com, (2) Maksim Kabakou/stock.adobe.com, (3, 4, 5) GAO File Photo, (6) weerapat1003/stock.adobe.com, (8) Andrey Popov/stock.adobe.com, (9) Executive Office of the President, (10) GAO analysis of Ericsson data, (11) GAO analysis of Congressional Research Service data, (12) metamorworks/stock.adobe.com, (13) GAO analysis of Department of Defense (DOD) information; Thaut Images/stock.adobe.com and U.S. Air Force/Staff Sgt. E. Nuñez (photos).

Contact Us:

For more information about this Cybersecurity High Risk Series, contact Marisol Cruz Cain, Director, Information Technology and Cybersecurity, (202) 512-5017.

Chuck Young, Managing Director, Public Affairs, (202) 512-4800

A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-4400

Contributors: Lauri Barnes, Chris Businsky, Corwin Hayward, Elena Epps (Assistant Director), and Keith Kim (Analyst-in-Charge)

Source (cover photo): GAO analysis; Who is Danny/stock.adobe.com.