U.S. GOVERNMENT ACCOUNTABILITY OFFICE

CYBERSECURITY HIGH-RISK SERIES:

Challenges in Securing Federal Systems and Information

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 second in a series of four reports that lay out the main cybersecurity areas the federal government should urgently address. It focuses on securing federal systems and information.[1] We have made 712 recommendations in public reports since 2010 in this area. About 150 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 should be taken to improve the implementation of government-wide cybersecurity initiatives?

The Cybersecurity and Infrastructure Security Agency (CISA) should complete its organizational transformation and fulfill its mission of protecting civilian agency systems and networks.

The CISA Act of 2018 (the act) established CISA within the Department of Homeland Security (DHS) to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure.[2] The act also assigned five key cybersecurity responsibilities to CISA, including securing federal information and systems, coordinating federal efforts to secure and protect against critical infrastructure risk, and carrying out emergency communication stakeholder outreach (see figure 1).

---

[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. For our report on the first challenge area, see GAO, *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight.* GAO-23-106415 (Washington, D.C.: Jan. 19, 2023).

[2]CISA Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169-70, section 2202(a)(1) (codified at 6 U.S.C. section 652c).

Figure 1: Five Key Responsibilities Assigned to the Cybersecurity and Infrastructure Security Agency

Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency Act of 2018; images: Buffaloboy/stock.adobe.com. | GAO-23-106428

To implement these responsibilities, CISA undertook a three-phased organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience. Also, since its establishment, CISA has been reorganizing offices and functions previously organized under the department's National Protection and Programs Directorate and aligning its new organizational structure with its mission.

In March 2021, we reported that CISA had completed 37 of 94 planned implementation tasks. Critical transformation tasks such as finalizing the mission-essential functions of CISA's divisions and defining incident management roles and responsibilities across the agency had not yet been completed. We also reported that the agency had not established an updated overall deadline for completing its transformation initiative.

Until CISA establishes updated milestones and an overall deadline for its efforts, and expeditiously carries out these plans, the agency will be hindered in meeting the goals of its organizational transformation initiative. Consequently, this could impair the agency's ability to identify and respond to cyber incidents.

- **We recommended** that CISA establish expected completion dates, plans for developing performance measures, and an overall deadline for the completion of the transformation initiative, as well as develop a strategy for comprehensive workforce planning. DHS agreed with our recommendations. As of December 2022, it had not yet implemented any of them.

What actions can be taken to address weaknesses in federal agency information security programs?

Since 2020, we have reported on government-wide and multiple individual agencies' management of the information security risk to their systems and data. The individual agencies we reviewed were the U.S. Secret Service, the Department of Defense (DOD), the U.S National Institutes of Health (NIH), and the Federal Communications Commission. Key examples include:

The Office of Management and Budget (OMB) should update inspectors general (IG) reporting guidance to increase rating consistency and precision.

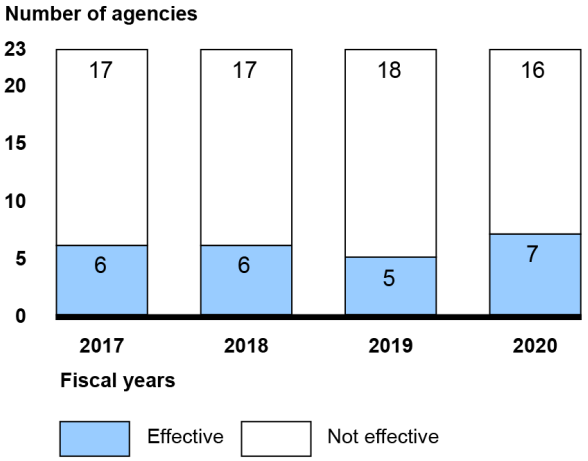
To protect federal information and systems, the *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies to develop, document, and implement information security programs. Congress included a provision in FISMA for GAO to periodically report on agencies' implementation of the act.

In March 2022, we reported on the information security programs of 23 federal civilian agencies, including annually required program reviews to be conducted by agency IGs. Among other things, we noted that IGs determined that 16 (or 70 percent) of the 23 agencies had ineffective programs for fiscal year 2020.[3] Figure 2 shows the number of

[3]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; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office

the 23 agencies that IGs rated as effective and not effective between fiscal years 2017 and 2020.

Figure 2: Number of the 23 Civilian Agencies with Effective and Not Effective Agency-Wide Information Security Programs, as Reported by Inspectors General for Fiscal Years 2017-2020



Source: GAO analysis of inspector general report data and Office of Management and Budget's *Federal Information Security Modernization Act of 2014* reports to Congress. | GAO-23-106428

We found that OMB's guidance to IGs on conducting agency evaluations was not always clear, leading to inconsistent application and reporting by IGs. Further, we reported that the binary effective/not effective scale resulted in imprecise ratings that did not clearly distinguish among the differing levels of agencies' performance. By clarifying its guidance and enhancing its rating scale, OMB could help ensure a more consistent approach and nuanced picture of agencies' cybersecurity programs.

- **We recommended** that OMB, in consultation with others, clarify its guidance to IGs and create a more precise overall rating scale. OMB did not concur with our recommendations, stating, in part, that they want to provide IGs with the flexibility to adapt their reviews. GAO maintains that the recommendations are warranted, but they had not yet been implemented as of December 2022.

The U.S. National Institutes of Health needs to resolve control deficiencies and improve its program.

NIH's duties include researching infectious diseases and administering over $30 billion a year in research grants. NIH uses IT systems containing sensitive data to carry out its mission.

In December 2021, we reported that NIH implemented information security controls—both for its security program and selected systems—intended to safeguard the confidentiality, integrity, and availability of its systems and information. However, we identified numerous control and program deficiencies in core security functions. These issues related to identifying risk, protecting systems from threats and vulnerabilities, detecting and responding to cyber security events, and recovering system operations. Until NIH resolves the associated control and program deficiencies, its information systems and information will remain at increased risk of misuse, improper disclosure or modification, and destruction.

- **We recommended** that NIH address these deficiencies, which resulted in 66 recommendations related to the security program and 153 recommendations related to system controls. As of December 2022, NIH had implemented about 71 percent of the total 219 recommendations. However, it had not yet implemented 15

of Personnel Management; the Small Business Administration; the Social Security Administration; and the U.S. Agency for International Development. We did not include the Department of Defense because our scope was the civilian agencies.

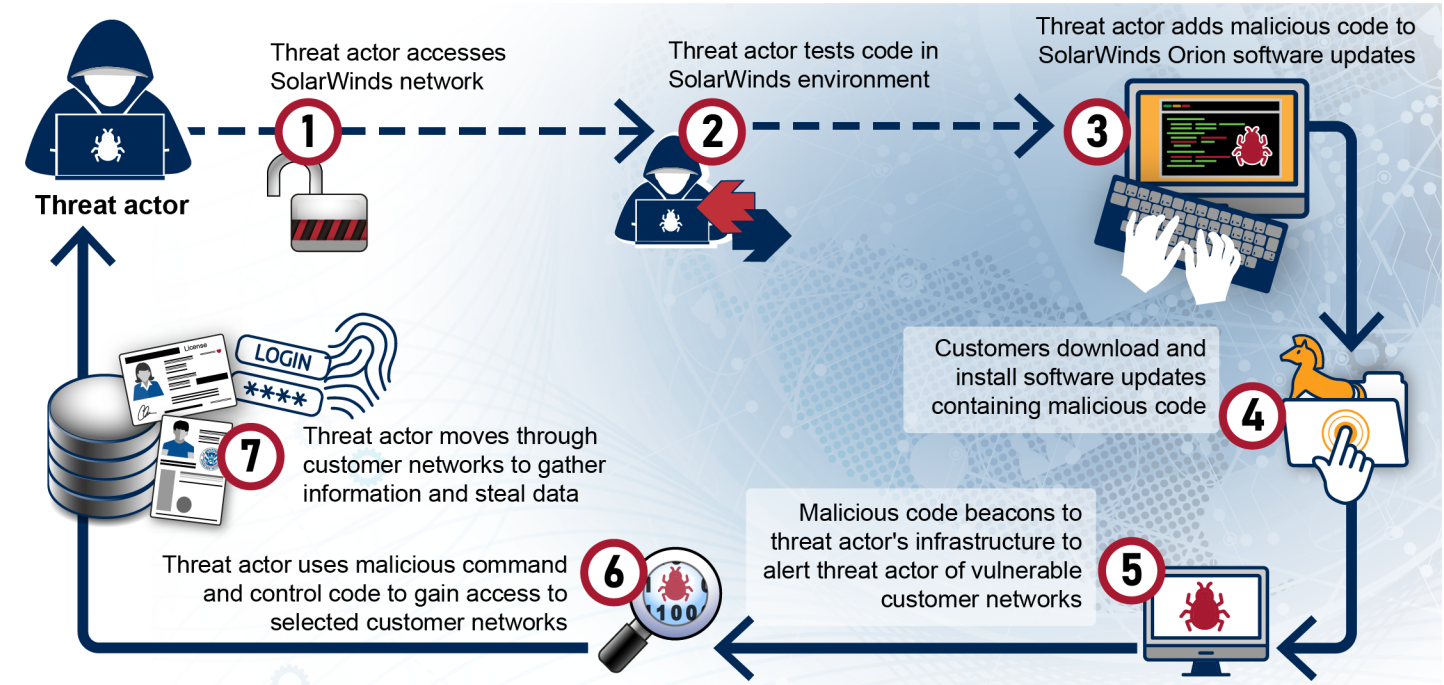
of the 66 on the information security program and 49 of the 153 on control deficiencies for selected systems.

What actions can be taken to enhance the federal response to cyber incidents targeting federal systems?

Agencies identified multiple lessons learned from SolarWinds and Microsoft Exchange incidents.

Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company. Since the company's software was widely used in the federal government, this incident allowed the threat actor to breach several federal agencies' networks that used the software (see figure 3). In March 2021, Microsoft reported the exploitation or misuse of vulnerabilities to gain access to versions of the Microsoft Exchange Server that federal agencies hosted and used. Federal agencies formed Cyber Unified Coordination Groups to investigate the incidents.[4]

Figure 3: Analysis of How a Threat Actor Exploited SolarWinds Orion Software



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-23-106428

In January 2022, we reported that the Cyber Unified Coordination Group agencies identified that information sharing and limited evidence collection led to challenges in coordinating and responding to the SolarWinds and Microsoft Exchange incidents. For example, we reported that an official from the Office of the Director of National Intelligence told us that information sharing among law enforcement, private sector, and intelligence groups was difficult and time consuming, as there were different classification levels for information.

In addition, the National Security Council, with input from the Cyber Unified Coordination Group agencies, conducted a review of the SolarWinds incident. The review identified that (1) aligning technology investments with operational priorities, (2) improving public-private engagement, and (3) improving threat intelligence acquisition, sharing, and use among federal agencies may help with preventing and responding to future cybersecurity incidents. If implemented effectively, the areas from the National

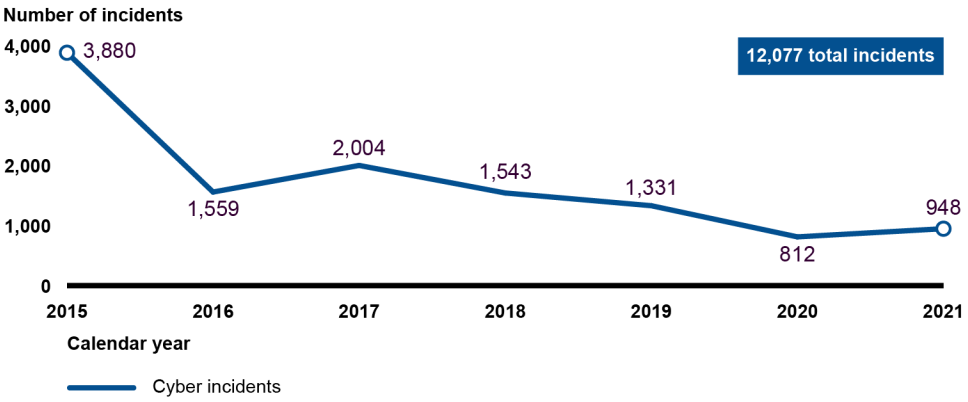
[4]Cyber Unified Coordination Group agencies for the SolarWinds and Microsoft Exchange incidents consisted of the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Office of the Director of National Intelligence, with support from the National Security Agency.

Security Council review could help address several challenges identified for both the SolarWinds and Microsoft Exchange incidents. We did not make any recommendations in this report, but we maintain that addressing these challenges should remain a priority.

The Department of Defense needs to ensure cyber incidents are appropriately reported and shared.

DOD and our nation's defense industrial base—which includes entities outside the federal government that provide goods or services critical to meeting U.S. military requirements—are dependent on information systems to carry out their operations. These systems continue to be susceptible to cyber incidents as cybersecurity threats have evolved and become more sophisticated (see figure 4).

Figure 4: Cyber Incidents Reported by Department of Defense's Cybersecurity Service Providers from Calendar Years 2015 through 2021



Source: GAO analysis of Department of Defense Joint Incident Management System (JIMS) data. | GAO-23-106428

In November 2022, we reported that DOD has taken steps to combat these attacks and the number of cyber incidents had declined in recent years. However, we found that the department (1) had not fully implemented its processes for managing cyber incidents, (2) did not have complete data on cyber incidents that staff report, and (3) did not document whether it notifies individuals whose personal data is compromised in a cyber incident. For example, DOD's system for reporting all incidents often contained incomplete information, and DOD could not always demonstrate that it had notified appropriate leadership of relevant critical incidents. Without addressing these deficiencies, DOD cannot ensure its leadership has an accurate understanding of the department's cybersecurity posture.

In addition, according to officials, DOD has not yet decided whether the defense industrial base's cyber incidents detected by cybersecurity service providers should be shared with all relevant stakeholders, such as the Department of Defense Chief Information Officer, Under Secretary of Defense for Intelligence and Security, and Defense Counterintelligence and Security Agency. Until DOD examines whether this information should be shared with all relevant parties, opportunities could be lost to identify system threats and improve system weaknesses.

- **We recommended** that the Department of Defense improve the sharing of defense industrial base-related cyber incident information and document when affected individuals are notified of a PII breach of their data. DOD concurred with our recommendations; however, it had not yet implemented these recommendations as of December 2022.

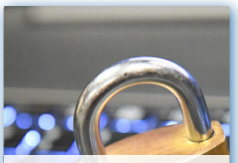
GAO's Prior Work

We have previously reported on the numerous challenges that the federal government faces and have made recommendations aimed at securing federal systems and information. Key reports focus on the following topics:

Improve the Implementation of Government-Wide Cybersecurity Initiatives

Cloud Computing: Federal Agencies Face Four Challenges **1**

Cybersecurity: OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision **2**



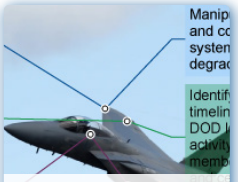
Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitorin Program **3**

Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed **4**

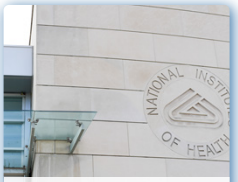
Federal Information Security: Agencies and OMB Need to Strengthen Policie and Practices **5**

Address Weaknesses in Federal Agency Information Security Programs

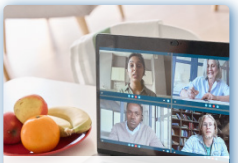
Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains **6**



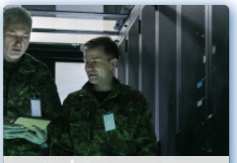
Information Environment: Opportunities and Threats to DOD's National Security Mission **7**



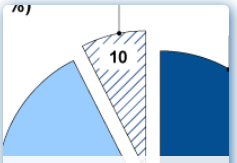
Cybersecurity: NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program **8**



COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls **9**



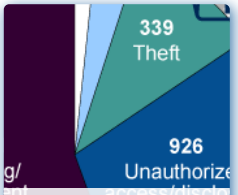
Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors **10**



Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program **11**

Enhance the Federal Response in Cyber Incidents Targeting Federal Systems

DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Re and Shared **12**



Electronic Health Information: HHS Needs to Improve Communications Breach Reportin **13**

Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents **14**

Source: Images: (1, 10) Gorodenkoff/stock.adobe.com, (2, 14) Alex/stock.adobe. com, (3, 5, 8) GAO file photo, (4) GAO, (6) ArtemisDiana/stock.adobe.com, (7) GAO analysis of Department of Defense (DOD) information; Thaut Images/stock.adobe.com and U.S. Air Force/Staff Sgt. E. Nuñez (photos), (9) insta_photos/stock.adobe.com, (11) GAO analysis of Federal Communications Commission data, (12) Maksim Kabakou/stock.adobe.com, (13) GAO analysis of Department of Health and Human Services' January 2022 data; images: bearsky23/stock.adobe.com, Chor muang/stock.adobe.com. GAO-23-106428

About GAO:

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. This document is based on GAO audit products. This work of the United States may include copyrighted material, details at https://www.gao.gov/copyright.

U.S. Government Accountability Office, 441 G Street NW, Washington, DC 20548

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: Elena Epps (Assistant Director), Keith Kim (Analyst-in-Charge), Freda Paintsil, Ibrahim Suleman, Lauri Barnes, and Chris Businsky

Source (cover photo): GAO analysis; images: Gorodenkoff/stock.adobe.com.