GAO Highlights

Highlights of GAO-24-107231, a report to congressional addressees

June 2024

HIGH-RISK SERIES

Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures depend 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 important to safeguarding individual privacy and protecting the nation's 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 the cybersecurity of critical infrastructure in 2003 and 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 the cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data. Within these four challenges are 10 actions essential to successfully dealing with the serious cybersecurity threats facing the nation.

GAO's objective was to describe the challenges facing the federal government in ensuring the cybersecurity of the nation and the progress it has made in addressing these challenges. To do so, GAO identified its recent public reports related to each challenge and summarized relevant findings from this work. GAO also determined the implementation status of relevant recommendations made in these reports. Further, GAO identified its ongoing and upcoming work covering each of the 10 critical actions needed to address the four major cybersecurity challenges.

View GAO-24-107231. For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.

Risks to our nation's essential technology systems are increasing. Threats to these systems can come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Federal agencies reported 30,659 information security incidents to the Department of Homeland Security's United States Computer Emergency Readiness Team in fiscal year 2022. Such attacks could result in serious harm to human safety, national security, the environment, and the economy.

Concerted action among the federal government and its nonfederal partners is critical to mitigating the risks posted by cyber-based threats. Recognizing the growing threat, the federal government urgently needs to take action to address the four major cybersecurity challenges and 10 associated critical actions (see figure 1).

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions

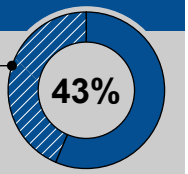
Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting the cybersecurity of critical infrastructure	Protecting privacy and sensitive data
Develop and execute a more comprehensive federal strategy for national cybersecurity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

Sources: GAO (analysis and icons), Who is Danny/stock.adobe.com (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); https://www.whitehouse.gov (logo). | GAO-24-107231

Since 2010, GAO has made 1,610 recommendations in public reports that address the four cybersecurity challenge areas. As of May 2024, federal agencies had implemented 1,043 of these recommendations; 567 remain unimplemented. Until these recommendations are fully implemented, the federal government will be hindered in ensuring the security of federal systems and critical infrastructure and the privacy of sensitive data. This increases the risk that the nation will be unprepared to respond to the cyber threats that can cause serious damage to public safety, national security, the environment, and economic well-being.

Challenge 1:
Establishing a comprehensive cybersecurity strategy and performing effective oversight

170 of 396 recommendations **have NOT** been implemented (as of May 2024)



Source: Kalyaka/stock.adobe.com. | GAO-24-107231

Source: Box Milk/stock.adobe.com. | GAO-24-107231

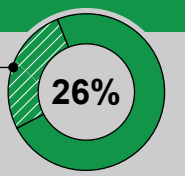
The White House, through the Office of the National Cyber Director, has taken important steps in providing cybersecurity leadership, including developing and publicly releasing the *National Cybersecurity Strategy* and its accompanying implementation plan. However, in February 2024, GAO reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of a national strategy. In particular, the strategy and implementation plan did not fully incorporate outcome-oriented performance measures and estimated resources and costs.

Additionally, the federal government needs to take actions to perform effective oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies, such as artificial intelligence (AI). For example:

- Emerging threats in the supply chain can put federal agencies, including the Department of Defense (DOD), at risk. GAO's 2023 report showed that DOD had addressed four and partially addressed three practices for managing supply chain risk. However, DOD has not yet implemented GAO's three recommendations on the partially addressed practices.
- Regarding the cyber workforce, in July 2023 GAO reported that the National Institute of Standards and Technology (NIST) had not fully addressed nine key performance assessment practices in its efforts to strengthen cybersecurity education, training, and workforce development. GAO's recommendations to fully address these practices have not yet been implemented.
- GAO's 2023 government-wide report on AI revealed that 20 federal agencies reported a total of about 1,200 current and planned use cases—specific challenges or opportunities that AI may solve. However, many agencies had not implemented AI requirements, such as preparing an inventory on AI use. GAO made 35 recommendations to address this; however, none of these have yet been implemented.

Challenge 2:
Securing federal systems and information

221 of 839 recommendations **have NOT** been implemented (as of May 2024)



Source: Justlight/stock.adobe.com. | GAO-24-107231

Source: momius/stock.adobe.com. | GAO-24-107231

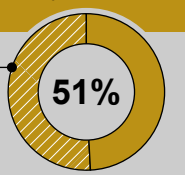
GAO has found that agencies remain limited in their ability to improve implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents. For example:

- In January 2024, GAO reported that Inspectors General at 15 of the 23 civilian agencies subject to the Chief Financial Officers Act of 1990 found their agencies' information security programs to be ineffective. Out of the 23 agencies, no more than eight received an effective rating in any given year over the last 6 years of reporting (fiscal years 2017 through 2022).
- GAO's May 2023 report highlighted that four selected agencies (the Departments of Agriculture, Homeland Security, Labor, and the Treasury) varied in their efforts to implement key security practices for cloud services, which provide on-demand access to shared resources such as networks, servers, and data storage. The practices included having a plan to respond to incidents and continuous monitoring of system security and privacy. GAO made 35 recommendations to the selected agencies, most of which have not been implemented.
- In December 2023, GAO reported that 23 federal civilian agencies had made progress in cybersecurity incident response preparedness, but 20 of the 23 agencies had not fully established an event logging capability. A log is a record of the events occurring within an organization's systems and networks, and maintaining such a record is crucial for responding to incidents. GAO recommended that 19 of the 20 agencies fully implement federal event logging requirements; however, these have not yet been implemented.

View GAO-24-107231. For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.

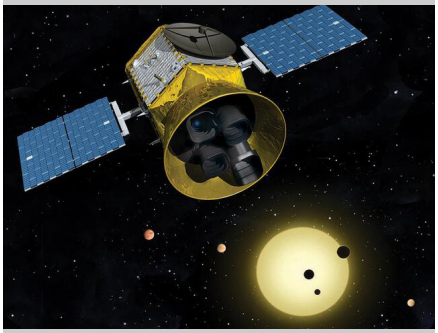
Challenge 3:
Protecting the cybersecurity of critical infrastructure

64 of 126 recommendations **have NOT** been implemented (as of May 2024)



Source: GAO. | GAO-24-107231

Source: U.S. Air Force. | GAO-24-107231

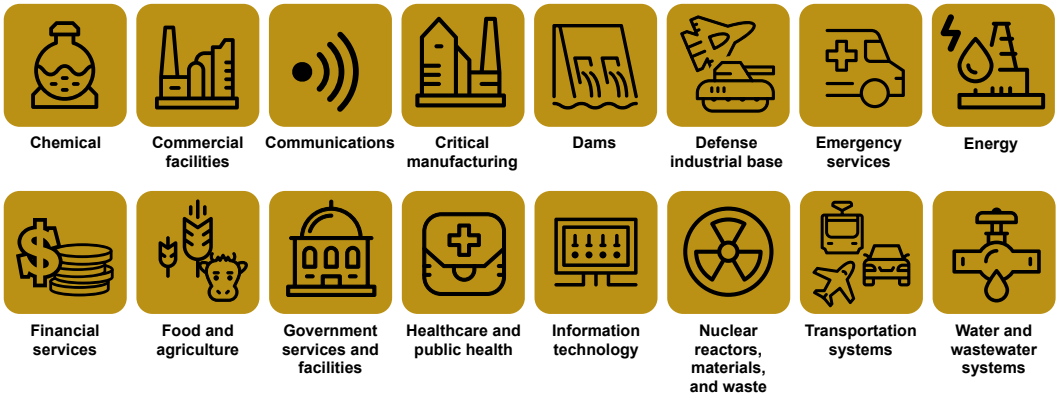


Source: National Aeronautics and Space Administration. | GAO-24-107231

Source: GAO. | GAO-24-107231

The nation's 16 critical infrastructure sectors provide the essential services that underpin American society (see figure 2).

Figure 2: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-24-107231

These sectors rely on electronic systems and data to support their missions, including operational technology, which consists of systems that interact with the physical environment. Attacks on these sectors continue to grow and could result in serious harm to human safety, national security, the environment, and the economy. For example, in February 2024, a cyberattack on Change Healthcare, a health payment processor, resulting in estimated losses of $874 million and widespread impacts on providers and patient care.

Other entities have also recognized the ongoing challenges of ensuring the cybersecurity of critical infrastructure. For example, the Cyberspace Solarium Commission has conducted studies of risks to critical infrastructure and recommended, for example, that space systems be designated as critical infrastructure.

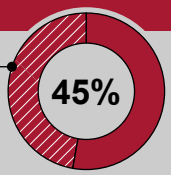
The administration and federal agencies have taken some steps to address challenges in protecting the cybersecurity of critical infrastructure. For example, in April 2024, the White House issued the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), which describes the approach the federal government will take to protect U.S. infrastructure against threats and hazards. Among other things, the memorandum reaffirms the designation of the existing 16 critical infrastructure sectors, while calling for a periodic evaluation of changes to critical infrastructure sectors. The memorandum also requires the Secretary of Homeland Security to develop a biennial National Risk Management Plan summarizing U.S. government efforts to manage risk to the nation's critical infrastructure.

However, GAO has continued to report shortcomings in efforts to ensure the security of key critical infrastructure sectors. For example:

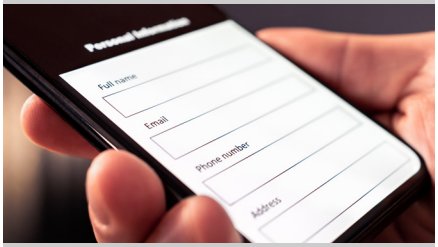
- In January 2024, GAO reported that the federal agencies responsible for the four critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, healthcare and public health, and transportation systems—had not determined the extent of their adoption of leading practices to address ransomware. GAO recommended that these agencies determine their respective sector's adoption of cybersecurity practices and assess the effectiveness of federal support. None of these recommendations have been implemented.
- GAO's March 2024 report identified challenges in collaboration between the Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies with responsibilities for mitigating cyber risks to operational technology in their sectors. The challenges were related to ineffective information sharing and a lack of sharing processes. GAO recommended that CISA take steps to address these challenges; however, the recommendations have not yet been implemented.
- In December 2023, GAO highlighted challenges identified by nonfederal entities in the healthcare sector in accessing federal support to address cybersecurity vulnerabilities in network-connected medical devices. GAO recommended that CISA and the Food and Drug Administration update existing agreements to better facilitate collaboration on these issues. However, the recommendations have not yet been implemented.

Challenge 4:
Protecting privacy and sensitive data

112 of 249 recommendations **have NOT** been implemented (as of May 2024)



Source: Grispb/stock.adobe.com. | GAO-24-107231



Source: terovesalainen/stock.adobe.com. | GAO-24-107231

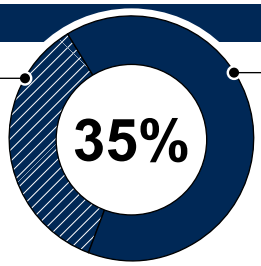
The protection of personal privacy has become a more significant issue in recent years. It is essential that both private and public entities take effective measures to safeguard the sensitive and personal information collected from American citizens. However, incidents threatening the security of this information continue to affect private and public entities. For example, in March 2024, AT&T reported that some of its data, which included sensitive personal information such as Social Security numbers and passcodes, had been released onto the dark web. Analysis revealed that this incident had impacted 7.6 million current AT&T account holders and approximately 65.4 million former account holders.

GAO has also found that federal agencies are limited in their ability to protect private and sensitive data entrusted to them. For example:

- In August 2023, GAO reported that the Internal Revenue Service's (IRS) monitoring of efforts to prevent contractors from gaining unauthorized access to sensitive taxpayer information was limited by its incomplete inventory of systems that process or store this information. GAO recommended that IRS maintain a comprehensive inventory of its systems that process or store taxpayer information; however, the recommendation has not been implemented.
- GAO's September 2022 report highlighted the risks that the increasing collection and use of personal information pose to consumer privacy and protection. For example, companies collect personal and transactional data to create consumer scores, which businesses and other entities use to predict how consumers will behave in the future. The report further noted that there remains no comprehensive U.S. internet privacy law governing private companies' collection, use, or sale of internet users' data, leaving consumers with limited assurance that their privacy will be protected.

Federal government's progress in addressing GAO's recommendations for the four major cybersecurity challenges

567 of 1,610 recommendations **have NOT** been implemented as of May 2024



GAO has made 1,610 recommendations in public reports to each of the four cybersecurity challenge areas (since 2010).

Source: GAO. | GAO-24-107231

While federal agencies have made progress in improving the security of federal and critical infrastructure IT systems, significant effort remains to address the cybersecurity challenges facing the nation. Since 2010, agencies have implemented 1,043 of the recommendations that GAO has made related to the four cybersecurity challenges. However, certain critical actions remain outstanding. For example, the federal government needs to fully establish the national cybersecurity strategy and strengthen efforts to protect the cybersecurity of critical infrastructure. Until these recommendations are fully implemented, federal agencies will be limited in their ability to:

- provide effective oversight of critical government-wide initiatives, mitigate global supply chain risks, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies;
- improve implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents;
- mitigate cybersecurity risks for key critical infrastructure systems and their data; and
- protect private and sensitive data entrusted to them.

View GAO-24-107231. For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.