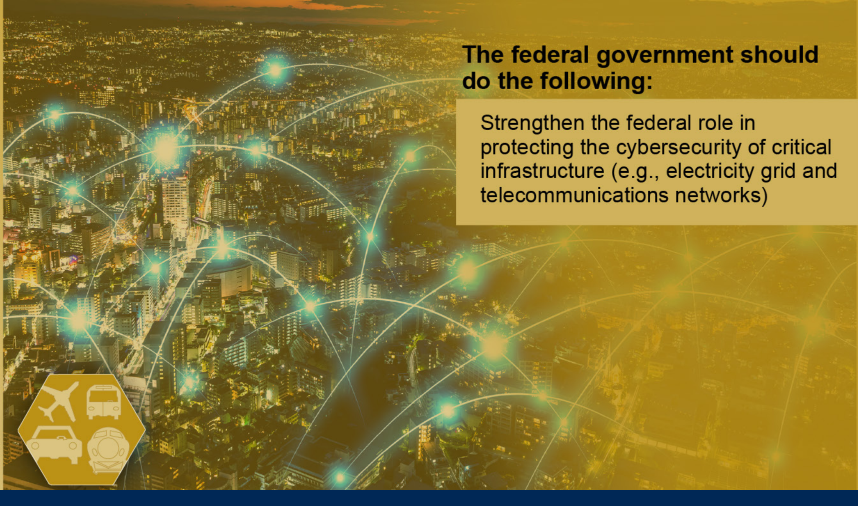
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

CYBERSECURITY HIGH-RISK SERIES:

Challenges in Protecting Cyber Critical Infrastructure



The federal government should do the following:

Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks)

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 third in a series of four reports that lay out the main cybersecurity areas the federal government needs to urgently address. It focuses on the need to protect cyber critical infrastructure.[1] We have made 106 recommendations in public reports since 2010 in this area. About 60 of these recommendations have not been implemented as of December 2022. Until these are fully implemented, key critical infrastructures will continue to have increased cybersecurity risks to their systems and data.

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

What actions should be taken to strengthen the federal role in protecting the cybersecurity of critical infrastructure?

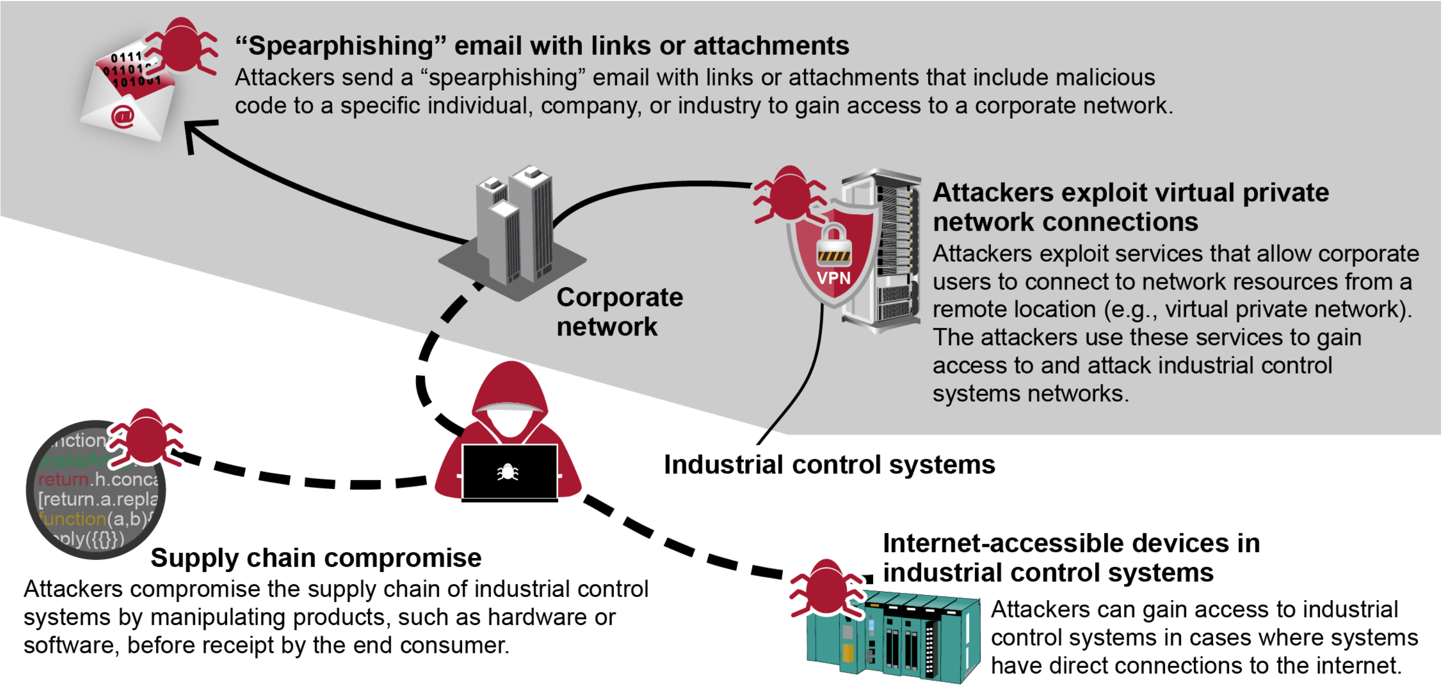
The Department of Energy (DOE) needs to address cybersecurity risks to distribution systems more fully in its plans to implement the national cybersecurity strategy for the power grid.

The U.S. grid's distribution systems—which carry electricity from transmission systems to consumers and are regulated primarily by states—are increasingly at risk from cyberattacks. Distribution systems are growing more vulnerable, in part because of industrial control systems' increasing connectivity.[2] As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations (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 reports on the first two challenge areas, 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) and GAO, *Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information*. GAO-23-106428 (Washington, D.C.: Jan. 31, 2023).

[2] Industrial control systems monitor and control sensitive processes and physical functions, such as the opening and closing of circuit breakers on the grid.

Figure 1: Examples of Techniques for Gaining Initial Access to Industrial Control Systems



"Spearphishing" email with links or attachments
Attackers send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network.

Attackers exploit virtual private network connections
Attackers exploit services that allow corporate users to connect to network resources from a remote location (e.g., virtual private network). The attackers use these services to gain access to and attack industrial control systems networks.

Supply chain compromise
Attackers compromise the supply chain of industrial control systems by manipulating products, such as hardware or software, before receipt by the end consumer.

Internet-accessible devices in industrial control systems
Attackers can gain access to industrial control systems in cases where systems have direct connections to the internet.

Source: GAO analysis of industry and federal documents. | GAO-23-106441

We reported in March 2021 that DOE, as the lead federal agency for the energy sector, developed plans to help combat these threats and implement the national cybersecurity strategy for the grid. However, DOE's plans did not address distribution systems' vulnerabilities related to supply chains. As a result, these plans will likely be of limited use in prioritizing federal support to states in addressing grid distribution systems' cybersecurity.

- **We recommended** that, in developing plans to implement the national cybersecurity strategy for the grid, DOE coordinate with the Department of Homeland Security (DHS), states, and industry to more fully address risks to the grid's distribution systems from cyberattacks. DOE agreed with our recommendation; however, it had not yet been implemented as of December 2022.

The Department of Education (Education) needs to increase coordination with its partners to address cybersecurity risks in K-12 schools.

In October 2022, we reported that K-12 schools had experienced significant educational impact due to cybersecurity incidents, such as ransomware attacks. For example, officials from state and local entities reported that the loss of learning following a cyberattack ranged from 3 days to 3 weeks, and recovery time ranged from 2 to 9 months.

The *National Infrastructure Protection Plan* (national plan) established Education as the sector risk management agency that is responsible for the protection of the education critical infrastructure subsector. As such, Education and CISA are to coordinate K-12 cybersecurity efforts with federal and nonfederal partners. For example, Education and CISA offer cybersecurity-related products and services to K-12 schools, such as online safety guidance. In addition, the Federal Bureau of Investigation (FBI) is to provide criminal investigative support. However, the federal agencies had little to no interaction with other agencies and the K-12 community regarding schools' cybersecurity. This was due, in part, to Education not establishing a government coordinating council, as called for in the national plan. Such a council could facilitate ongoing communication and coordination among federal agencies and with the K-12 community and enable federal agencies to better address the cybersecurity needs of K-12 schools.

- **We recommended** that Education establish a collaborative mechanism, such as an applicable government coordinating council, to coordinate cybersecurity efforts, among other things. Education partially agreed with this recommendation; it remained not implemented as of December 2022.

CISA needs to assess the effectiveness of its programs and services to support the communications sector.

The communications sector is an integral component of the U.S. economy and faces serious physical, cyber-related, and human threats that could affect the operations of local, regional, and national level networks, according to CISA and sector stakeholders (see figure 2). In addition to managing federal coordination during incidents impacting the communications sector, CISA shares information with sector stakeholders to enhance their cybersecurity and improve interoperability, situational awareness, and preparedness for responding to and managing incidents.

Figure 2: Examples of Potential Security Threats to the Communications Sector

Type of threat	Description
Physical	• Natural occurrences, such as hurricanes, floods, and ice storms • Human-made occurrences, such as explosive, chemical, biological, or radiological contaminant attacks on communications network infrastructure and personnel
Cyber-related	• Malicious actors, such as adversaries who intentionally disrupt the systems on a communications network • Nonmalicious actors, such as employees that accidentally alter a communication network's configuration, negatively affecting the network's ability to function properly
Human	• Threats to a communications network due to the failure of employees to plan for security incidents and implement protocols to protect networks from the impacts of such incidents

Source: GAO analysis of Department of Homeland Security documentation. | GAO-23-106441

In November 2021, we reported that CISA had not assessed the effectiveness of its programs and services supporting the security and resilience of the communications sector. By completing such an assessment, CISA would be better positioned to determine which programs and services are most useful or relevant in supporting the sector's security and resilience. We also reported that CISA had not updated its 2015 *Communications Sector-Specific Plan.* CISA officials acknowledged that certain elements of the plan are out of date and agreed the plan should be revised. Developing and issuing a revised plan would help CISA to address emerging threats and risks to the communications sector.

- **We recommended** that CISA assess the effectiveness of its programs and services to support the communications sector and, in coordination with public and private communications sector stakeholders, produce a revised *Communications Sector-Specific Plan*. CISA agreed with our recommendations; however, neither of them had been implemented as of December 2022.

The Department of the Interior's Bureau of Safety and Environmental Enforcement (the bureau) needs to take action to address oil and gas infrastructure cybersecurity risks.

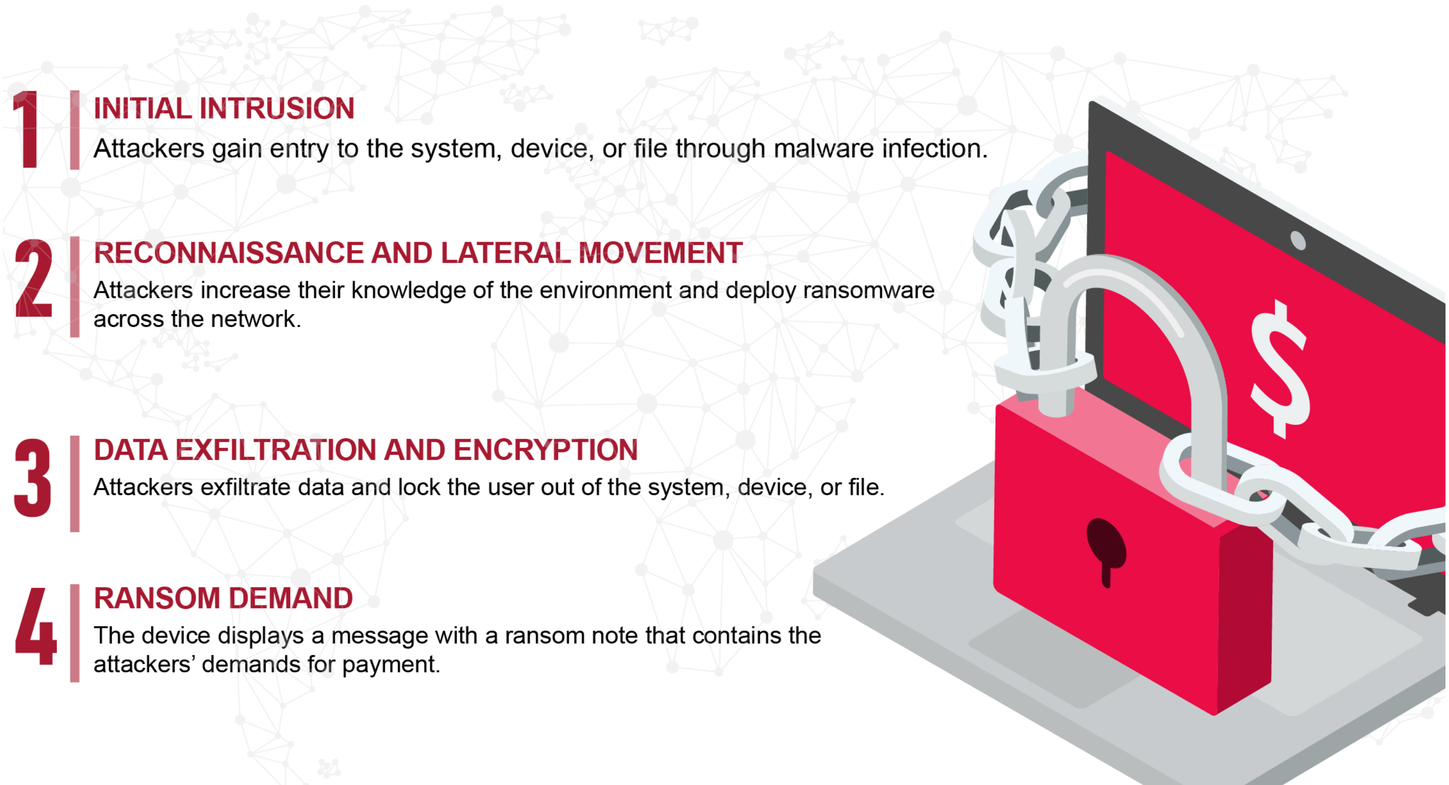
Offshore oil and gas infrastructure faces significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts. In October 2022, we reported that the bureau had long recognized the need to address cybersecurity risks and initiated efforts to do so in 2015, 2020, and 2022. However, the initiatives did not result in substantial action, and the bureau had not yet developed a cybersecurity strategy. To address the lack of progress, the bureau hired a cybersecurity specialist to lead its risk-mitigation initiative in 2022, but bureau officials said the initiative will be paused until the specialist is adequately versed in relevant issues. Absent the immediate development and implementation of an appropriate strategy, the offshore oil and gas infrastructure will remain at significant risk.

- **We recommended** that the bureau develop and implement a strategy for its most recent cybersecurity initiative. Such a strategy should include, among other things, a risk assessment, performance measures, and identification of needed resources. The Department of Interior generally agreed with our recommendation; however, it remained not implemented as of December 2022.

DHS and the Department of Justice need to enhance interagency coordination against ransomware threats.

Ransomware is a form of malicious software that threat actors use in a multistage attack to encrypt files on a device and render data and systems unusable. These threat actors then demand ransom payments in exchange for restoring access to the locked data and systems (see figure 3).

Figure 3: Four Stages of a Common Ransomware Attack



1 INITIAL INTRUSION
Attackers gain entry to the system, device, or file through malware infection.

2 RECONNAISSANCE AND LATERAL MOVEMENT
Attackers increase their knowledge of the environment and deploy ransomware across the network.

3 DATA EXFILTRATION AND ENCRYPTION
Attackers exfiltrate data and lock the user out of the system, device, or file.

4 RANSOM DEMAND
The device displays a message with a ransom note that contains the attackers' demands for payment.

Source: GAO analysis based on information from the Cybersecurity and Infrastructure Security Agency, Center for Internet Security, and Federal Bureau of Investigation; image: tomasknopp/stock.adobe.com. | GAO-23-106441

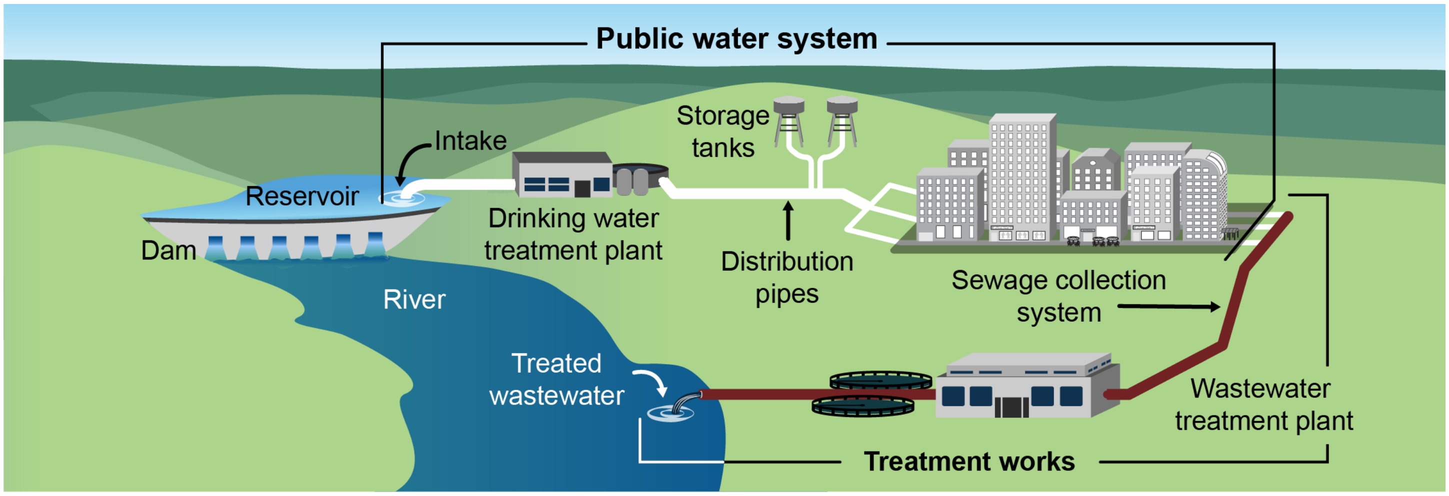
In September 2022, we reported that CISA, FBI, and Secret Service provide assistance in preventing and responding to ransomware attacks on tribal, state, local, and territorial government organizations. The agencies coordinated through existing mechanisms—such as interagency detailees and field-level staff—and demonstrated coordination on a joint ransomware website, guidance, and alerts. However, respondents identified challenges related to awareness, outreach, and communication. Further, the three agencies had not addressed aspects of six of seven key practices for interagency collaboration in their ransomware assistance to tribal, state, local, and territorial governments. For instance, existing interagency collaboration on ransomware assistance to tribal, state, local, and territorial governments was informal and lacked detailed procedures.

- **We recommended** that DHS and the Department of Justice address identified challenges and incorporate key collaboration practices in delivering services to tribal, state, local, and territorial governments. Both Departments agreed with their respective recommendations; however, the recommendations had not yet been implemented as of December 2022.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) needs to engage stakeholders and document strategies and goals for the National Critical Functions framework.

In 2019, CISA published the National Critical Functions framework, which is a set of 55 critical functions (such as “supply water”) of government and the private sector considered vital to the security, economy, and public health and safety of the nation. According to CISA officials, this framework is intended to better assess how failures in functions across the 16 critical infrastructure sectors may cascade into key systems (such as public water systems) and assets (including infrastructure such as water treatment plants) as shown in figure 4.

Figure 4: Examples of Critical Infrastructure Systems and Assets That Support the National Critical Function “Supply Water”



Source: GAO (graphic) and U.S. Environmental Protection Agency and Department of Homeland Security (information). | GAO-23-106441

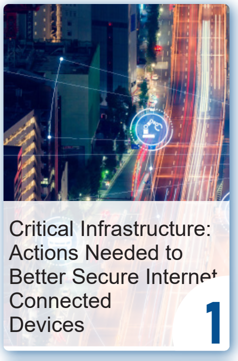
In March 2022, we reported that CISA planned to integrate the National Critical Functions framework into broader prioritization and risk management efforts. However, the federal and nonfederal critical infrastructure stakeholders that we interviewed reported that they did not understand how the framework related to prioritizing infrastructure, how it affected planning and operations, or where their particular organizations fell within it.

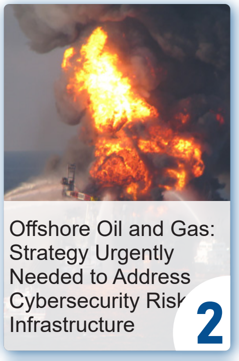
CISA officials acknowledged the need to improve the connection between the National Critical Functions framework and local and operational risk management activities and communications. In addition, CISA lacked documented goals and strategies for its framework. Without such documented goals and strategies, stakeholders’ questions regarding the framework will likely persist.

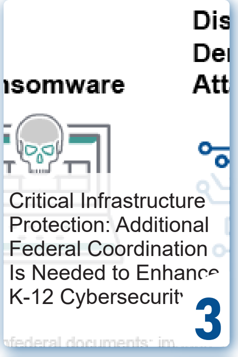
➢ **We recommended that** CISA ensure that stakeholders are fully engaged in the implementation of the framework and document the framework’s goals and strategies. CISA agreed with these and four additional related recommendations on setting priorities, seeking states’ input, improving coordination, and sharing threat information. However, none of the recommendations had been implemented 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 improving the protection of cyber critical infrastructure. Key reports focus on the following topics:


Critical Infrastructure: Actions Needed to Better Secure Internet Connected Devices 1


Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risk Infrastructure 2



Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurit 3

Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration 4

Cyber Insurance: Action Needed to Assess Potential Federal Response Catastrophic Atta 5

Cybersecurity: Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks 6

Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing 7

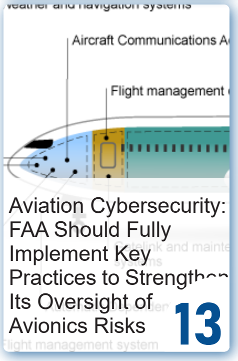
Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance 8

Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certificati Framework 9

Critical Infrastructure Protection: CISA Should Assess Effectiveness of Its Actions to Support the Communicati Sector 10

Critical Infrastructure Protection: TSA is Taking Steps to Address Some Pipeline Security Program Weakn 11

Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems 12



Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strength Its Oversight of Avionics Risks 13

Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts 14

Source: Images: (1) metaworks/stock.adobe.com, (2) United States Coast Guard, (3) GAO analysis of federal and nonfederal documents; images: marinashevchenko/stock.adobe.com, (4) alexlmx/stock.adobe.com, (5, 8) Murrstock/stock.adobe.com, (6) VideoFlow/stock.adobe.com, (7) Department of Homeland Security, (9) Gorodenkoff/stock.adobe.com, (10) TebNad/stock.adobe.com, (11) Maksim Kabakou/stock.adobe.com, (12) GAO; Art Explosion (images), (13) GAO analysis of FAA and industry documentation, (14, 15) GAO File Photo. | GAO-23-106441

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

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