United States Government Accountability Office

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Natural Resources, House of Representatives

For Release on Delivery
Expected at 2 p.m. ET
Wednesday, June 7, 2023

CYBERSECURITY

Interior Needs to Address Threats to Federal Systems and Critical Infrastructure

Statement of Marisol Cruz Cain, Director, Information Technology and Cybersecurity

GAO-23-106869

June 7, 2023

CYBERSECURITY

Interior Needs to Address Threats to Federal Systems and Critical Infrastructure

GAO Highlights

Highlights of GAO-23-106869, a testimony before the Subcommittee on Oversight and Investigations, Committee on Natural Resources, House of Representatives

Why GAO Did This Study

More than a quarter of a century has passed since GAO first designated information security as a government-wide high-risk area in 1997. Since then, challenges related to ensuring the cybersecurity of the nation have led GAO to expand this high-risk area to include the protection of cyber critical infrastructure and the privacy of personal information.

The Department of the Interior is responsible for safeguarding its information systems and sensitive data by establishing an effective information security program. The department also has regulatory oversight of critical infrastructure supporting offshore oil and gas production, including identifying and helping to address cyber-based risks.

GAO was asked to testify on threats and cybersecurity risks at the Department of the Interior. This statement summarizes types of threat actors and cyberattacks that could compromise federal systems and critical infrastructures, such as those Interior oversees. It also discusses cybersecurity reports and recommendations from GAO and Interior's Office of Inspector General.

This statement is based on prior GAO work at Interior and other federal agencies. GAO also reviewed Interior OIG reports and other public information sources.

What GAO Recommends

In prior reports, GAO has made several recommendations to Interior to improve its cybersecurity practices. Of the six recommendations discussed in this statement, Interior has fully implemented three.

View GAO-23-106869. For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov .

What GAO Found

Malicious threat actors continue to present risks to federal systems and the nation's critical infrastructure. Such attacks can result in serious harm to human safety, the environment, and the economy. The table below describes common cyber threat actors.

Common Cyber Threat Actors

Threat actor	Description
Nations	Nations—including nation-states, state-sponsored, and state-sanctioned groups or programs—use cyber tools as part of their efforts to further economic, military, and political goals.
Transnational criminal groups	Transnational criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain.
Hackers and hacktivists	Hackers break into networks for reasons including the challenge, revenge, stalking, or monetary gain. In contrast, hacktivists are ideologically motivated actors who use cyberattack tools to further political goals.
Insiders	Insiders are individuals (such as employees, contractors, or vendors) with authorized access to an information system or enterprise and who have the potential to cause harm, wittingly or unwittingly.

Source: GAO analysis. | GAO-23-106869

Cyberattacks can disrupt or damage critical infrastructure, including facilities and assets supporting offshore oil and gas production. For example, the May 2021 ransomware attack on the Colonial Pipeline Company resulted in a temporary disruption in the delivery of gasoline and other petroleum products.

In October 2022, GAO reported that Interior's Bureau of Safety and Environmental Enforcement had taken few actions to address cybersecurity risks to offshore oil and gas infrastructure. GAO recommended that the bureau immediately develop and implement a strategy to address such risks.

Interior's Office of the Inspector General (OIG) has identified weaknesses in the department's cybersecurity program and practices. For example:

- In January 2023, Interior's OIG found that the department's management practices and password complexity requirements were insufficient to protect active user passwords, including accounts with elevated privileges. The OIG made eight recommendations to help the department strengthen its IT security.
- In April 2023, the OIG released a summary of a contractor's independent audit of the department's information security program. The summary indicated that the program did not fully comply with applicable federal requirements and guidelines.

Likewise, GAO has reported on gaps in Interior's approach to cybersecurity risk management. For instance:

- In September 2022, GAO reported on the 24 Chief Financial Officer Act agencies' implementation of programs to protect the privacy of personal information. GAO found that Interior had not fully incorporated privacy into its organization-wide risk management strategy. GAO recommended that Interior take steps to do so.

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee:

I am pleased to be here today to discuss cybersecurity risks at the Department of the Interior, such as threats posed by malicious actors, including nation-state actors. As you know, federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—depend on technology systems to carry out operations and process, maintain, and report essential information. The security of these systems and data is vital to protecting individual privacy and national security, prosperity, and well-being. Moreover, recent incidents highlight the impact that cyberattacks can have on these systems.

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.[1]

This statement discusses various types of threat actors and attacks that could compromise federal systems and our nation's critical infrastructure, such as that overseen by Interior. It also discusses cybersecurity risks that we and the Office of the Inspector General have identified at the department.

This statement is based on previously issued GAO reports on cybersecurity at Interior and other federal agencies. We also reviewed Interior Office of Inspector General reports and other public information sources.

We conducted the work on which this testimony is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1]See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

Background

The U.S. Department of the Interior's mission is to protect and manage the nation's natural resources and cultural heritage, provide scientific and other information about those resources, and honor its trust responsibilities and special commitments to American Indians, Alaska Natives, and affiliated Island Communities. The department plays a central role in how the United States stewards its public lands, increases environmental protections, pursues environmental justice, and honors our nation-to-nation relationship with Tribes. The department carries out its mission through 11 technical bureaus:

- Bureau of Indian Affairs
- Bureau of Indian Education
- Bureau of Land Management
- Bureau of Ocean Energy Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- Bureau of Trust Funds Administration
- National Park Service
- Office of Surface Mining Reclamation and Enforcement
- U.S. Fish and Wildlife Service
- U.S. Geological Survey

In addition to the 11 bureaus, a number of offices fall under the Office of the Secretary, Office of the Assistant Secretary for Policy, Management and Budget, the Solicitor's Office, and the Office of Inspector General.

Interior IT Security Responsibilities

Interior is responsible for protecting the confidentiality, integrity, and availability of its information and information systems. Specifically, the Federal Information Security Modernization Act of 2014 (FISMA) was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[2]

[2]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

FISMA requires agencies to develop, document, and implement an agency-wide information security program to secure federal information operations and assets of the agency. These information security programs are to provide risk-based protections for the information and information systems that support the agency's operations. FISMA requires agencies to comply with the Office of Management and Budget's (OMB) policies and procedures, the Department of Homeland Security's (DHS) binding operational directives, and the National Institute of Standards and Technology's (NIST) information security standards.

Interior's Office of the Chief Information Officer (OCIO) leads Interior's security management program. The office's mission and primary objective is to establish, manage, and oversee a comprehensive information resources management program. The Interior Chief Information Security Officer (CISO) reports to the Chief Information Officer and oversees the Information Assurance Division. This division is responsible for Interior's IT security and privacy policy, planning, compliance, and operations.

Each of Interior's bureaus and offices have an Associate Chief Information Officer (ACIO) that reports to the department Chief Information Officer and the Deputy Bureau Director. The ACIO serves as the senior leader over all IT resources within the bureau or office. Each also has an Associate Chief Information Security Officer that represents the Bureau and reports to the Bureau ACIO and Interior's CISO.

Interior Offshore Oil and Gas Responsibilities

Interior's Bureau of Safety and Environmental Enforcement (BSEE) is responsible for overseeing offshore oil and gas operations, including cyber risks. The bureau's mission is to promote safety, protect the environment, and conserve resources offshore through regulatory oversight and enforcement. It is responsible for overseeing offshore operations, which includes the authority to investigate incidents that occur on the outer continental shelf, monitor operator compliance with environmental stipulations, and take enforcement actions against operators that violate safety or environmental standards.

BSEE's regulatory programs advise a wide range of offshore activities and facilities, including drilling, well completion, production, pipeline, and decommissioning operations. The bureau implements advancements in technology and conducts onsite inspections to assure compliance with regulations, lease terms, and approved plans. To date, BSEE's regulations do not explicitly mention cybersecurity, but the bureau has determined that addressing cybersecurity risks to offshore oil and gas infrastructure aligns with its mission to promote safety and protect the environment.

Cyber Threat Actors Pose Serious Risks to Federal Systems and Critical Infrastructure

Risks to technology systems are increasing. In particular, systems and networks supporting federal agencies and U.S. critical infrastructure are becoming more vulnerable to cyberattacks. These systems and networks are composed of, and connected to, enterprise IT systems and operational technology systems.[3] Because of their complexity and interconnections with other systems, these systems are vulnerable to cyberattacks. Such attacks could result in serious harm to human safety, the environment, and the economy.

Overview of Cyber Threat Actors

Key cybersecurity risks to federal agencies and U.S. critical infrastructure also include the growing attack capabilities of threat actors. According to the 2023 *Annual Threat Assessment of the U.S. Intelligence Community*, China, Iran, North Korea, and Russia pose the greatest cyber threats.[4] Of particular concern, these countries possess the ability to launch cyberattacks that could have disruptive effects on critical infrastructure, including facilities and assets supporting offshore oil and gas production. Further, the assessment stated that transnational organized ransomware actors continue to improve and execute high-impact ransomware attacks, extorting funds, disrupting critical services, and exposing sensitive data. Table 1 describes common types of cyber threat actors.

Table 1: Common Cyber Threat Actors

Threat actor	Description and potential motivation
Nations	Nations—including nation-states, state-sponsored, and state-sanctioned groups or programs—use cyber tools as part of their efforts to further economic, military, and political goals. Chinese and Russian cyber threat actors have previously targeted the U.S. energy sector, including oil and gas companies. In addition, Iran has previously targeted foreign oil and gas companies using cyberattack techniques.
Transnational criminal groups	Transnational criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. Further, cyber criminals are increasing the number, scale, and sophistication of ransomware attacks that threaten to cause greater disruptions of critical services.

[3]Enterprise IT systems encompass traditional IT computing and communications hardware and software components that may be connected to the internet. Operational technology systems monitor and control sensitive processes and physical functions, such as offshore oil and gas operations.

[4]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023).

Threat actor	Description and potential motivation
Hackers and hacktivists	Hackers break into networks for reasons including the challenge, revenge, stalking, or monetary gain. In contrast, hacktivists are ideologically motivated actors who use cyberattack tools to further political goals. For example, according to U.S. Coast Guard officials, the agency considers environmental groups opposed to petroleum development to be a threat actor that could potentially target offshore oil and gas infrastructure.
Insiders	Insiders are individuals (such as employees, contractors, or vendors) with authorized access to an information system or enterprise and who have the potential to cause harm, wittingly or unwittingly. This can occur through the destruction, disclosure, or modification of data, or through denial of service. Bureau of Safety and Environmental Enforcement officials indicated that insiders, such as a disgruntled employee, could cause issues on an offshore oil and gas facility.

Source: GAO analysis. | GAO-23-106869

Examples of Cyberattacks

Cyber adversaries use a variety of tactics and techniques to exploit vulnerabilities and attack systems and networks. According to MITRE's ATT&CK® Framework, attackers tend to follow common methodologies to compromise targets and achieve their goals. For example, threat actors can use multiple techniques, such as compromising the supply chain of hardware and software, to gain initial access to IT and operational technology systems.[5]

In fiscal year 2022, federal agencies reported 30,659 information security incidents across nine categories,[6] which represents a 5.7 percent decrease from the over 32,500 incidents reported in fiscal year 2021.[7] Examples of successful cyberattacks demonstrate the impact they can have on federal systems and the nation's critical infrastructure:

- In May 2023, Microsoft reported that it uncovered cyberattacks by Volt Typhoon, a state-sponsored actor based in China. According to Microsoft, Volt Typhoon has been active since 2021 and has targeted critical infrastructure in communications, manufacturing, utility,

[5]The supply chain is a linked set of resources and processes that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

[6]The nine categories of incidents are (1) attrition, (2) email/phishing, (3) external/removable media, (4) impersonation/spoofing, (5) improper usage, (6) loss or theft of equipment, (7) web, (8) other/unknown, and (9) multiple vectors.

[7]Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report Fiscal Year 2022*. The number of incidents are from OMB's fiscal year 2022 annual FISMA report to Congress, which is based on incidents reported to the Cybersecurity and Infrastructure Security Agency by federal agencies. OMB notes that drawing conclusions based on this data point would be premature, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years.

transportation, government, and IT, among other sectors. Microsoft also reported that Volt Typhoon is aiming to develop capabilities that could disrupt communication infrastructure between the United States and Asia during future crises.

- In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyberattack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. According to a joint advisory released by DHS and the FBI, the company proactively disconnected certain systems that monitor and control physical pipeline functions to ensure the safety of the pipeline. This resulted in a temporary halt to all pipeline operations, which led to gasoline shortages throughout the southeast U.S.

- In December of 2020, the cybersecurity firm FireEye discovered that a SolarWinds product known as Orion was compromised and being leveraged by a threat actor for access to its customer systems. Hackers inserted malicious code into Orion—a product widely used in both the federal government and private sector to monitor network activity and manage devices. The threat actor, the Foreign Intelligence Service of the Russian Federation, used Orion to breach several federal agency networks. The initial breach opened a backdoor to agency systems that enabled the threat actor to deliver additional malicious code. This allowed the actor to move laterally, gathering information and compromising data.

- In 2015, Russian threat actors conducted a cyberattack on the Ukrainian power grid that systematically disconnected substations, resulting in a power outage for about 225,000 customers.

- According to the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, from December 2011 to 2013, state-sponsored Chinese actors conducted a spearphishing and intrusion campaign targeting U.S. oil and gas pipeline companies. Of the 23 targeted pipeline operators, 13 were confirmed compromises.

Progress Has Been Made, but Interior’s Cybersecurity Practices Have Weaknesses

While Interior has made progress in addressing previously reported cybersecurity weaknesses, both the department’s Office of Inspector General (OIG) and GAO have continued to identify multiple weaknesses

in the department's cybersecurity program and practices. These include issues affecting both Interior's own security environment and its oversight of offshore oil and gas infrastructure.

Interior's Inspector General Identified Weaknesses in Cybersecurity Practices

In January 2023, Interior's OIG issued a report examining the department's password complexity requirements.[8] The OIG found that the department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Specifically, the OIG determined that the department (1) had not consistently implemented multifactor authentication, (2) used password complexity requirements that were outdated and ineffective, (3) used password complexity requirements that implicitly allowed unrelated staff to use the same inherently weak passwords, and (4) did not promptly disable inactive (unused) accounts or enforce password age limits. The OIG noted that if a malicious actor were to compromise an account with elevated privileges, such as a system administrator's account, the magnitude of harm would increase. The OIG made eight recommendations to help the department strengthen its IT security by improving user account management practices. The department concurred with the OIG's recommendations.

In April 2023, the OIG released a summary of an independent audit, carried out by a contractor on behalf of OIG, of the department's information security program.[9] The summary indicated that Interior's program was not effective because it was not consistent with applicable FISMA requirements, OMB policy and guidance, or NIST standards and guidelines.[10] The contractor identified needed improvements in the areas of risk management, supply chain risk management, identity and access management, configuration management, data protection and privacy, information security continuous monitoring, incident response, and

[8]Department of the Interior Office of Inspector General, *P@$$words at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk*, 2021–ITA–005 (January 2023).

[9]Department of the Interior Office of Inspector General, *Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2022,* 2022–ITA–028 (April 2023).

[10]According to OMB's fiscal year 2022 Core IG Metrics Implementation Analysis and Guidelines, a security program is considered effective if most of the fiscal year 2022 Core Inspector General Metrics are at least Level 4, "Managed and Measurable." Using OMB's guidance and the CyberScope results, the contractor determined that most of the cybersecurity functions were Level 3, "Consistently Implemented."

contingency planning. To address these weaknesses, the contractor made 24 recommendations intended to strengthen the Interior's information security program as well as those of the bureaus and offices. The department concurred with all recommendations and established a target completion date for each corrective action.

GAO Has Reported on Gaps in Interior's Approach to Managing Cybersecurity and Privacy Risks

Cybersecurity risk management: In July 2019, we reviewed the cybersecurity risk management practices at the 23 civilian Chief Financial Officers (CFO) Act agencies, which includes Interior.[11] We found that the department had not fully addressed three of five key practices for establishing its cybersecurity risk management program. Specifically, the department had not (1) developed a cybersecurity risk management strategy that addressed key elements, (2) fully documented risk-based policies and procedures, or (3) fully established a process or mechanism for coordination between its cybersecurity risk executive and its enterprise risk management governance structure. We recommended that Interior take steps to address these gaps. Since then the department has implemented all three recommendations. Implementing these foundational practices is a critical step in ensuring Interior can make consistent, informed risk-based decisions to protect agency systems and information against cyber-based threats.

IT workforce planning: In October 2019, we reported on the extent to which the 24 CFO Act agencies had implemented key IT workforce planning activities.[12] We found that Interior had partially, minimally, or not implemented the key practices. This included, for example, assessing gaps in competencies and staffing. Accordingly, we recommended that Interior fully address the workforce planning activities. As of May 2023, Interior had taken some steps, but work remained to fully implement these activities. A key to having a successful cybersecurity program is having a well-trained, highly qualified workforce that is versed in identifying cyber threats and recognizes steps to take once confronted with them.

[11]GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019).

[12]GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities,* GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

Information and communications technology supply chain risk management: In December 2020, we issued a public version of a sensitive report reviewing the information and communications technology (ICT) supply chain risk management programs and practices at the 23 civilian CFO Act agencies (which includes Interior).[13] None of the 23 agencies, including Interior, fully implemented all of the foundational practices for supply chain risk management. Fourteen of the 23 agencies had not implemented any of the practices. In the sensitive version of the report, we made a total of 145 recommendations to the 23 agencies to fully implement these practices. Implementing these practices will help organizations protect against supply chain risks, such as the insertion of counterfeits and malicious software, unauthorized production, and tampering, as well as poor manufacturing and development practices throughout the system development life cycle.

Privacy of personal information: In September 2022, we reported on a review of privacy programs at the 24 CFO Act. Agencies.[14] We found that Interior had addressed most of the key practices for establishing a privacy program. However, the department had not fully incorporated privacy into its department-wide risk management strategy, to include a determination of risk tolerance. We recommended that Interior establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. Interior concurred with this recommendation and plans to implement it by November 2023. Such a strategy will help the agency ensure that it is managing risks to sensitive personal information consistently and within acceptable parameters.

Cybersecurity of offshore oil and gas infrastructure: In October 2022, we reported that BSEE had long recognized the need to address cybersecurity risks to offshore oil and gas infrastructure but had taken few actions to do so.[15] In 2015 and 2020 BSEE initiated efforts to address cybersecurity risks, but neither resulted in substantial action. In 2022,

[13]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020). This is a public version of a sensitive report that GAO issued in October 2020. Information that agencies deemed sensitive was omitted and, due to sensitivity concerns, GAO substituted numeric identifiers that were randomly assigned for the names of the agencies.

[14]GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges,* GAO-22-105065 (Washington, D.C.: Sept. 22, 2022).

[15]GAO, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, GAO-23-105789 (Washington, D.C.: Oct. 26, 2022).

BSEE started another such initiative and hired a cybersecurity specialist to lead it. However, bureau officials said the initiative will be paused until the specialist is adequately versed in the relevant issues.

We recommended that BSEE immediately develop and implement a strategy to address offshore infrastructure risks. Such a strategy should include an assessment and mitigation of risks and identify objectives, roles, responsibilities, resources, and performance measures, among other things. Absent the immediate development and implementation of an appropriate strategy, offshore oil and gas infrastructure will remain at significant risk. In March 2023, the department indicated that BSEE is developing a cybersecurity strategy and anticipates that this strategy will be complete by the end of calendar year 2023.

In summary, cyber threats continue to pose a significant threat to systems supporting the federal government and critical infrastructure. Successful cyberattacks, including those carried out by nation-state actors, could have catastrophic consequences for the economy, national security, and human safety and well-being. The Department of the Interior needs to continue to take steps to ensure that its systems and data are protected from cyber-based attacks carried out by malicious actors. Moreover, Interior needs to ensure that it is addressing cybersecurity risks to critical infrastructure assets for which it has responsibility.

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Marisol Cruz Cain, Director, Information Technology and Cybersecurity at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Lee McCracken (assistant director), Keith Kim (analyst in charge); Amanda Andrade; Lauri Barnes; Latesha Love-Grayer; Frank Rusco; Scott Pettis; Tina Won Sherman; Walter Vance; and Adam Vodraska.