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 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.