U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

June 27, 2023

The Honorable Paul Gosar
Chairman
Subcommittee on Oversight and Investigations
Committee on Natural Resources
House of Representatives

Ongoing Cybersecurity Threats within the Department of the Interior Hearing: Responses to Questions for the Record

Dear Chairman Gosar:

Thank you for the opportunity to testify before the Subcommittee on Wednesday, June 7, 2023 to discuss cybersecurity risks that threaten the Department of the Interior and the infrastructure it manages. We also appreciate the opportunity to provide the Subcommittee with additional information in response to the questions for the record, which can be found in the enclosures to this letter.

If you have any questions, please contact me at (202) 512-5017 or CruzCainM@gao.gov.

Sincerely yours,

Marisol Cruz Cain

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Enclosures - 2

Enclosure I

Post-Hearing Questions for the Record
Submitted to Ms. Marisol Cruz Cain
From Chairman Paul Gosar

1. **Is anything stopping the Department of the Interior from allocating a greater percentage of its existing budget to cybersecurity initiatives?**

   The need to conduct risk assessments and budget constraints due to operating and maintaining legacy systems are stopping the Department of the Interior from allocating a greater percentage of its existing budget to cybersecurity initiatives. Key steps for agencies to ensure adequate funding for cybersecurity initiatives are to identify and assess cyber risks, prioritize initiatives for addressing those risks, and allocate the necessary funds as appropriate. For example, as we reported, the Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) had committed minimal resources and demonstrated a lack of urgency in addressing cybersecurity risks to offshore oil and gas production infrastructures.[1] Accordingly, it is critical that BSEE move expeditiously to develop and implement a strategy to guide its most recent cybersecurity initiative. This strategy should include (1) a risk assessment; (2) objectives, activities, and performance measures; (3) roles, responsibilities, and coordination; and (4) identification of needed resources and investments. In March 2023, Interior indicated that BSEE is developing a cybersecurity strategy that includes identifying resource needs, which may be complete by the end of calendar year 2023. By developing such a strategy, Interior will be better positioned to identify and prioritize the funds it needs to support critical cybersecurity initiatives. These priorities can then be reflected in future budget requests. Similarly, we recently recommended that Interior incorporate privacy into its organization-wide risk management strategy.[2] This is a key step for the department to identify, assess, and prioritize risks to the sensitive personal information with which it is entrusted.

   As we have noted, however, agencies such as Interior are sometimes constrained in making new investments by the large portion of their IT budgets that are allocated to the operations and maintenance of legacy systems. For example, in fiscal year 2023, Interior's budget allocates approximately $297 million to the development, modernization, and enhancement of its IT systems while allocating nearly $1.5 billion to the operation and maintenance of existing systems. As we have previously reported, legacy systems can be costly and difficult to maintain, may have unsupported hardware and software, and may operate with known security vulnerabilities.[3] Such security vulnerabilities may be either technically difficult or prohibitively expensive to address.

---

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

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

[3]GAO, *Information Technology: Agencies Need to Continue Addressing Critical Legacy Systems*, GAO-23-106821 (Washington, D.C.: May 10, 2023).

2. How can DOI better prioritize cybersecurity initiatives with its existing budget?

Interior can better prioritize its cybersecurity initiatives within its existing budget by continuing to utilize its cybersecurity risk management strategy and ensuring that it is fully implementing risk-based policies. Federal guidance, such as the National Institute of Standards and Technology Special Publication 800-39, identifies practices for establishing effective agency-wide cybersecurity risk management programs. Specifically, the practices include aligning agency priorities with resource allocation and prioritization at all levels of the organization, including the enterprise, business, and system levels.

We reported in July 2019 that managing competing priorities between operations and cybersecurity presents a challenge for many agencies.[4] In particular, agencies highlighted the competition for limited resources between cybersecurity risk management activities and operational or mission needs. For example, Interior's Deputy Chief Information Officer noted that the need to balance mission priorities with those related to cybersecurity risk management leads to fiscal and operational challenges when making investment, architectural, and operational decisions. To its credit, as we recommended in our July 2019 report, Interior developed an organization-wide cybersecurity risk management strategy to define how the department intends to identify, assess, and respond to risks. It also updated its policies to require an organization-wide cybersecurity risk assessment and established a process for coordination between its cybersecurity and enterprise risk management functions. By establishing and implementing these risk-based policies and procedures, Interior should be better positioned to prioritize cybersecurity initiatives within its existing budget as well as to identify areas for future investment.

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

Post-Hearing Questions for the Record
Submitted to Ms. Marisol Cruz Cain
From Ranking Member Raúl Grijalva

1. **If threat actors were to obtain personally identifiable information during a breach of the Department of the Interior's (DOI) systems, how would federal employees and members of the public be impacted? How would infrastructure under the DOI, such as oil and gas infrastructure, drinking water sources, and power grid maintenance, be impacted?**

   A successful attack on Interior's systems involving personally identifiable information (PII) could significantly impact both federal employees and members of the public, leaving them more susceptible to identity theft, fraud, and other crimes. The advent of new technologies and the proliferation of PII has increased the government's reliance on IT to collect, store, and transmit this sensitive information. Consequently, vulnerabilities arising from agencies' increased dependence on IT can result in the compromise of personal information, such as inappropriate use, modification, or disclosure. Recently reported breaches involving PII show that PII such as names, addresses, dates of birth, and Social Security numbers can be compromised when attackers exploit vulnerabilities in IT systems.

   With respect to critical infrastructure, we previously reported that cyberattacks against critical infrastructure (e.g., electric grid, water and wastewater systems, etc.) were increasing in frequency, sophistication, and scale.[5] 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.[6] Successful cyberattacks on systems supporting critical infrastructure can compromise sensitive information, such as businesses' proprietary information or individuals' financial or medical information.

   Moreover, operational technology (OT) systems, which are used to monitor and control physical equipment, were once largely isolated from internet and business IT systems but are now frequently connected with those systems both within a company and accessible by internet systems globally. As a result, cyberattacks are now more likely to originate in business IT systems and migrate to OT. According to Interior's Bureau of Safety and Environmental Enforcement, results of a successful cyberattack on offshore oil and gas infrastructure could include deaths and injuries, damaged or destroyed equipment, and pollution to the marine environment.

[5]GAO, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing*, GAO-22-104279 (Washington, D.C.: Mar. 1, 2022).

[6]GAO, *Cybersecurity: Interior Needs to Address Threats to Federal Systems and Critical Infrastructure*, GAO-23-106869 (Washington, D.C.: June 7, 2023).