Committee on Natural Resources
Subcommittee on Oversight and Investigations
Oversight Hearing
1324 Longworth House Office Building
June 7, 2023
2:00p.m.

Oversight Hearing titled *"Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State Sponsored Cyber Actors"*

Questions from Rep. Paul Gosar for Brian Cavanaugh, Fellow for Cybersecurity, Intelligence, and Homeland Security, The Heritage Foundation, Washington, DC

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

a) In general, there could be several factors that may influence the allocation of the Department's budget towards cybersecurity initiatives including prioritization and mandates, resource constraints, risk assessment, legislative and regulatory requirements, and awareness and understanding.

The Department of the Interior's public facing priorities include:

- Identifying steps to accelerate responsible development of renewable energy on public lands and waters,
- Strengthening government-to-government relationship with sovereign Tribal Nations,
- Making investments to support the Administration's goal of creating millions of family-supporting and union jobs,
- Working to conserve at least 30% each of our lands and waters by the year 2030, and
- Centering equity and environmental justice.

None of the publicly identified priorities discuss cybersecurity or ensuring the security of stakeholders' data held by the Department. These public facing priorities compete for funding alongside cybersecurity initiatives.

While the Department's overall budget may be limited, given the findings of both the OIG and GAO reports, there should be nothing stopping the Department from re-allocating existing funding and requesting future funding to address appropriate cybersecurity investments. These investments should include cyber risk assessments, investment prioritization, and the adoption of basic cybersecurity protocols.

The department's leadership and decision-makers have demonstrated a lack of adequate awareness of the importance of cybersecurity and its potential implications. If there is a lack of understanding or appreciation for cybersecurity risks, it will adversely impact the allocation of resources to address those risks effectively. The leadership of the Department are focused on centering equity and environmental justice, while leaving the data it has been entrusted with open to our adversaries.

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

a) The Department of Interior could better prioritize cybersecurity initiatives with its existing budget by developing a comprehensive risk assessment which assess the Department's current cybersecurity posture, identifies vulnerabilities and potential threats, and determines the potential impact of cyber incidents on critical operations, systems, and data. This assessment will help in understanding the specific cybersecurity needs and guide resource allocation well into the future.

Additionally, the Department should develop a cybersecurity strategy and policy. Establishing a clear strategy and policy framework that outlines the Department's approach to cybersecurity. This should include goals, objectives, and specific measures to protect sensitive information, secure systems, and mitigate cyber risks. The strategy should serve as a foundation for budget allocation and proper oversight by both the OIG and Congress.

These two steps will help identify a long-term plan to fund and address cybersecurity efforts that are capable of planning for phased implementation as well as be adaptable to unexpected developments in the cybersecurity field. Providing comprehensive training and awareness programs for employees at all levels—especially the leadership level—to enhance the Department’s understanding of cybersecurity risks and best practices. Well-trained personnel are essential for implementing effective security measures and responding to potential incidents, just as well trained and educated leaders are to recognize the need for adequate investment in cybersecurity measures.

The Department should also establish a regular review and update of cybersecurity policies. Continuously monitoring and assessing the effectiveness of existing cybersecurity policies, procedures, and controls ensures the Department remains aligned with emerging threats, industry best practices, and regulatory requirements.