MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

T. Charles Clancy, PhD
Senior Vice President
General Manager, MITRE Labs
Chief Futurist
MITRE

Response to Questions for the Record from Chairman Paul Gosar

The Committee on Natural Resources, Subcommittee on Oversight and Investigations
June 7, 2023 Hearing titled "Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State-Sponsored Cyber Actors"

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

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

Chairman Gosar,

Thank you for these important and timely questions. As was discussed during the hearing, DOI faces two separate cybersecurity challenges: securing their own enterprise IT infrastructure, and effectively governing the security of certain critical infrastructure under their purview.

In general, some level of improved cybersecurity is possible within current budgets, but robust implementations will require modernization and new funding. The absence of new funding will require evaluating budgetary tradeoffs between existing priorities and critical modernization needs.

Enterprise IT

With respect to enterprise IT security, many of the baseline recommendations from the Inspector General are achievable within their current budget for many of their IT systems. Enabling and requiring passphrases and multi-factor authentication requires little software change, and is primarily changes to system policies. The costs are primarily around user training, which should be absorbable into the broader training requirements for federal employees.

However there are two areas that would likely require additional investment above and beyond their current IT budget: deploying zero trust, and addressing legacy systems.

Executive Order 14028 put into motion requirements for federal agencies to adopt zero trust architectures to deal with increased threats from cyber adversaries. Implementing zero trust requires procuring and deploying additional software systems within the enterprise, and implementing it fully often requires rearchitecting enterprise networks with concepts like micro-segmentation. These changes would best be achieved if done as part of a larger enterprise IT modernization that looked to more fully embrace a FEDRAMP-approved cloud-based solutions.

With respect to legacy systems, based on testimony during the hearing, DOI has certain IT systems that are aging and lack the capability to be upgraded with modern cybersecurity defenses. Many federal

agencies are facing these same challenges, such as the Internal Revenue Service[1]. While it may be possible to put "band aid" solutions on top of these legacy systems to achieve some level of compliance, they represent serious technology debt whose modernization costs only continue to increase over time. The solution is modernization, the sooner the better. While these represent increased costs in the near term, over time they represent cost savings as smaller IT teams are needed long term when leveraging cloud-based Software as a Service (SaaS) solutions.

Of course, the cybersecurity safeguards being discussed for DOI represent really only the bare minimum for best practices by federal agencies. A more comprehensive solution would be to fully embrace and implement the NIST Risk Management Framework (RMF) within DOI's enterprise systems.

Critical Infrastructure

Addressing cybersecurity for critical infrastructure under DOI's purview, such as offshore oil and gas production, is implemented by an entirely different portion of the DOI enterprise, and is more focused on developing and promulgating cybersecurity policy, and ensuring appropriate compliance auditing across industry. Organizations like BSEE are sufficiently resourced for baseline policy development, but need to prioritize cybersecurity as part of their safety mission. However, BSEE is likely insufficiently resourced to undertake the the needed auditing function. Many critical infrastructure sector risk management agencies lack the needed resourcing to fully provide the needed capacity building and compliance auditing for their industries.

[1] https://www.gao.gov/products/gao-23-104719