Testimony of Dr. Charles Clancy

Senior Vice President, MITRE

before the House Committee on Natural Resources, Subcommittee on Oversight and Investigations, Hearing on Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State-Sponsored Cyber Actors

7 June 2023

Chairman Gosar, Ranking Member Stansbury, Ranking Member Grijalva, and Committee Members:

Thank you for inviting me to testify before you today on a topic of critical national importance. My name is Charles Clancy and I am a Senior Vice President at MITRE where I lead science, technology, and engineering for the company. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of over 1,500 cybersecurity professionals provide deep expertise across the executive branch and federal judiciary, including in support of organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and U.S. Cyber Command. MITRE's ATT&CK™ framework has become the *de facto* language between government and industry for describing and combatting cyber threats.

Prior to joining MITRE, I spent nine years as a member of the faculty at Virginia Tech where I held the Bradley Distinguished Professorship of Cybersecurity in the Department of Electrical and Computer Engineering, and served as executive director of what is now the National Security Institute. I started my career at the National Security Agency leading research and development programs.

Threat Environment

Over the past five years, the cyber threat environment has changed considerably.

Among criminal elements we have seen the dramatic rise of ransomware giving organized crime new business models for exploiting enterprise computer networks and systems. This has fueled secondary industries, such as hacker groups focused exclusively on penetrating organizations and selling that access to the highest bidder. Well-financed criminal hacker groups now develop new cyber tools on par with nation-state hackers. While U.S. action against major ransomware groups has stunted what was astronomical growth in the ransomware economy, it remains a major threat.

Meanwhile China and Russia have elevated their offensive cyber programs into strategic instruments of statecraft.

China's cyber program had been primarily focused on espionage: stealing secrets from governments and intellectual property from companies. However, the Chinese Communist Party (CCP) has expanded their operations to also hack into critical infrastructure systems and preposition access that could be used for strategic effect in the U.S. and beyond.

Russia's espionage and information operations posture has similarly expanded to include critical infrastructure. But unlike China, Russia has the ongoing war in Ukraine as a backdrop for pulling the trigger on their cyber weapons, normalizing destructive cyber attacks against civilian infrastructure as part of military conflict. Beyond shifting international norms, they are also gaining experience they can employ beyond Ukraine, in Europe and North America.

The Director of National Intelligence released their annual threat assessment in February in which they assessed that China could almost certainly disrupt oil and gas pipelines and rail infrastructure in the U.S. and would do so to deter U.S. military action by impeding our decision making, inducing societal panic, and disrupting military mobilization. It also assessed that Russia is focused on attacking U.S. undersea cables and industrial control systems[1].

Importantly, the goal of inducing societal panic skews the nature of traditional state actor cyber tactics. Beyond targeting specific civilian infrastructure that has downstream military impacts, state actors are now acting more like terrorist groups, using cyber attacks—or the threat of cyber attacks—to induce fear.

With this as a backdrop, all federal agencies need to remain vigilant against cyber attacks targeting their enterprise infrastructure and take steps to promote cybersecurity within the industries and jurisdictions they oversee.

[1] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community", 6 February 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Enterprise Security for the Department of the Interior (DOI)

Recent reports by DOI's Inspector General highlighted cybersecurity concerns[2,3]. While I am not able to assess these specific reports, there are a range of recommendations and best practices used by other federal agencies that could be beneficial if adopted by DOI.

Much of the U.S. federal cybersecurity ecosystem is governed by requirements stemming from the Federal Information Security Modernization Act (FISMA) originally enacted in 2002, updated in 2014[4], and currently undergoing another legislative update in both the House and Senate to account for the modern threat environment and new defensive technologies[5]. The act emphasizes a risk-based approach to cybersecurity, with protections commensurate with the level of data that needs to be protected by agencies. There are a variety of resources that reinforce and provide detailed guidance on implementation of FISMA, including Office of Management and Budget (OMB) circulars[6], the NIST Risk Management Framework[7], and NIST's security control baselines[8].

In response to continued threats from advanced threat actors, the White House has taken steps to move beyond these tools and require federal agencies to implement zero trust architectures, through executive action[9] and OMB memoranda[10]. These provisions are expected to be part of legislative updates to FISMA.

[2] Office of the Inspector General, Department of the Interior, "Semiannual Report to Congress", 31 March 2023. https://www.doioig.gov/sites/default/files/2021-migration/DOIOIGSemiannualReporttoCongressMarch2023.pdf

[3] Office of the Inspector General, Department of the Interior, "The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise", 2020-ITA-030, February 2023. https://www.doioig.gov/sites/default/files/2021-migration/Final%20Evaluation%20Report_DOI%20Cyber%20Risk%20Management_Public.pdf

[4] "Federal Information Security Act of 2014", Public Law 113-283, December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[5] Dave Powner, "When it comes to federal cybersecurity policy, the executive branch is far ahead of Congress", Nextgov, 17 June 2022. https://www.nextgov.com/ideas/2022/06/closing-gap-cyber-policy-focusing-fisma/368353/

[6] Office of Management and Budget, "Managing Federal Information as a Strategic Resource", Circular A-130, June 28, 2016. https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

[7] National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations", NIST Special Publication 800-37, rev2, December 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[8] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations", NIST Special Publication 800-53, rev5, 23 September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[9] The White House, "Executive Order on Improving the Nation's Cybersecurity", EO 14028, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[10] Office of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", M-22-09, 26 January 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

DOI would be well served by developing a plan to implement the NIST Risk Management Framework and federal Zero Trust Cybersecurity Principles into their enterprise network infrastructure.

Critical Infrastructure Security

A decade ago, a variety of executive[11] and legislative[12] actions created much of the critical infrastructure cybersecurity environment we operate in today. Critical infrastructure is most often operated by private organizations and subjected to some form of regulation. These actions established Sector Risk Management Agencies (SRMAs) responsible for cybersecurity of named critical infrastructure sectors, ultimately led to the Department of Homeland Security establishing CISA, and resulted in NIST creating its Cybersecurity Framework[13] to provide an approach to securing critical infrastructure.

Much of this ecosystem today relies on voluntary compliance and the establishment of communities where sectors can freely share cyber threat information called Information Sharing and Analysis Centers (ISACs). While this approach has dramatically improved cybersecurity, major gaps remain across every industry, and there are periodic calls to shift voluntary compliance regimes to compulsory, with corresponding push back from industry over the associated costs. The National Cybersecurity Strategy published earlier this year seeks to establish required minimum cybersecurity safeguards for U.S. critical infrastructure[14].

Recent reports from the Government Accountability Office[15] and the National Security Agency[16] highlight cybersecurity concerns connected with infrastructure over which DOI has some oversight. While not a designated SRMA, the Bureau of Safety and Environmental

[11] The White House, "Improving Critical Infrastructure Cybersecurity", EO 13636, 12 February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[12] "Cybersecurity Information Sharing Act of 2015", Public Law 114-113, 18 December 2015. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

[13] National Institute of Standards and Technology, "Cybersecurity Framework". https://www.nist.gov/cyberframework

[14] Office of the National Cyber Director, "National Cybersecurity Strategy", March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[15] Government Accountability Office, "Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure", GAO-23-105789, October 2022. https://www.gao.gov/assets/gao-23-105789.pdf

[16] Joint Cybersecurity Advisory, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection", PP-23-1143, May 2023. https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

Enforcement (BSEE) does oversee security for the offshore energy industry. BSEE could leverage its rulemaking authorities, in collaboration with other federal partners, to develop a minimum set of cybersecurity requirements based on the NIST Cybersecurity Framework and consistent with the National Cybersecurity Strategy. Major operators of offshore energy infrastructure and their corresponding onshore transportation infrastructure could implement an integrated strategy for securing both, which the Intelligence Community assesses is specifically under threat from China[1].

Recent cyber attacks against Guam attributed to China are also concerning[17], though the tactics used by the CCP are not unique to Guam. Given the strategic importance of Guam's critical infrastructure to the Department of Defense (DOD) strategy, DOI and DOD should develop a closer partnership on securing infrastructure upon which both the U.S. military and the citizens of Guam depend. This should include leveraging DOD's Cyber Protection Teams and other assets to collaboratively perform cybersecurity vulnerability assessments of Guam's infrastructure and systems.

Workforce and Leadership

A major challenge across the board in cybersecurity is workforce. The cybersecurity workforce gap nationally continues to grow, with 40% of the 1.9 million cybersecurity positions currently being vacant[18]. In this climate, DOI has stiff competition in recruiting and retaining cybersecurity talent. Partnering with an FFRDC could be a good part of the solution, but longer-term, the department needs to build its organic talent base. One option could be to target students graduating from the Cybercorps Scholarship for Service program who have a federal service commitment upon graduation[19].

The Department needs a permanent Chief Information Security Officer (CISO). Such a position is critical to securing enterprise infrastructure.

Other departments and regulatory commissions have consolidated organizations focused on cybersecurity and resilience for the industries they regulate. While BSEE has that remit, it

[17] Wired, "China Hacks US Critical Networks in Guam, Raising Cyberwar Fears", 24 May 2023. https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/

[18] Cyberseek, "Cybersecurity Supply/Demand Heat Map", accessed 5 June 2023. https://www.cyberseek.org/heatmap.html

[19] Office of Personnel Management, "Cybercorps Scholarship for Service", accessed 5 June 2023. https://sfs.opm.gov/

only focuses on offshore resources and reportedly has only one employee focused on cybersecurity[20]. One option could be to establish a cybersecurity cell within the Office of the Secretary focused on coordinating cybersecurity strategy and policy across all segments of DOI's regulatory and oversight apparatus. The team could participate in interagency efforts like the *Cybersecurity Forum for Independent and Executive Branch Regulators*[21].

Conclusion and Recommendations

DOI is not alone. It can leverage deep expertise across the interagency to improve its own enterprise cybersecurity, and work with key partners across DHS and DOD to help secure infrastructure over which it has some oversight. With a proactive cybersecurity strategy, it can build momentum by adopting best practices and forging interagency relationships.

[20] Kevin Sligh, "BSEE proactively addressing cybersecurity and offshore energy production", 3 January 2023. https://www.bsee.gov/kevin-sligh-bsee-proactively-addressing-cybersecurity-and-offshore-energy-production

[21] Cybersecurity Forum for Independent and Executive Branch Regulators, "Charter". https://www.nrc.gov/docs/ML1501/ML15014A296.pdf