EXAMINING ONGOING CYBERSECURITY THREATS WITHIN THE DEPARTMENT OF THE INTERIOR AND THE NEXUS TO STATE-SPONSORED CYBER ACTORS

OVERSIGHT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON NATURAL RESOURCES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

Wednesday, June 7, 2023

Serial No. 118–36

Printed for the use of the Committee on Natural Resources

Available via the World Wide Web: http://www.govinfo.gov
or
Committee address: http://naturalresources.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
52–515 PDF WASHINGTON : 2024

COMMITTEE ON NATURAL RESOURCES

BRUCE WESTERMAN, AR, *Chairman*
DOUG LAMBORN, CO, *Vice Chairman*
RAÚL M. GRIJALVA, AZ, *Ranking Member*

Doug Lamborn, CO
Robert J. Wittman, VA
Tom McClintock, CA
Paul Gosar, AZ
Garret Graves, LA
Aumua Amata C. Radewagen, AS
Doug LaMalfa, CA
Daniel Webster, FL
Jenniffer González-Colón, PR
Russ Fulcher, ID
Pete Stauber, MN
John R. Curtis, UT
Tom Tiffany, WI
Jerry Carl, AL
Matt Rosendale, MT
Lauren Boebert, CO
Cliff Bentz, OR
Jen Kiggans, VA
Jim Moylan, GU
Wesley P. Hunt, TX
Mike Collins, GA
Anna Paulina Luna, FL
John Duarte, CA
Harriet M. Hageman, WY

Grace F. Napolitano, CA
Gregorio Kilili Camacho Sablan, CNMI
Jared Huffman, CA
Ruben Gallego, AZ
Joe Neguse, CO
Mike Levin, CA
Katie Porter, CA
Teresa Leger Fernández, NM
Melanie A. Stansbury, NM
Mary Sattler Peltola, AK
Alexandria Ocasio-Cortez, NY
Kevin Mullin, CA
Val T. Hoyle, OR
Sydney Kamlager-Dove, CA
Seth Magaziner, RI
Nydia M. Velázquez, NY
Ed Case, HI
Debbie Dingell, MI
Susie Lee, NV

Vivian Moeglein, *Staff Director*
Tom Connally, *Chief Counsel*
Lora Snyder, *Democratic Staff Director*
http://naturalresources.house.gov

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

PAUL GOSAR, AZ, *Chairman*
MIKE COLLINS, GA, *Vice Chair*
MELANIE A. STANSBURY, NM, *Ranking Member*

Matt Rosendale, MT
Wesley P. Hunt, TX
Mike Collins, GA
Anna Paulina Luna, FL
Bruce Westerman, AR, *ex officio*

Ed Case, HI
Ruben Gallego, AZ
Susie Lee, NV
Raúl M. Grijalva, AZ, *ex officio*

CONTENTS

OVERSIGHT HEARING ON EXAMINING ONGOING CYBERSECURITY THREATS WITHIN THE DEPARTMENT OF THE INTERIOR AND THE NEXUS TO STATE-SPONSORED CYBER ACTORS

Wednesday, June 7, 2023
U.S. House of Representatives
Subcommittee on Oversight and Investigations
Committee on Natural Resources
Washington, DC

The Subcommittee met, pursuant to notice, at 2:01 p.m. in Room 1324, Longworth House Office Building, Hon. Paul Gosar [Chairman of the Subcommittee] presiding.

Present: Representatives Gosar, Collins, Westerman; Stansbury, Case, and Lee.

Dr. GOSAR. The Subcommittee on Oversight and Investigations will come to order.

Without objection, the Chair is authorized to declare a recess at any time.

The Subcommittee is meeting today to hear testimony on examining ongoing cybersecurity threats within the Department of the Interior and the nexus to state-sponsored cyber actors.

Under Committee Rule 4(f), any oral opening statement at the hearings are limited to the Chairman and the Ranking Minority Member. I therefore ask unanimous consent that all other Members' opening statements be made part of the hearing record if they are submitted in accordance with Committee Rule 3(o).

Without objection, so ordered.

The Chairman now recognizes myself for my introductory statement.

STATEMENT OF THE HON. PAUL GOSAR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARIZONA

Dr. GOSAR. Good afternoon, everyone. I would like to thank all of our witnesses, both those from the public and the private sector, for being here today, as well as many of the colleagues that will surely be showing up for their participation.

When you think of the House Committee on Natural Resources, a hearing on cybersecurity probably isn't the first thing that comes to mind. However, in today's world of hyperconnectivity, technology touches almost every aspect of our lives. From toothbrushes with apps to children playing games on tablets in restaurants, it seems we cannot escape the growing role of technology in our daily lives.

With more connectivity, more information, and more data, there is an ever-increasing need for vigilance, protection, and cybersecurity to guard against these threats. These threats are foreign and

domestic, and come from private actors and nation states like China.

As our experts may mention later, cybersecurity refers to the security of our devices: infrastructure, data, and users of computers, computer networks, information, and communication technology, virtual systems, or computer-enabled control of physical components. As individuals, we are increasingly aware of the potential for cyber criminal activities. In both our personal and professional lives, there is more awareness of the need for best practices like changing our password, not clicking on links from Nigerian princes offering us a small fortune if we help them out.

But jokes aside, small actions by individuals protect our work from both lone cyber criminals and large-scale hacking groups who hope to make money by exploiting hard-working, earnest Americans. Unfortunately, individual vigilance often gets lost in the large governmental bureaucracies.

Federal agencies are responsible for collecting, processing, storing, and disposing of massive amounts of digital information related to individuals, businesses, and sensitive government matters. As a result, even the slightest cyber vulnerability as government agencies can manifest itself as a large-scale breach and, therefore, our nation's economic prosperity, national security, and our personal privacy.

Sadly, many government agencies, including the Department of the Interior, are increasingly vulnerable to today's world of omnipresent technology and information. At the same time, foreign nation states like China are aware of even the slightest cyber security weaknesses, and are increasingly seizing vulnerabilities in America's cybersecurity infrastructure as opportunities to advance their strategic, economic, geopolitical, and military interests.

For example, on May 24, Microsoft, in partnership with the U.S. Intelligence Agency, announced the discovery of stealth and malicious activity aimed at critical infrastructure in the United States. The attack, carried out by a state-sponsored actor based in China called Volt Typhoon, targeted critical infrastructure in Guam and elsewhere in the United States.

In the most recent campaign, communications and government infrastructure sectors were included in the attack. The infrastructure is a key component to maintaining America's interests in the Indo-Pacific region. Unfortunately, this is just one attack of many, and we know of and can speak of those that are unclassified, but we can't even talk about the ones that are classified in an open forum.

China's threat looms large over the national security interests of the United States and the world. Ongoing aggressions in the Indo-Pacific highlight the need to support our territories, including holding the Department of the Interior accountable to ensure their assets are cyber-secure. There are no quick fixes to cybersecurity and the agencies are never done with the project.

Rather, cybersecurity is an ongoing process that requires agency planning, implementing processes, and conducting programing. I am grateful for the men and women in both the private sector and the government services who devote their professional lives to protecting America's information technology assets.

In my own state, we set up the Arizona Cyber Command Center, which is run by the Department of Public Safety's Arizona Counter Terrorism Information Center in Phoenix. I have actually been there. This center works together with the state and Federal officials to protect our assets from cyber criminals.

The critical nature of the mission does not excuse any government agency at the Federal, state, or local level from fulfilling their duties and implementing necessary changes, especially when they are told time and time again that they are falling short.

Today, we will hear from both the Office of the Inspector General and the Government Accountability Office about cybersecurity vulnerabilities at the Department of the Interior. They found absurd levels of password insecurity at the Department and "long-recognized but unaddressed cyber risks to BSEE's offshore energy infrastructure that would be catastrophic to our national and economic security if attacked." I appreciate both the IG and the GAO's work on this important issue, as accountability is a key component to resolving the cybersecurity problem across the government.

In addition to our government witnesses, we have a very accomplished panel from the private sector, all of whom can speak to the very real threat that nation states like China continue to pose not only to the Department of the Interior, but across the Federal Government.

Moreover, these witnesses can speak to the best practices providing recommendations and policies that are available today to make our taxpayer-owned assets more secure and less vulnerable to the Chinese Communist Party. I think that is great news, and something that doesn't even necessarily take a change in the law. Often a change in individual behavior like updating passwords, using two-factor authentication, and increasing interagency collaboration to ensure that those with access to our critical infrastructure keep it safe and secure.

Again, I appreciate the witnesses' time today, and I turn to the Ranking Member, Ms. Stansbury, for her opening statement.

STATEMENT OF THE HON. MELANIE A. STANSBURY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW MEXICO

Ms. STANSBURY. Thank you, Chairman. It is actually really wonderful to be here today, and to have had such a productive bipartisan effort to examine these critical issues affecting our nation's national security and our Federal agencies.

While cybersecurity may be a subject that many do not immediately think of when they think about this Committee's jurisdiction, we are well aware of the rising frequency of cyber attacks and the implications for the agencies that this Committee has jurisdiction over. Agency assets are targeted by, as was said, state-sponsored actors, cybercrime groups, and even hobbyist hackers.

Our Federal agencies are particularly attractive targets because of their high profiles, their access to sensitive and privileged information, and, of course, the national security implications. But our Federal agencies are prioritizing cybersecurity, and are prepared to strike back at cyber criminals who threaten us.

And I, too, would also like to thank our cyber professionals who work in the area, especially those who work in my district at our national labs and at our base.

Cyber attacks can affect everyone in our country. In New Mexico, our local institutions have been under cyber attack this past year, including our public school system, our county, and one of our universities. A cyber attack on these systems or operations related to these missions could have devastating and long-lasting effects on any institution.

I look forward to hearing testimony from our government and expert witnesses today to understand the vulnerabilities, what is at stake, and what we can do to address these issues.

A recent GAO and OIG report revealed that there is, of course, significant room for improvement when it comes to modernizing our systems and procedures, identifying and resolving weaknesses, improving coordination between agencies and the private sector, and addressing the risks to our critical infrastructure. These recommendations are particularly important for the Department of the Interior, which manages billions of dollars in assets, including the financial assets of tribal communities and insular areas, as well as operations related to oil and gas leasing, our national parks, and our water supplies across the western United States, as well as our exploration for critical minerals.

One of the OIG reports from February found that offshore oil and gas infrastructure regulated by DOI faces significant risks, and a successful cyber attack could have significant implications to environmental, physical, and economic harm in terms of a potential oil spill or other impacts to our energy systems, not to mention disruptions that could occur to energy supplies and markets, as we saw with the Colonial Pipeline and SolarWinds.

By improving our understanding of our cyber security vulnerabilities as we are going to do in this hearing, as well as bad actors' motivations for launching these attacks, we can prevent them and minimize the damage when they do happen.

Strengthening our cybersecurity infrastructure is more than just patching and having the most state-of-the-art technology. We must also ensure that our agencies have the necessary resources and personnel to properly monitor and address their needs.

I do want to take a moment before we begin to hear testimony to say this to anyone who is involved in cyber attacks or cyber crime: the United States is prepared to respond to, dismantle, and disrupt any cyber criminal enterprise attempting to attack its networks, data, and systems. Earlier this year, the Justice Department completed a disruption campaign against a ransomware group, and the FBI successfully penetrated the network. The stakes with cybersecurity are huge, but so are the consequences. So, if you are coming for the Federal Government, we will be coming for you.

With that, I yield back.

Dr. GOSAR. That was a nice end to that statement.

I now recognize the Chairman of the Full Committee, the gentleman from Arkansas.

STATEMENT OF THE HON. BRUCE WESTERMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARKANSAS

Mr. WESTERMAN. Good afternoon, everyone, and thank you to Subcommittee Chairman Gosar and Ranking Member Stansbury for holding this very important bipartisan hearing today, as well as to the witnesses and my colleagues for their time and participation.

I think it is safe to say that we all recognize the power of technology in our day-to-day lives. With the devices in our hands we can control the temperature of our homes, monitor weather around the globe, and harness the power of this metadata for all kinds of new uses, even things like monitoring soil moisture to track the growth of trees and crops.

Just like regular folks, government agencies depend on information technology systems for pretty much everything, including national defense, maintaining our critical energy infrastructure, and protecting personally identifiable information for Federal Government employees.

Most of us in this room have probably been targets of a cyber attack. In March of this year, the FBI announced that the personal data of Members and staff were breached in an attack on the D.C. Health Link site. Unfortunately, this is a common occurrence, too common of occurrence, as foreign nation states recognize the growing role that technology plays in America's government operations.

Nation states like China are launching increasingly sophisticated cyber attacks to further their strategic and geopolitical priorities. Because of this growing threat, industry leaders described cyber weapon deployment as "the dawn of a new age of conflict."

Despite the critical and growing importance of cybersecurity, U.S. Government agencies often fall short of best practices and align with the recommended standards. The results can be catastrophic.

For instance, in 2015, affiliates of the Chinese Communist Party hacked systems at OPM and stole personally identifiable information for 4.2 million government employees and security clearance background information on 21.5 million individuals. The Director of the FBI at the time called it a treasure trove of information about everybody who has worked for, or tried to work for, the U.S. Government. His successor said that data theft allows China to identify targets for espionage campaigns, and aids in the nation's development of artificial intelligence systems.

Sadly, this breach was not a surprise to those monitoring cybersecurity vulnerabilities at OPM. The IG issued warnings to the agency for years over alarming cybersecurity security vulnerabilities. Those warnings were ignored, the Chinese Communist Party exploited the vulnerabilities, and our national security suffered. You would think that the lesson was learned, and other government agencies would prioritize cybersecurity, especially when notified time and again that their agencies are vulnerable. However, many agencies still fall short.

The Department of the Interior is no exception. On behalf of the Committee of Natural Resources, I thank both the Inspector

General and the GAO for their work highlighting cybersecurity weaknesses at the Department of the Interior.

But let me make it clear that the Department of the Interior is not alone. All government agencies must make a renewed commitment to cybersecurity in order to protect America's information, data, and technology. Indeed, with the ever-increasing role of technology and the rapid rise of artificial intelligence, effective and ongoing cybersecurity is of utmost importance and, quite frankly, it is a matter of life and death.

We have an impressive slate of witnesses today from both the private and public sectors. I look forward to listening to them and learning more about cybersecurity as we work to protect America's information technology infrastructure.

With that, I yield back, and thank you again to the witnesses.

Dr. GOSAR. I thank the Chairman. Now I will introduce our witnesses from the first panel.

First we have the Honorable Mark Greenblatt, Inspector General of the U.S. Department of the Interior; and then we have Ms. Marisol Cruz Cain, Director, Information Technology and Cybersecurity, Government Accountability Office. I work a lot with you, so thank you so much for being here today.

Let us remind the witnesses that under Committee Rules, they must limit their oral statements to 5 minutes, but their entire statement will appear in the hearing record.

To begin your testimony, please press the "on" button on your microphone so we can all hear you.

We use timing lights here. When you begin, you will see a green light. At the end of 5 minutes, that light will turn to red. When you see that red, I will ask you to please complete your statement.

I will also allow all the witnesses in the panel to testify before Member questioning.

I now recognize Mr. Greenblatt for 5 minutes.

STATEMENT OF THE HON. MARK GREENBLATT, INSPECTOR GENERAL, U.S. DEPARTMENT OF THE INTERIOR, WASHINGTON, DC

Mr. GREENBLATT. Chairman Gosar, Ranking Member Stansbury, and members of the Subcommittee, thank you for the opportunity to appear before you today.

My office has identified IT security as a top management challenge for the Department of the Interior for more than 20 years. With that in mind, we have prioritized cybersecurity oversight as an important part of our portfolio, and have built a track record, a long track record of effective oversight into these vulnerabilities.

Our latest inspection focused on password security at the Department. It goes without saying that passwords are a prime target of attack for malicious actors who are attempting to gain unauthorized access to sensitive data. Our team tested whether DOI's password complexity and enforcement controls were effective to prevent a malicious attack. To do this, our testers spent less than $15,000 to design a system to crack or hack passwords. Our tools compared the Department's 85,000 passwords, on the one hand, with 46 quadrillion potential passwords on the other.

It is important to note two things: first, all of the equipment, tools, and information that our team used is available to malicious actors across the globe; second, the methodology that we used is similar to that used by hackers in the past.

The results of our testing were troubling. In total, we cracked more than 20 percent of the Department's active passwords, which amounts to more than 18,000 passwords. Get this: Our team was able to crack more than 14,000 in the first 90 minutes alone.

Even worse, the cracked passwords included hundreds of accounts belonging to senior government officials, and hundreds more of accounts with elevated privileges such as what a systems administrator would have.

Moreover, our testers found that the most commonly used password at the Department was "password1234." In fact, 5 of the top 10 passwords in the Department included the word "password" and some combination of 1234. Even so, 99.99 percent of the accounts that we hacked met DOI's password complexity requirements. As I said, the results of our tests were disturbing.

But the good news is that there are solutions. The first one is requiring what is called multi-factor authentication, or MFA. MFA refers to the requirement to use at least two factors to access computer systems, and the factors can be broken down into three categories: something you have, such as an ID card; something you know, such as a password; and something you are, such as a fingerprint or a retinal scan. Multi-factor authentication would require at least two of those, such as a password with a fingerprint. MFA is the gold standard for cybersecurity because it is much easier for an attacker to obtain a password than it is to obtain a retinal scan.

MFA is already required on all Federal information systems and has been for decades. But our inspection showed that the Department of the Interior still allowed passwords alone on an unknown number of systems. In fact, our inspection found that nearly 90 percent of Interior's high-value IT assets permitted authentication through passwords alone, or allowed MFA to be bypassed.

Let me say that again, because that might be the most significant aspect of our findings: We found that nearly 90 percent of the Department's high-value assets did not enforce multi-factor authentication requirements. We therefore recommended that the Department prioritize implementing and requiring MFA that cannot be bypassed on all of its systems, starting with the high-value assets.

While MFA is the cornerstone for cybersecurity, we recognize that there may be cases in which MFA cannot be fully implemented. So, we recommended that the DOI improve its password policies. In particular, we recommend shifting away from clumsy passwords that have special characters and numbers and are simply impossible to remember.

Specifically, we recommend that the Department shift away from requiring a password, which is hard for a person to remember and easy for a computer to crack, to a passphrase, which is a string of unrelated words which is easy for a person to remember and hard for a computer to crack. Using passphrases is part of the mandatory technical requirements for Federal agencies, and we

recommended that the Department adopt policies and controls that are consistent with that guidance.

To its credit, the Department concurred with our recommendations, and has generally provided target dates for their implementation.

Thank you for your time, and I look forward to answering your questions.

[The prepared statement of Mr. Greenblatt follows:]

PREPARED STATEMENT OF THE HONORABLE MARK LEE GREENBLATT, INSPECTOR GENERAL, U.S. DEPARTMENT OF THE INTERIOR

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee, thank you for giving me the opportunity to discuss cybersecurity at the Department of the Interior (DOI) and in particular, our office's January 2023 report, P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk. As you know, inspectors general have a direct reporting relationship to Congress. My office and I take this obligation seriously, and we appreciate the Subcommittee's continued support for our independent and objective oversight.

In our recent inspection of the DOI's password security, we found that the DOI's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. In fact, during our inspection, we cracked 18,174 of 85,944—or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees. As the result of our findings, we made eight recommendations to help the Department strengthen its IT security by improving user account management practices. The DOI concurred with our recommendations.

I. Background

The DOI Office of Inspector General (OIG) has recognized IT security as one of the DOI's top management challenges for many years. The DOI relies on complex, interconnected information systems to carry out its daily operations and spends approximately $1.7 billion annually on its portfolio of IT assets. Our work has found that the DOI continues to face challenges in implementing an enterprise IT security program that balances compliance, cost, and risk while enabling bureaus to meet their diverse missions.

The OIG prioritizes cybersecurity oversight as an important part of our portfolio. For example, our 2023–2024 oversight plan includes planned reviews of the DOI's vulnerability remediation practices and cyber threat hunting efforts. We also currently have an ongoing review of the DOI's public cloud computing security practices.

In April 2023, we issued the fiscal year 2022 annual independent Federal Information Security Modernization Act (FISMA) audit for the DOI.[1] That audit identified needed improvements and made 24 recommendations intended to strengthen the DOI's information security program as well as those of the bureaus and offices. Using FISMA metrics, the Office of Management and Budget (OMB) scored the cybersecurity performance of 23 Federal agencies, including the DOI. The DOI scored a 68 percent and ranked 23rd on the list.

Other recent work published by our office includes the results of our testing of the DOI's cyber threat detection and defense controls. Specifically, in August 2022, we issued a memorandum concluding that this evaluation could be closed without a full-scale report because we were satisfied with the Department's response to our technical tests, conducted between May and November 2021.[2] Our review of the Department's cyber incident tracking system demonstrated that the DOI's IT staff identified our simulated attacks. Moreover, the Department mitigated confirmed technical vulnerabilities identified by our technical tests.

---

[1] *Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2022* (Report No. 2022-ITA-028).

[2] *The U.S. Department of the Interior's Cyber Threat Detection and Defense Controls* (Report No. 2020-ITA-067).

In addition, in September 2020, we issued a report of our evaluation of the security of the DOI's wireless networks.[3] Our evaluation revealed that the Department did not deploy and operate a secure wireless network infrastructure. We conducted reconnaissance and penetration testing of wireless networks representing each bureau and office. To do this, we assembled portable test units for less than $200 that were easily concealed in a backpack or purse and operated these units with smartphones from publicly accessible areas and locations open to visitors. Our attacks simulated the techniques of malicious actors attempting to break into departmental wireless networks, such as eavesdropping, so-called "evil twin" attacks,[4] and password cracking. We made 14 recommendations that will help prevent malicious actors from eavesdropping on internal communications and gaining unauthorized access to the DOI's wireless networks. The Department concurred with and has implemented all recommendations.

Given the team's success rate cracking passwords during our September 2020 evaluation, we decided to conduct a formal test of passwords throughout the Department. That prompted this passwords project, in which we inspected the DOI's password complexity requirements after defining rules of engagement[5] with the Department to ensure that it was able to protect its IT systems and that any vulnerabilities could be addressed promptly.

II. The DOI OIG's Inspection of the DOI's Password Complexity Requirements

Identifying and authenticating users is a fundamental security control for granting access to computer systems and information resources. As such, authentication methods such as passwords are a prime target of attack for malicious actors attempting to gain unauthorized access to sensitive data. In this inspection, our objective was to determine whether the Department's password management and enforcement controls were effective enough to prevent a malicious actor from gaining unauthorized access to Department computer systems by capturing and "cracking" user passwords.

A. Methodology

A "clear text password" is what a user types when prompted to log in to a system. To avoid exposing a sensitive password, user passwords are stored in a secure, unintelligible format called "hashes." The hashed version of a password is not usually accepted through typical authentication operations, such as computer login prompts. This restriction prevents a malicious actor from using captured password hashes to gain unauthorized access to a computer system. So, for example, the clear text password "Password-1234" is stored in its hashed form as "A71FB31235347EA75956B6155ED36899."

Hashes are generally considered secure because they cannot be directly reverted to clear text—their original state. However, there are indirect methods attackers can use to attempt to recover hashed passwords. Once attackers have captured hashes, they must attempt to recover their original clear text form through a process referred to as "hash cracking."[6] If successful, this enables the attacker to use the password to gain unauthorized access to an organization's computer systems and data.

To test the Department's passwords, our inspectors spent less than $15,000 on a system designed to crack—or hack—passwords using open-source software and a custom wordlist, consisting of publicly available password lists harvested from past data breaches, dictionaries from multiple languages, U.S. Government terminology, and pop culture references. We created a set of rules and processes for manipulating

---

[3] *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks* (Report No. 2018-ITA-020).

[4] In such attacks, bad actors seek to capture usernames and passwords and then crack the passwords.

[5] As explained in our report, according to the National Institute of Standards and Technology, "rules of engagement" define detailed guidelines and constraints regarding the execution of information security testing. The rules are established before the start of a security test and give the test team authority to conduct defined activities without the need for additional permissions.

[6] "Hash cracking" is the automated process of generating clear text password "candidates" and then computing hashes of those candidates and comparing the results against captured hashes. If the candidate's hash matches the captured hash, it means the password candidate and the clear text version of the captured hash are the same. If the two hashes do not match, the process continues until either a match is found or the attacker gives up and attempts to crack other captured password hashes.

and combining those words into password candidates; we then attempted to crack the hashes for every DOI user account.[7]

B. Findings

We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Over the course of our inspection, we cracked 18,174 of 85,944—or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.

Specifically, we found that:

1. The Department did not consistently implement multifactor authentication (MFA), including for 89 percent of its High Value Assets, which are assets that could have serious impacts to the Department's ability to conduct business if compromised. This lack of MFA left these systems vulnerable to password compromising attacks.
2. The Department's password complexity requirements were outdated and ineffective, allowing users to select easy-to-crack passwords (e.g., Changeme$12345, Polar_bear65, Nationalparks2014!). We found, for example, that 4.75 percent of all active user account passwords were based on the word "password." In the first 90 minutes of testing, we cracked the passwords for 16 percent of the Department's user accounts.
3. The Department's password complexity requirements implicitly allowed unrelated staff to use the same inherently weak passwords—meaning there was not a rule in place to prevent this practice. For example, the most reused password (Password-1234) was used on 478 unique active accounts. In fact, 5 of the 10 most reused passwords at the Department included a variation of "password" combined with "1234"; at the time of our report, this combination met the Department's requirements, even though it is not difficult to crack.
4. The Department did not timely disable inactive (unused) accounts or enforce password age limits, which left more than 6,000 additional active accounts vulnerable to attack.

The Department Did Not Consistently Implement MFA on Its Systems

MFA refers to the requirement to use at least two factors to access computer systems, such as a password plus a PIN from a smartphone app or a PIV card plus a password. When MFA is implemented correctly, it adds a layer of security that protects organizations, even when passwords are compromised.

MFA is already required on all Federal information systems and has been for decades. As our inspection showed, however, the Department still allowed single-factor authentication (username and password) on an indeterminate number of its systems, including high-value IT assets.

Because the Department relied on authentication methods that were not in line with National Institute of Science and Technology (NIST) recommendations, Governmentwide mandates, and industry best practices, the burden of the Department's security controls rested on obsolete password complexity requirements. Further, the Department did not have a full picture of which systems complied with which standards. Without requiring and enforcing MFA across its systems—including those that contain sensitive information—the Department's data remains at risk of unauthorized exposure.

The Department's Ineffective Password Complexity Requirements Allowed Easy-To-Crack Passwords

Department policy at the time of our inspection required that all passwords have a minimum length of 12 characters and contain at least 3 of 4 character types consisting of uppercase, lowercase, digits, and special characters. We found that these requirements were not sufficient to prevent us from successfully recovering the clear text passwords for 18,174 active user accounts (21 percent) using our hash-cracking system. We recovered passwords for 13,924 of those accounts in the first

[7] As part of our rules of engagement with the Department, we waited 90 days to begin testing hashes from the Department. At that time, all accounts should have had their passwords changed or been disabled due to inactivity pursuant to departmental policy. As of June 8, 2021, we provided the Department with a list of all user accounts with passwords we cracked to ensure that the Department forced those accounts to change passwords.

90 minutes of testing and recovered the passwords for the remaining 4,250 accounts over an additional 8 weeks of testing.

We note that 99.99 percent of the accounts we cracked met the Department's password complexity requirements. These passwords, however, were consistently made up of single dictionary words, patterns, or slightly modified existing passwords—all of which people tend to use to construct memorable passwords. Although the Department's password policy at the time of the inspection appeared to encourage complex passwords, in practice, its policies were not sufficient to prevent users from creating passwords that are easy to crack.[8]

Further, frequent password change requirements, while crucial when weak passwords are permitted, tend to encourage users to continue to use passwords that are easy to crack. NIST states that, when frequent password changes are required, users are most likely to change a single character, or append a character to the end of an existing password (e.g., Password-1234 might become Password-1234!). This ensures that the password remains memorable to the user, but it also remains weak and easy to crack. This creates a feedback loop that frustrates users, perpetuates the weak password cycle, and does not improve security.

The Department's Password Complexity Requirements Implicitly Allowed Hundreds of Unrelated Accounts To Use the Same Passwords

Password reuse is a security risk because it reduces both the time and effort necessary for a successful attack. The risk is greatly increased when the same easy-to-crack passwords are allowed to be used on multiple accounts. We found that the same easy-to-crack passwords (which all met the Department's complexity requirements) were used across multiple active accounts. Even though many of these accounts were unrelated to each other, the passwords were so common that multiple employees from different bureaus and offices independently chose the same passwords. Because the Department did not have an explicit rule in place denying this practice, it implicitly allowed users to create the same passwords across multiple accounts.[9]

We found that 20 percent of all active accounts had passwords that were used across multiple distinct accounts (16,812 out of 85,944). This includes both cracked and uncracked passwords. We were able to identify when the same passwords were used based on the hashes, so even if we did not crack a password, we could identify and determine which accounts shared the same password.

NIST standards require agencies to check potential passwords and disallow them if they are on a list of commonly used, expected, or compromised passwords. We found that none of the Department's bureaus had implemented the ability to check for and prevent weak passwords.

The Department Did Not Timely Disable Inactive Accounts or Enforce Password Age Limits

We found that the Department failed to enforce its own account management policies regarding account disabling and password changes on a significant number of accounts. The Department's policy requires accounts to be disabled after 45 days of inactivity. Enforcing this provision is important because unused accounts pose a higher risk to Department systems and networks, as they offer more opportunities for a malicious actor to gain unauthorized access. Disabling accounts after a period of inactivity reduces this risk. We found that 6,243 of all active accounts had not been used for more than 45 days; the Department failed to disable these accounts as required by its own policy and instead left implementation and enforcement of this policy to the bureaus and offices. We cracked 23 percent (1,405) of these accounts.

We also found that 28 percent of the accounts we cracked did not comply with the Department policy requiring password changes at 60-day intervals, suggesting that these accounts were still using the passwords after we cracked them. Without that password age limit, an attacker is not limited by time. According to

---

[8] Most of the passwords we cracked were based on a single dictionary word with the inclusion of enough characters or character substitutions to meet the complexity requirement. For example, "Password-1234" was the most used password at the Department. Even though a password of this type meets requirements because it includes uppercase letters, lowercase letters, digits, and a special character, it is, in fact, easy to crack.

[9] In other cases, we found common passwords reused across multiple related accounts, such as new accounts with temporary passwords, shared mailboxes, or service accounts. (Service accounts are often granted elevated privileges over systems or data, and shared mailboxes often contain sensitive data or attachments.) Understanding the purpose and extent of access granted to these accounts was out of the scope of our inspection; therefore, we were unable to identify the extent of the risk posed by these and other nonadministrative accounts.

Department policy in place at the time of our inspection, an attacker would have only 60 days to intercept or otherwise acquire a hash, crack it, and then use it.

C. Recommendations

Given our findings, we made eight recommendations to the Department to help it strengthen its IT security by improving account management practices. In summary, our recommendations can be grouped into four broad categories:

- First, we recommended that the Department prioritize implementing MFA across all systems and develop a system to track the status of the implementation of MFA.
- Second, we recommended that the Department revise password complexity requirements to bring them in line with current NIST guidance, such as using longer passphrases and less frequent change intervals.
- Third, we recommended that the Department revise policy to prohibit accounts from reusing the same passphrases and passwords.
- Fourth, we recommended that the Department ensure compliance with policies regarding timely disabling of inactive accounts.

In response to the report, the Department concurred with our recommendations and provided target implementation dates. We are engaged in ongoing communication with the Department regarding the status of these recommendations and will report on Oversight.gov when actions sufficient to close the recommendations have occurred.

III. Conclusion

In the current cyberthreat environment, strong authentication methods and robust account and password management practices are necessary to help protect computer systems from unauthorized access. Overreliance on passwords to restrict system access to authorized personnel can have catastrophic consequences.

The Department's reliance on single-factor authentication only increased the importance of aligning its account management requirements with NIST's recommendations.

To best mitigate the risk of easy-to-crack passwords, the Department should prioritize MFA on all systems and applications. In those instances where MFA has not yet been implemented, password complexity requirements should be updated to comply with NIST guidance.

Thank you for your time. I look forward to answering questions.

QUESTIONS SUBMITTED FOR THE RECORD TO THE HON. MARK GREENBLATT, INSPECTOR GENERAL, U.S. DEPARTMENT OF THE INTERIOR

Questions Submitted by Representative Gosar

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

Answer. The Department of the Interior (DOI) did not address budget issues in its response to our office's report (the DOI's response is included in the report as Appendix 2). The Office of Inspector General (OIG) also has not independently evaluated the DOI's budget. Given that we have not conducted oversight work in this area, we do not have a basis to make findings or draw conclusions about the Department's ability to allocate a greater percentage of its existing budget to cybersecurity initiatives.

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

Answer. Although we have not conducted specific work regarding the DOI's prioritization of cybersecurity initiatives within its existing budget, we have evaluated various aspects of DOI's IT environment, and 64 IT-related open recommendations have yet to be implemented. We have identified seven of these recommendations as "significant," including four from the passwords inspection report that was discussed at the hearing. Designation of a recommendation as "significant" considers a range of factors but, overall, is an indication that we have concluded that it is a particularly important issue to address. Beyond noting this designation, we do not have a basis to make findings or draw conclusions about how the DOI should make prioritization decisions within its current budget.

Dr. GOSAR. Thank you, Inspector General. I now recognize Ms. Cruz Cain for her 5 minutes.

STATEMENT OF MARISON CRUZ CAIN, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Ms. CRUZ CAIN. Chairman Gosar, Ranking Member Stansbury, Chairman Westerman, and members of the Subcommittee, thank you for inviting GAO to contribute to this important discussion about cybersecurity risks at the Department of the Interior.

As you know, Federal agencies and our nation's critical infrastructure, such as energy and transportation, depend on technology systems to carry out operations and to process essential information. The security of these systems and data is vital to protecting individual privacy and our nation's security and well-being. GAO has long emphasized the urgent need for the Federal Government to improve its ability to protect against cyber threats. In fact, we have designated cybersecurity as a government-wide, high-risk area since 1997.

Today, I will focus on cyber threat actors and incidents facing Federal systems and critical infrastructure. I will also discuss recent findings related to Interior's cybersecurity program and practices.

Risk to technology systems are increasing. Malicious actors are becoming more willing and capable of carrying out cyber attacks, which can result in serious harm to human safety, the environment, and the economy. Because of this, agencies and critical infrastructure owners and operators need to protect the confidentiality, integrity, and availability of their systems, and effectively respond to cyber attacks.

According to the 2023 annual threat assessment of the U.S. intelligence community, China, Iran, North Korea, and Russia continue to pose the greatest cyber threats. These countries possess the ability to launch cyber attacks that could disrupt the operations of critical infrastructure, including facilities and assets supporting offshore oil and gas production. Recent attacks demonstrate the impact these threat actors can have on critical infrastructure and systems.

The ransomware attack on the Colonial Pipeline Company led to a shutdown of the pipeline, which resulted in widespread gasoline shortages throughout the southeastern United States. Federal agencies have continued to report tens of thousands of information security incidents each year, which further highlights the importance of protecting their systems and those that support our critical infrastructure.

Accordingly, the Department of the Interior has significant responsibilities, both for protecting its own systems and data, and overseeing the safety of the offshore oil and gas infrastructure. However, both we and Interior's OIG have identified needed improvements in the Department's cybersecurity program and practices.

As my colleague mentioned, in January 2023, Interior's OIG reported that the Department had numerous weaknesses in its

password management. Also, its computer authentication mechanisms and account management practices had weaknesses similar to those that were allegedly exploited in the Colonial Pipeline attack.

Also, in September 2022, we reported on Interior's efforts to establish a comprehensive privacy program. We found that the Department had addressed several important privacy practices, but had not yet incorporated privacy into its organization-wide risk management strategy. This practice is key to ensuring that the Department has established a strategic approach to identify, assess, and manage privacy risks.

Further, in October 2022, we reported that Interior's Bureau of Safety and Environmental Enforcement had not developed a strategy to identify and assess cyber risks to infrastructure supporting offshore oil and gas. Absent such a strategy, offshore oil and gas infrastructure will continue to remain at significant risk from cyber threat actors.

Much to its credit, Interior generally agreed with the recommendations that we and the OIG have made to address these issues, and has outlined plans to implement them. It will be important for the Department to follow through on their commitments to help ensure that the Department is capable of both preventing and responding to the ongoing cyber threats it faces.

In summary, to protect Federal systems and critical infrastructure from cyber-related threats, Federal agencies such as Interior need to ensure that they are effectively implementing risk-based cybersecurity programs and practices. Doing so provides the best protection from cyber attacks that threaten our nation's economic well-being and national security.

This concludes my remarks, and I look forward to answering any questions you may have. Thank you for your time.

[The prepared statement of Ms. Cruz Cain follows:]

PREPARED STATEMENT OF MARISOL CRUZ CAIN, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee: I am pleased to be here today to discuss cybersecurity risks at the Department of the Interior, such as threats posed by malicious actors, including nation-state actors. As you know, federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—depend on technology systems to carry out operations and process, maintain, and report essential information. The security of these systems and data is vital to protecting individual privacy and national security, prosperity, and well-being. Moreover, recent incidents highlight the impact that cyberattacks can have on these systems.

We have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure. In 2015, we expanded it again to include protecting the privacy of personally identifiable information.[1]

This statement discusses various types of threat actors and attacks that could compromise federal systems and our nation's critical infrastructure, such as that overseen by Interior. It also discusses cybersecurity risks that we and the Office of the Inspector General have identified at the department.

[1] See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, DC.: Apr. 20, 2023).

This statement is based on previously issued GAO reports on cybersecurity at Interior and other federal agencies. We also reviewed Interior Office of Inspector General reports and other public information sources.

We conducted the work on which this testimony is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The U.S. Department of the Interior's mission is to protect and manage the nation's natural resources and cultural heritage, provide scientific and other information about those resources, and honor its trust responsibilities and special commitments to American Indians, Alaska Natives, and affiliated Island Communities. The department plays a central role in how the United States stewards its public lands, increases environmental protections, pursues environmental justice, and honors our nation-to-nation relationship with Tribes. The department carries out its mission through 11 technical bureaus:

- Bureau of Indian Affairs
- Bureau of Indian Education
- Bureau of Land Management
- Bureau of Ocean Energy Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- Bureau of Trust Funds Administration
- National Park Service
- Office of Surface Mining Reclamation and Enforcement
- U.S. Fish and Wildlife Service
- U.S. Geological Survey

In addition to the 11 bureaus, a number of offices fall under the Office of the Secretary, Office of the Assistant Secretary for Policy, Management and Budget, the Solicitor's Office, and the Office of Inspector General.

Interior IT Security Responsibilities

Interior is responsible for protecting the confidentiality, integrity, and availability of its information and information systems. Specifically, the Federal Information Security Modernization Act of 2014 (FISMA) was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[2]

FISMA requires agencies to develop, document, and implement an agency-wide information security program to secure federal information operations and assets of the agency. These information security programs are to provide risk-based protections for the information and information systems that support the agency's operations. FISMA requires agencies to comply with the Office of Management and Budget's (OMB) policies and procedures, the Department of Homeland Security's (DHS) binding operational directives, and the National Institute of Standards and Technology's (NIST) information security standards.

Interior's Office of the Chief Information Officer (OCIO) leads Interior's security management program. The office's mission and primary objective is to establish, manage, and oversee a comprehensive information resources management program. The Interior Chief Information Security Officer (CISO) reports to the Chief Information Officer and oversees the Information Assurance Division. This division is responsible for Interior's IT security and privacy policy, planning, compliance, and operations.

Each of Interior's bureaus and offices have an Associate Chief Information Officer (ACIO) that reports to the department Chief Information Officer and the Deputy Bureau Director. The ACIO serves as the senior leader over all IT resources within

[2] The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

the bureau or office. Each also has an Associate Chief Information Security Officer that represents the Bureau and reports to the Bureau ACIO and Interior's CISO.

Interior Offshore Oil and Gas Responsibilities

Interior's Bureau of Safety and Environmental Enforcement (BSEE) is responsible for overseeing offshore oil and gas operations, including cyber risks. The bureau's mission is to promote safety, protect the environment, and conserve resources offshore through regulatory oversight and enforcement. It is responsible for overseeing offshore operations, which includes the authority to investigate incidents that occur on the outer continental shelf, monitor operator compliance with environmental stipulations, and take enforcement actions against operators that violate safety or environmental standards.

BSEE's regulatory programs advise a wide range of offshore activities and facilities, including drilling, well completion, production, pipeline, and decommissioning operations. The bureau implements advancements in technology and conducts onsite inspections to assure compliance with regulations, lease terms, and approved plans. To date, BSEE's regulations do not explicitly mention cybersecurity, but the bureau has determined that addressing cybersecurity risks to offshore oil and gas infrastructure aligns with its mission to promote safety and protect the environment.

Cyber Threat Actors Pose Serious Risks to Federal Systems and Critical Infrastructure

Risks to technology systems are increasing. In particular, systems and networks supporting federal agencies and U.S. critical infrastructure are becoming more vulnerable to cyberattacks. These systems and networks are composed of, and connected to, enterprise IT systems and operational technology systems.[3] 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.

Overview of Cyber Threat Actors

Key cybersecurity risks to federal agencies and U.S. critical infrastructure also include the growing attack capabilities of threat actors. According to the 2023 *Annual Threat Assessment of the U.S. Intelligence Community*, China, Iran, North Korea, and Russia pose the greatest cyber threats.[4] Of particular concern, these countries possess the ability to launch cyberattacks that could have disruptive effects on critical infrastructure, including facilities and assets supporting offshore oil and gas production. Further, the assessment stated that transnational organized ransomware actors continue to improve and execute high-impact ransomware attacks, extorting funds, disrupting critical services, and exposing sensitive data. Table 1 describes common types of cyber threat actors.

Table 1: Common Cyber Threat Actors

Threat actor	Description and potential motivation
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. Chinese and Russian cyber threat actors have previously targeted the U.S. energy sector, including oil and gas companies. In addition, Iran has previously targeted foreign oil and gas companies using cyberattack techniques.
Transnational criminal groups	Transnational criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. Further, cyber criminals are increasing the number, scale, and sophistication of ransomware attacks that threaten to cause greater disruptions of critical services.

[3] Enterprise IT systems encompass traditional IT computing and communications hardware and software components that may be connected to the internet. Operational technology systems monitor and control sensitive processes and physical functions, such as offshore oil and gas operations.

[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023).

Threat actor	Description and potential motivation
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. For example, according to U.S. Coast Guard officials, the agency considers environmental groups opposed to petroleum development to be a threat actor that could potentially target offshore oil and gas infrastructure.
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. This can occur through the destruction, disclosure, or modification of data, or through denial of service. Bureau of Safety and Environmental Enforcement officials indicated that insiders, such as a disgruntled employee, could cause issues on an offshore oil and gas facility.

Source: GAO analysis / GAO-23-106869

Examples of Cyberattacks

Cyber adversaries use a variety of tactics and techniques to exploit vulnerabilities and attack systems and networks. According to MITRE's ATT&CK® Framework, attackers tend to follow common methodologies to compromise targets and achieve their goals. For example, threat actors can use multiple techniques, such as compromising the supply chain of hardware and software, to gain initial access to IT and operational technology systems.[5]

In fiscal year 2022, federal agencies reported 30,659 information security incidents across nine categories,[6] which represents a 5.7 percent decrease from the over 32,500 incidents reported in fiscal year 2021.[7] Examples of successful cyberattacks demonstrate the impact they can have on federal systems and the nation's critical infrastructure:

- In May 2023, Microsoft reported that it uncovered cyberattacks by Volt Typhoon, a state-sponsored actor based in China. According to Microsoft, Volt Typhoon has been active since 2021 and has targeted critical infrastructure in communications, manufacturing, utility, transportation, government, and IT, among other sectors. Microsoft also reported that Volt Typhoon is aiming to develop capabilities that could disrupt communication infrastructure between the United States and Asia during future crises.
- In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyberattack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. According to a joint advisory released by DHS and the FBI, the company proactively disconnected certain systems that monitor and control physical pipeline functions to ensure the safety of the pipeline. This resulted in a temporary halt to all pipeline operations, which led to gasoline shortages throughout the southeast U.S.
- In December 2020, the cybersecurity firm FireEye discovered that a SolarWinds product known as Orion was compromised and being leveraged by a threat actor for access to its customer systems. Hackers inserted malicious code into Orion—a product widely used in both the federal government and private sector to monitor network activity and manage devices. The threat actor, the Foreign Intelligence Service of the Russian Federation, used Orion to breach several federal agency networks. The initial breach opened a backdoor to agency systems that enabled the threat actor to deliver additional malicious code. This allowed the actor to move laterally, gathering information and compromising data.

[5] The supply chain is a linked set of resources and processes that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

[6] The nine categories of incidents are (1) attrition, (2) email/phishing, (3) external/removable media, (4) impersonation/spoofing, (5) improper usage, (6) loss or theft of equipment, (7) web, (8) other/unknown, and (9) multiple vectors.

[7] Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report Fiscal Year 2022*. The number of incidents are from OMB's fiscal year 2022 annual FISMA report to Congress, which is based on incidents reported to the Cybersecurity and Infrastructure Security Agency by federal agencies. OMB notes that drawing conclusions based on this data point would be premature, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years.

- In 2015, Russian threat actors conducted a cyberattack on the Ukrainian power grid that systematically disconnected substations, resulting in a power outage for about 225,000 customers.
- According to the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, from December 2011 to 2013, state-sponsored Chinese actors conducted a spearphishing and intrusion campaign targeting U.S. oil and gas pipeline companies. Of the 23 targeted pipeline operators, 13 were confirmed compromises.

Progress Has Been Made, but Interior's Cybersecurity Practices Have Weaknesses

While Interior has made progress in addressing previously reported cybersecurity weaknesses, both the department's Office of Inspector General (OIG) and GAO have continued to identify multiple weaknesses in the department's cybersecurity program and practices. These include issues affecting both Interior's own security environment and its oversight of offshore oil and gas infrastructure.

Interior's Inspector General Identified Weaknesses in Cybersecurity Practices

In January 2023, Interior's OIG issued a report examining the department's password complexity requirements.[8] The OIG found that the department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Specifically, the OIG determined that the department (1) had not consistently implemented multifactor authentication, (2) used password complexity requirements that were outdated and ineffective, (3) used password complexity requirements that implicitly allowed unrelated staff to use the same inherently weak passwords, and (4) did not promptly disable inactive (unused) accounts or enforce password age limits. The OIG noted that if a malicious actor were to compromise an account with elevated privileges, such as a system administrator's account, the magnitude of harm would increase. The OIG made eight recommendations to help the department strengthen its IT security by improving user account management practices. The department concurred with the OIG's recommendations.

In April 2023, the OIG released a summary of an independent audit, carried out by a contractor on behalf of OIG, of the department's information security program.[9] The summary indicated that Interior's program was not effective because it was not consistent with applicable FISMA requirements, OMB policy and guidance, or NIST standards and guidelines.[10] The contractor identified needed improvements in the areas of risk management, supply chain risk management, identity and access management, configuration management, data protection and privacy, information security continuous monitoring, incident response, and contingency planning. To address these weaknesses, the contractor made 24 recommendations intended to strengthen the Interior's information security program as well as those of the bureaus and offices. The department concurred with all recommendations and established a target completion date for each corrective action.

GAO Has Reported on Gaps in Interior's Approach to Managing Cybersecurity and Privacy Risks

Cybersecurity risk management: In July 2019, we reviewed the cybersecurity risk management practices at the 23 civilian Chief Financial Officers (CFO) Act agencies, which includes Interior.[11] We found that the department had not fully addressed three of five key practices for establishing its cybersecurity risk management program. Specifically, the department had not (1) developed a cybersecurity risk management strategy that addressed key elements, (2) fully documented risk-based policies and procedures, or (3) fully established a process or mechanism for coordination between its cybersecurity risk executive and its enterprise risk man-

---

[8] Department of the Interior Office of Inspector General, *P@$$words at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk*, 2021-ITA-005 (January 2023).

[9] Department of the Interior Office of Inspector General, *Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2022*, 2022-ITA-028 (April 2023).

[10] According to OMB's fiscal year 2022 Core IG Metrics Implementation Analysis and Guidelines, a security program is considered effective if most of the fiscal year 2022 Core Inspector General Metrics are at least Level 4, "Managed and Measurable." Using OMB's guidance and the CyberScope results, the contractor determined that most of the cybersecurity functions were Level 3, "Consistently Implemented."

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

agement governance structure. We recommended that Interior take steps to address these gaps. Since then the department has implemented all three recommendations. Implementing these foundational practices is a critical step in ensuring Interior can make consistent, informed risk-based decisions to protect agency systems and information against cyber-based threats.

IT workforce planning: In October 2019, we reported on the extent to which the 24 CFO Act agencies had implemented key IT workforce planning activities.[12] We found that Interior had partially, minimally, or not implemented the key practices. This included, for example, assessing gaps in competencies and staffing. Accordingly, we recommended that Interior fully address the workforce planning activities. As of May 2023, Interior had taken some steps, but work remained to fully implement these activities. A key to having a successful cybersecurity program is having a well-trained, highly qualified workforce that is versed in identifying cyber threats and recognizes steps to take once confronted with them.

Information and communications technology supply chain risk management: In December 2020, we issued a public version of a sensitive report reviewing the information and communications technology (ICT) supply chain risk management programs and practices at the 23 civilian CFO Act agencies (which includes Interior).[13] None of the 23 agencies, including Interior, fully implemented all of the foundational practices for supply chain risk management. Fourteen of the 23 agencies had not implemented any of the practices. In the sensitive version of the report, we made a total of 145 recommendations to the 23 agencies to fully implement these practices. Implementing these practices will help organizations protect against supply chain risks, such as the insertion of counterfeits and malicious software, unauthorized production, and tampering, as well as poor manufacturing and development practices throughout the system development life cycle.

Privacy of personal information: In September 2022, we reported on a review of privacy programs at the 24 CFO Act. Agencies.[14] We found that Interior had addressed most of the key practices for establishing a privacy program. However, the department had not fully incorporated privacy into its department-wide risk management strategy, to include a determination of risk tolerance. We recommended that Interior establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. Interior concurred with this recommendation and plans to implement it by November 2023. Such a strategy will help the agency ensure that it is managing risks to sensitive personal information consistently and within acceptable parameters.

Cybersecurity of offshore oil and gas infrastructure: In October 2022, we reported that BSEE had long recognized the need to address cybersecurity risks to offshore oil and gas infrastructure but had taken few actions to do so.[15] In 2015 and 2020 BSEE initiated efforts to address cybersecurity risks, but neither resulted in substantial action. In 2022, BSEE started another such initiative and hired a cybersecurity specialist to lead it. However, bureau officials said the initiative will be paused until the specialist is adequately versed in the relevant issues.

We recommended that BSEE immediately develop and implement a strategy to address offshore infrastructure risks. Such a strategy should include an assessment and mitigation of risks and identify objectives, roles, responsibilities, resources, and performance measures, among other things. Absent the immediate development and implementation of an appropriate strategy, offshore oil and gas infrastructure will remain at significant risk. In March 2023, the department indicated that BSEE is developing a cybersecurity strategy and anticipates that this strategy will be complete by the end of calendar year 2023.

---

[12] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, DC.: Oct. 30, 2019).

[13] GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, DC.: Dec. 15, 2020). This is a public version of a sensitive report that GAO issued in October 2020. Information that agencies deemed sensitive was omitted and, due to sensitivity concerns, GAO substituted numeric identifiers that were randomly assigned for the names of the agencies.

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

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

In summary, cyber threats continue to pose a significant threat to systems supporting the federal government and critical infrastructure. Successful cyberattacks, including those carried out by nation-state actors, could have catastrophic consequences for the economy, national security, and human safety and well-being. The Department of the Interior needs to continue to take steps to ensure that its systems and data are protected from cyber-based attacks carried out by malicious actors. Moreover, Interior needs to ensure that it is addressing cybersecurity risks to critical infrastructure assets for which it has responsibility.

Chairman Gosar, Ranking Member Stansbury, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

*****

GAO Highlights

Highlights of GAO-23-106869, a testimony before the Subcommittee on Oversight and Investigations, Committee on Natural Resources, House of Representatives

June 7, 2023

CYBERSECURITY

Interior Needs to Address Threats to Federal Systems and Critical Infrastructure

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 the 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.

United States Government Accountability Office

Ms. Cruz Cain submitted her prepared statement as a GAO report. The statement as a GAO report can be viewed on the Committee Repository at:

https://docs.house.gov/meetings/II/II15/20230607/115966/HHRG-118-II15-Wstate-CruzCainM-20230607.pdf

QUESTIONS SUBMITTED FOR THE RECORD TO MS. MARISOL CRUZ CAIN, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Questions Submitted by Representative Gosar

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

Answer. 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.

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

Answer. 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

---

[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).

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

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.

Questions Submitted by Representative Grijalva

Question 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?

Answer. 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.

Dr. GOSAR. I thank Ms. Cruz for her testimony. We will now go to Members for their 5 minutes. I first recognize the gentleman from Arkansas, the Chairman of the Full Committee, Mr. Westerman.

Mr. WESTERMAN. Thank you, Chairman Gosar. And, again, thank you to the witnesses.

Inspector General Greenblatt, a lot of interesting stuff in your testimony. The Password Complexity Report discusses how passphrases that you mentioned may be more effective than passwords, and how a "negative feedback loop" has developed for password requirements. Can you explain what passphrases are in a little more detail, what you mean by a negative feedback loop for passwords, how passphrases are a better solution, you alluded to

[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, DC.: June 7, 2023).

that, but also how AI can be used to crack passwords, and even maybe passphrases?

Mr. GREENBLATT. Passphrases, in short, are just a string of unrelated words. The example that we used in our report is "dinosaur letter trail chants." It takes a computer 550 years to figure that out, as opposed to a password, which might appear to be more complicated. It actually is easier for the computer to crack that. For example, that can take a computer 3 days, as opposed as opposed to 550 years to crack a passphrase.

So, the key is, as hackers have been getting better about hacking into passwords, we have increased the complexity requirements on the passwords, which means as humans, we have to adopt mechanisms to make them easier to remember. Making them easier to remember makes them easier to crack. So, that is this negative feedback loop that, as the complexity requirements have increased, the quality of the passwords has decreased.

That is why the movement throughout government, and this is set by the NIST, the National Institute of Standards and Technology, which is the standard-setting body for the U.S. Government with respect to these issues, has said we should go to passphrases. Again, that is a string of unrelated words which is almost impossible for a computer to crack in a reasonable amount of time.

Mr. WESTERMAN. So, will AI help aid in cracking even those passphrases in a shorter amount of time, my understanding with AI is it can profile you and learn, if you will. Will it somehow be able to know that you picked dinosaur whatever it was?

[Laughter.]

Mr. GREENBLATT. Yes, right. I am sure it is going to get better. The technology is going to get better and better, so we will have to stay in front of it. The key is the length of the passphrase. The longer it is, the more difficult it is for a computer to figure it out.

Mr. WESTERMAN. And then doing the multi-factor authorization on top of a passphrase sounds like the direction we need to head.

Mr. GREENBLATT. That is exactly right. Here is the mnemonic that I use to remember this, because I am a layman, I am not a cybersecurity expert. But the way I remember it is password is bad; passphrase is better; MFA best. That boils down my entire testimony in seven words.

Mr. WESTERMAN. That is pretty easy. Thank you.

Ms. Cain, your testimony declared that DOI had not fully implemented key information technology workforce planning recommendations that were originally made in 2019. What were those recommendations? What are the recommendations DOI has failed to implement, and why have they still failed to implement them 5 years later?

And maybe a follow-up to that is, with this hearing, with your reports, hopefully they have gone in and changed the passwords, the ones that you cracked in 90 minutes, 16 percent of them. Are you seeing any improvements at DOI, or do we know?

Ms. CRUZ CAIN. Much to its credit, we can say today that we have received information from Interior, and we are going to close each one of those workforce recommendations that we had.

Some of the workforce recommendations were looking at their skilled workers and filling up gaps in different types of technical

workers that they needed, and they have, to this date, given us documentation to prove that they have closed all of their workforce recommendations.

So, we are very happy about that. Yes, it did take 5 years, but much to Interior's credit, they have been continually working on it, and have gotten to a good place with our recommendations specific to the workforce.

We have not done any password work at Interior, or really haven't looked into Interior's systems. We would be more than happy, if there is a specific Interior system you would like for us to look at, but we do not have any recent work that has looked into a specific Interior system.

Mr. WESTERMAN. Thank you.

And just real quickly, Inspector General, when did you do the hacks? When did you crack these? How long ago was that?

Mr. GREENBLATT. It was at least a year ago, because we gave the Department a chance to fix much of this. So, it had to be at least a year ago.

Mr. WESTERMAN. OK, thank you.

Thank you, Chairman. I yield back.

Dr. GOSAR. I thank the gentleman. The gentleman from Hawaii, Mr. Case, is recognized.

Mr. CASE. Thank you, Mr. Chair.

Mr. Greenblatt, you testified that DOI, I think your words were, generally concurred in your recommendations, or the OIG's recommendations, and established target dates. Are you satisfied with their target dates, are they reasonable?

What kind of time frames are we talking about?

And what are the obstacles to expeditious implementation?

Mr. GREENBLATT. Yes. Generally speaking, they have been very constructive. The relationship we have had has been very productive with them. I have had a number of engagements with the Chief Information Officer there. They, and the Deputy Secretary, frankly, appear to be oriented in the right direction.

In terms of the target dates, they do seem reasonable to us. We would have said so in the report if we did not find them reasonable. We have done that in other contexts. In this context, we found them to be reasonable. In fact, one of the recommendations, they have already submitted the packet of materials to close one of our recommendations, and we are just going through the process of looking at that right now.

I also understand that they have taken some steps already to implement measures with respect to the passwords and shifting over to passphrases. So, that was a very constructive result.

In terms of the problems with respect to timing, this would appear likely on the multi-factor authentication piece, where there are some systems that are so old that they can't handle MFA. So, that is my understanding from the Chief Information Officer.

But this is information you would have to get from them. They know this better than we do, but that is my understanding, is that it is something like that, where they are technologically having difficulty actually handling it on the infrastructure that they have right now.

Mr. CASE. So, is it your understanding, from your perspective, that the target date implementations, are any of them reliant on supplemental funding, or insufficient personnel, or inability or unavailability of technical resources?

I guess what I am asking is, what are the obstacles to getting them done fast, and can we do anything about any of those obstacles?

Mr. GREENBLATT. Well, I think one undercurrent for everything with respect to IT and cybersecurity is finding qualified staff. It is very difficult in the public sector to hire the types of folks with the types of experience that you need in the IT security space, so that is underlying sort of all of this.

With respect to these specific recommendations, I don't know the answer to that, whether there are technological hiccups or supplemental funding. We can get back to you on that. I think that is a fair question that I just don't know, off the top of my head.

Mr. CASE. OK, thank you. I guess I have heard it said or described, or at least my understanding of cybersecurity cyber attacks is they kind of fall into a couple of different categories. One would be state-sponsored for state goals, as we apparently or may well have seen just recently with respect to Guam. Another is issue-oriented to influence a particular issue. Another would be extortion disruption, so money. And then the fourth category would just be to see whether you can get away with it.

Talking about DOI specifically for now, I guess my real question is what is the direct subject of a cyber attack to DOI?

What is the real exposure at DOI?

Ms. Cruz Cain made reference three or four times to offshore oil, so I assume that it is our management of our natural resources themselves, and the implications to our economy and our defense. But where does a cyber attacker tend to engage with DOI?

Mr. GREENBLATT. Again, I think you would have to go to the Department with respect to specific attacks and where they came from. But I think what is fair to say is that DOI houses significant information, be it proprietary information related to oil and gas sales and from the energy leasing, offshore security, offshore oil and gas extraction and security issues as we were saying a second ago.

But you know we have hydroelectric dams that power hydroelectric power plants that feed into the electrical grid. So, I don't know how an attack could compromise, say, an electrical grid or something along those lines. These folks are very, very creative, and very malicious. It is sort of impossible to know at this point. But I think the full scope of the damage is fairly daunting if we were to see an attack unfold.

Mr. CASE. Thank you very much.

Dr. GOSAR. I thank the gentleman. The gentleman from Georgia, Mr. Collins, is recognized for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman. I had some other questions, but as you all were speaking, Inspector General, you led me to a whole bunch of other questions.

Being in the private sector, in the trucking industry, I mean, this is something we deal with daily because of the nature of what we are in, and the possibility of getting hacked, mostly from the

monetary side of it. So, I have a few I was just going to run by you. If it doesn't apply to you and maybe Ms. Cruz Cain, if you can answer it, then just feel free to jump in there.

You did the study in 2022, and you said you had a reasonable timeline for them to implement this, correct? What was that timeline?

Mr. GREENBLATT. We can get you the dates in particular.

Mr. COLLINS. Was it 6 months, or 2 months, or——

Mr. GREENBLATT. It is probably more than 6 months for us to write the report. We share our findings with the Department, especially in something like this, where we want them to take steps to cure the problems before we were going public. So, it is a good amount of time. It may be a full year.

Mr. COLLINS. OK. So, the problems, though, that you are speaking about are maybe software-related, the reason they can't use multi-factor authentication?

Mr. GREENBLATT. Sometimes, certainly, like——

Mr. COLLINS. Are they just running old systems?

Mr. GREENBLATT. It could be, yes. And that is what I have heard. That is my understanding, yes.

Mr. COLLINS. OK.

Mr. GREENBLATT. On some of the systems.

Mr. COLLINS. When you do multi-factor authentication that you put in there—we all use phrases now, instead of just passwords, it is easier to remember it, too. Is there a length that you put in there for the password, the passphrase, and then capital letters, numbers, and symbols, as well?

Mr. GREENBLATT. You don't have to do that. That is the beauty of the passphrase, is that it is designed to be easy to remember. So, it can just be words.

What I have seen is between 16 and 64 characters long. That is what I have seen, just generally speaking, out in the world. But the longer you go, the more and more difficult it becomes for a hacker to crack it.

Mr. COLLINS. Yes, I just know that the nature of people, if you say, "Give me three words," it is going to be "at," "the," and "I," you know.

[Laughter.]

Mr. GREENBLATT. Fair enough. But I think what you can do is you can limit the nature of what is a permissible passphrase.

Mr. COLLINS. Yes, that is what I am saying——

Mr. GREENBLATT. You can limit that sort of thing. Again, it is really length, not the quality of the words.

Mr. COLLINS. So, when you recommended that they implement, and you said it was high-quality assets first, is this now agency-wide?

Mr. GREENBLATT. The passphrases, yes. My understanding is, again, this is a question that they can give you a better answer. But, yes, my understanding is that they have implemented on the passphrases, getting away from the passwords.

On multi-factor authentication, that is a longer fuse, because they have some of those legacy systems that are very, very old that apparently can't handle multi-factor authentication.

The other thing, by the way, when you were just asking a second ago about the software, they had a number of systems that could handle multi-factor authentication. But they were allowing people to solely use passwords. So, what we are saying is turn that bypass off.

Mr. COLLINS. Yes, are you all doing, for lack of better words, follow-up hacks? I mean, my IT group does it on a monthly basis.

Mr. GREENBLATT. We are doing a number of penetration testing. We have a number of jobs in the works, and that is what the team does on a day-to-day basis.

But on this issue we now have turned it over to the Department and, hopefully, they will be doing that on their own.

Mr. COLLINS. Is that something, Ms. Cruz Cain, that you would answer?

Ms. CRUZ CAIN. We don't have any work planned at Interior. We really respond as requests from Committees or Members. So, if that is something that you would like us to do, we would be more than happy to take on another password job, or look at multi-factor authentication at Interior.

Mr. COLLINS. I know this may be off subject, but you all don't do phishing expeditions with e-mails to see if people bite, I mean, that is another way that people hack in pretty easy.

Mr. GREENBLATT. The Department should be doing that on their own. Any agency should be doing penetration testing on their own. We could conceivably do that sort of thing, but we take a risk-based analysis on where we can add the most value. But the Department, in theory, should be doing that as part of its regular, day-to-day maintenance, if you will.

Mr. COLLINS. So, you set up the parameters, right, for any agency, you set that up. Do you have password expiration dates, where they have to change the passwords? Do you recommend that?

Mr. GREENBLATT. We did. But if you have passphrases, you don't—

Mr. COLLINS. I know, passphrase.

Mr. GREENBLATT. Yes, you don't need to. For passphrases, they are so robust that you actually don't need to change them. That is part of the problem with the passwords, is that you need to change them every 60 to 90 days, and people need to make them easy to remember. But that makes it easier to hack. With the passphrases, if they are long enough, you don't need to change it.

Mr. COLLINS. My time is expired, but I will tell you that in my world we always say those are famous last words.

Mr. GREENBLATT. There is no question that the hackers and their technology will evolve. There is no question about that. I am not saying that this is the forever answer, but right here, right now, this is the best technology that we can do. And they are going to have to do something pretty robust to figure it out.

Mr. COLLINS. Right.

Sorry, Mr. Chairman.

Dr. GOSAR. Just as long as it is not "Run, Spot, run," right?

[Laughter.]

Dr. GOSAR. The gentlewoman from Nevada, Ms. Lee, is recognized.

Ms. LEE. Thank you, Mr. Chairman, and thank you, Ranking Member Stansbury. Before I get into my question for Ms. Cruz Cain I just wanted to ask Mr. Greenblatt.

The software that DOI is using, sometimes when I am using software there are limitations on the length. So, you are saying the software that DOI now uses does not have that limitation, or do we need to invest in new software?

Mr. GREENBLATT. Those are great questions for the agency. They have dozens of different systems at play.

Ms. LEE. Oh, OK.

Mr. GREENBLATT. So, I don't know each and every one of theirs and what their length requirements are, but that is something that I would think they can change, they can modify. But my understanding is that they have moved to passphrases of an appreciable length, like I said, 16 characters or something along those lines. But that is a good question for them to flesh out.

Ms. LEE. Ms. Cruz Cain, in your opinion, does DOI have the sufficient resources to address these threats and make the needed changes?

Ms. CRUZ CAIN. We have made the observation that they are challenged by their IT budget. Most of their IT budget, about 83 percent of it, goes toward just operating and maintaining its IT systems. And that includes a lot of the aging and legacy systems that we have been mentioning, which do not allow newer technologies to be used, such as multi-factor authentication. And it really hinders the ability to deal with the new cyber risks. You are constantly going back to outdated software, outdated hardware, and these legacy systems.

So, that is one challenge that we have noted at GAO, that they are spending about 83 percent of their budget just maintaining. And we really are asking them to shift their focus of their budget to development, modernization of those legacy systems, and making enhancements that would better position Interior to modernize those legacy systems, and then address the associated vulnerabilities with those systems, and be able to engage with the new cybersecurity technologies like multi-factor authentication.

Ms. LEE. Do you have any dollar estimate on what is necessary, or is that something I need to get from DOI?

Ms. CRUZ CAIN. No, that is definitely something you need to get from the DOI.

Ms. LEE. All right. I am also deeply concerned, being from the West, on a potential cyber attack on critical DOI water infrastructure. As you know, 40 million people rely on the Colorado River and its reservoirs, which have long been under DOI care, including Lake Mead, which is the main water source for my hometown and home state of Nevada.

With this in mind, how do you think infrastructure under the DOI, whether it is water resources, power grid maintenance, or oil and gas would be impacted by a hack?

Mr. GREENBLATT. I think it would depend on the hack and what they did. But it could be devastating. Like I said, it just depends on where, and how, and what they do with it. If they are just stealing information versus doing something actively malicious, it is impossible to know.

But also, they could be using the pathway into the Department to then try to get up to higher-level access to other departments that DOI may be connected to. So, that is the kind of thing, they may be a pass-through if they are connected to other networks. It is very difficult to say, but it could be devastating.

Ms. LEE. Can you expand on the measures that DOI is taking right now to ensure that we prevent such a hack?

Are you comfortable that they are taking the measures, or is this a resource issue that we need to give them more funding so they can modernize?

What is the, I guess, the chicken-and-the-egg type of thing? What are the priorities?

Mr. GREENBLATT. So, there are a couple of answers to that.

First of all, with respect to implementing the passphrase requirements, that looks like that has happened, I think that is 100 percent. I remember speaking with the Chief Information Officer, and I believe he said that was 100 percent at this point. So, on the passphrases, that is a good thing.

With MFA, that is going to take a little bit longer. But I believe they are oriented in the right direction with respect to MFA, it is just going to take a little heavier lifting for them.

In terms of their specific timing on all the various systems, you will have to get a breakdown from them in terms of the individual ones.

The thing that was most troubling to me was the MFA, the multi-factor authentication, with respect to the high-value IT assets. The ability to bypass multi-factor authentication on those systems was troubling. So, I believe they have a constructive posture with respect to those systems, I just don't know where they actually sit with respect to all of those that had permitted the bypass or the password alone.

Ms. LEE. Great, thank you.

I am over my time.

Dr. GOSAR. I thank the gentlelady from Nevada. I recognize the Ranking Member from New Mexico, Ms. Stansbury, for her 5 minutes.

Ms. STANSBURY. Thank you, Mr. Chairman, and thanks again to our witnesses for being here today. I wonder if we could start with Ms. Cruz Cain.

What exactly did these attacks look like? I think we all think we know what a cyber attack looks like, but what does the experience of a hacker and an attack actually look like?

Ms. CRUZ CAIN. I think it depends on what kind of attack is being executed. My colleague gave the examples of different attacks. If you are looking on attacks to operational technology, and when we did our report on the oil and gas infrastructure, an attack on that operational technology, which is the software and the hardware that are used to control the industrial equipment, that is going to look very different depending on who hacks. So, you can put malicious code into some of the software and hardware, and that might take a little bit longer to detect.

It could be a ransomware attack. Somebody could completely shut down that operational technology, which makes it unable to use the production, which would slow down oil and gas. It could

prevent water flow. It could do a lot of harm to the economy, to our well-being.

I think it just all depends on what type of attack you are trying to perpetrate.

Ms. STANSBURY. Yes, and I think, like I said, oftentimes we think we are all talking about the same things, but there are a multitude of different kinds of actors and different kinds of attacks that we are talking about here. So, the implications of whether or not it is the password infrastructure of the individuals who are holding files, who have access to shared systems, who are operating systems that may be related to energy infrastructure or water infrastructure, or it is just the personal identifying information of Federal employees, all of these things are vulnerabilities to these kinds of hacks and these actors.

And as we were preparing for this hearing, I was actually sharing with some of the staff that I am a former Fed myself. I used to work for a Federal agency, and we actually experienced a hack while I was working for a Federal agency by a foreign actor. And I can tell you they were inside our system, we studied them, we shut them down, and we made sure it never happened again. But these hacks can have very significant implications for agencies, so we take them very, very seriously.

And Ms. Cruz Cain, we were interested in particular in the report that you helped to co-author on privacy, dedicated leadership report. And one of the recommendations in that report suggested that our agencies institute privacy leadership in each of the agencies. Could you tell us a little bit more about what that means, what it would look like, and how Congress could help to support an initiative like that?

Ms. CRUZ CAIN. Sure. What we found when we were looking at the 24 CFO Act agencies was that outside of the ones who were mandated by law to have a chief privacy officer that serves at the executive level alongside the CIO, the CFO, and other high-level executives, most of the agencies differed. Some of the chief privacy officers could have been their CIO. They could have been just a person who was in charge of privacy.

So, we also noticed that their responsibilities differed. Some of them solely focused on privacy, which was very few, but others had different responsibilities, some were doing records management, as well; some were doing financial management; some were doing information technology.

And with the increasing nature of these cyber attacks, GAO and all of the agencies that we talked to really think that having someone, some executive-level senior official focused just on privacy as their only responsibility will really elevate privacy to where it needs to be in all of the agencies. Not only do you have the personal information of your employees, you also have proprietary information in many agencies, different types of information that, if leaked, could be very harmful for the Federal agencies.

And in our report, the matter to Congress was to just go into law and say there should be a senior official at that executive level that can have visibility into privacy, and bring that to the table when you are making the high-level decisions.

Ms. STANSBURY. So, really standardizing that leadership within each of the agencies. And I think that brings me to my final question for this panel, which is for Mr. Greenblatt.

We had the opportunity to chat briefly before the hearing, and one of my questions, which you touched on, but I want to just ask you to expand on a little bit more, is about DOI's leadership in addressing not only the password considerations, but also these other cyber risks that have been talked about today in this hearing.

Talk to us about what Interior has been doing to address these vulnerabilities, and what we in Congress can do to help support the Department of the Interior and other agencies on their journeys in securing their cyber programs.

Mr. GREENBLATT. Yes, like I said, we have had a very constructive engagement with them. They concurred with all the recommendations with respect to this report, and they have already implemented some of them. We have to close those recommendations. They give us the information for us to close them. They have done that with one of the recommendations that we have to then sort of go through and make sure that it is done. The other ones are pending.

But, so far, the posture has been very constructive. I engaged with the Deputy Secretary and with the CIO on these topics, and I know that they at least have represented to me that they are taking it very seriously, and I have no reason to challenge that.

Ms. STANSBURY. Thank you. And I know we are out of time, but certainly we will be looking to both the OIG, as well as GAO for recommendations for how we can address this at the structural level, whether that is funding, as my colleague brought up, or through statutory and leadership needs within the agency. So, thank you.

Dr. GOSAR. I thank the gentlelady. I am going to start with you, Inspector General.

Are there any problems for the Department of the Interior to access high-end technology?

Mr. GREENBLATT. No, I think they could, subject to FedRAMP authorization and that sort of thing. But no, I don't think there are any barriers that are unique to DOI, as opposed to other Federal agencies.

Dr. GOSAR. So, on these passwords, are there random checks on employees?

Mr. GREENBLATT. I do not know the answer to that question, actually.

Dr. GOSAR. Would that be something of value?

Mr. GREENBLATT. It could be, sure.

Dr. GOSAR. I mean, I get lazy, and all of us get that notice that you have to change your password. So, I mean, from that standpoint it would be nice to know that they are implemented. I think that it sounds like that is one area we can really close.

Mr. GREENBLATT. Certainly, they have certain parameters on what you can do. It has to be a certain length and there may be some prohibited terms, I don't know. But that is the kind of thing that I think in order to set it up, it has to meet those parameters. I don't know if they do checks following the setup.

Dr. GOSAR. OK. Ms. Cruz Cain, the GAO has been sounding the alarm over the cybersecurity vulnerabilities at BSEE since 2015. Finally, in 2022, BSEE hired a cybersecurity specialist to address vulnerabilities to offshore infrastructure. But Bureau officials said the initiative would be paused until the specialist is adequately versed in the relevant issues. Do you have any update on this?

Ms. CRUZ CAIN. The one update that Interior gave us was that they are, in fact, developing their cybersecurity strategy that encompasses all the elements that we recommended, and they anticipate the strategy being done at the end of this calendar year.

Dr. GOSAR. And then you will follow up with that?

Ms. CRUZ CAIN. Absolutely. We do normal follow-up for all recommendations.

Dr. GOSAR. OK. Now, from your vantage point at GAO, is there a prioritization process that you see that should be followed in addressing these cybersecurities?

Ms. CRUZ CAIN. Well, definitely, the strategy is the key. You have to have a strategy. You have to identify your cyber risks. And each sector and each agency is going to have different priorities and different cyber risks.

So, you have Interior's internal systems that will probably have different risks to them. And then, with BSEE, they have the offshore oil and gas infrastructure. So, our report focused on that, and wanted them to just have a strategy. How are you going to identify your risks? How are you going to assess those risks? What are your objectives? What are your activities and performance measures that you are going to measure up to when you are putting your cybersecurity strategy into place? Roles and responsibilities are important, and also coordination with CISA and any other entities that they need to talk to in order to make their strategy successful.

But then lastly, as we have mentioned, the needed resources. What resources are they going to need after they have identified all their risks and made the strategy to actually be able to take the actions that the strategy wants them to take?

Dr. GOSAR. I have gone over to see some of these centers, particularly like East Mesa, where we see the active bombardment. It is pretty amazing to see those attacks coming in, and how they are fronting them. Is Interior big enough to have to be doing that type of qualification?

Ms. CRUZ CAIN. I don't have the answer to that question, but I think all Federal agencies have skills that they need. I know that they have recently hired their cybersecurity specialist to take on, specifically, the oil and gas cybersecurity role so they can start there. And in that strategy and any workforce planning that they do for BSEE specific to oil and gas, they should do their skills need. What do they need to make those strategies successful? Where are they going to get them?

As my colleague mentioned and GAO has mentioned, it is an outstanding challenge in the Federal Government to have a qualified IT workforce. So, there are going to be lots of things that go into this strategy and making it successful. But we don't have any indication that Interior cannot handle it.

Dr. GOSAR. OK.

Inspector General, how does the DOI coordinate with CISA?

Mr. GREENBLATT. That is a very good question. Frankly, I don't know the answer to that. I would have to defer to the agency in that regard.

Dr. GOSAR. Sounds good. Do you have any answer to that, Ms. Cruz Cain?

Ms. CRUZ CAIN. I can tell you from the perspective that their regulatory oversight of the oil and gas, they would coordinate with CISA, being that that is a subsector of the energy sector, and CISA being the—they are not the SRMA for the energy sector, but they would have significant coordination with CISA when it comes to attacks or threat information when it comes to oil and gas infrastructure.

Dr. GOSAR. I am going to end by asking each one of you, what was the question you most wanted to have asked that we feel is very important, and what was its answer?

I will start with you, Inspector General.

Mr. GREENBLATT. I guess I am particularly proud of the team, so how they accomplished the password cracking, I think, is pretty fascinating. If you will just bear with me for a moment, and I can explain it, because it was fascinating to this layman.

But, basically, we took the 85,000 passwords from the Department, which are then made into what is called hash, which is 30 characters to prevent. It is a security mechanism designed to protect those passwords. So, we took the hashes of the 85,000 passwords in the Department, and then the team built a dictionary of 1.5 billion words. This is multiple different languages, government terminology, pop culture references, and passwords that had been hacked in prior hacks that were posted online, put that all together and then did permutations of those, 31 million permutations of each one of the 1.5 billion words, which led to 46 quadrillion potential passwords.

Then they compared those two things. They compared the hashes to the hashes of the 46 quadrillion potential passwords, and compared them. That, in the first 90 minutes, led to 16,000 hits. Those are the easy ones. Those are the password1234's of the world. And then it took a little bit longer for them to get through and get those few thousand remaining ones.

So, that is something that I am particularly proud of the team, in how they conceived of this, and how they pulled it off for less than $15,000.

Dr. GOSAR. Wow, that tells me that there is still hope for me as a Pictionary player.

[Laughter.]

Dr. GOSAR. So, Ms. Cruz Cain, your question?

Ms. CRUZ CAIN. Sure. I think pointing out one of the most critical actions that the Federal Government needs to take to better protect our critical infrastructure, I wanted to make a plug for updating our national infrastructure protection plan. The most recent update has been 2003. We have been in discussions with DHS, and they mentioned that it might be until September 2025 that this plan would be fully updated.

So, it is, in GAO's opinion, very important that we have a timely update to this plan. That is going to allow each of the 16 sectors to update their sector plans, and then those subsectors like oil and

gas and energy to update their specific subsector plans to address cyber risks.

So, from the top down, the most important action we can take is updating that plan, and also filling the vacant cybersecurity director role. The coordination amongst all Federal agencies can really benefit from getting a permanent cyber director, and being able to have the leadership from that office be how each Federal agency approaches their cybersecurity posture.

Dr. GOSAR. That really helps breaking down the silos, as well.

I want to thank the panel for your testimony today, and there will be some written questions for you from Members.

Thank you very much, and we will seat the second panel.

Mr. GREENBLATT. Thank you.

Ms. CRUZ CAIN. Thank you.

[Pause.]

Mr. COLLINS [presiding]. All right, we will get started with the second panel. As you can tell, I am not Mr. Gosar, and I am a freshman. So, I am in the trucking business, this is not what I do for a living. But we are going to go ahead and get started.

I will introduce our second panel of witnesses. And if I mess up your name, I am totally sorry.

We have Mr. Brian Cavanaugh with the Heritage Foundation; Mr. Dean Cheng with the United States Institute of Peace; Ms. Rhea Siers with the Johns Hopkins University; and Dr. Charles Clancy, Sr. with the MITRE Corporation.

Let me remind the witnesses that under Committee Rules, they must limit their oral statements to 5 minutes, but their entire statement will appear in the hearing record.

To begin your testimony, press the "on" button for the microphone.

We use timing lights. When you begin, the light will turn green. At the end of the 5 minutes, your light will turn red, and I will ask you to please complete your statement.

I will also allow all witnesses in this panel to testify before Member questioning.

The Chair now recognizes Mr. Cavanaugh for 5 minutes.

STATEMENT OF BRIAN CAVANAUGH, FELLOW FOR CYBERSECURITY, INTELLIGENCE, AND HOMELAND SECURITY, HERITAGE FOUNDATION, WASHINGTON, DC

Mr. CAVANAUGH. Chairman Collins, Ranking Member Stansbury, and members of the Committee, as the government increasingly relies on interconnected systems, cloud computing, and data-driven decision-making, the very fabric of our national security, economic stability, and public trust hangs in the balance.

Cybersecurity is no longer a mere accessory or an afterthought. It is the cornerstone on which the functioning of our government rests. The landscape of cyber threats is ever-evolving, with the cyber threat posed by China to U.S. infrastructure significant and complex.

First, China has demonstrated a high level of sophistication in cyber capabilities, including cyber espionage.

Secondly, China's large-scale and persistent cyber campaigns target every sector of our critical infrastructure, including

communications, manufacturing, utility, maritime government, and information technology. Volt Typhoon, a PRC-sponsored hacking group, has been specifically targeting sectors that support Pacific operations for the past 2 years.

Finally, China's ability to leverage vast resources, both in terms of human capital and technology such as AI, quantum computing, and essential chip manufacturing, enhanced their cyber capabilities. The scope and efforts and the nature of their capabilities underscore the potential for significant economic and national security consequences, especially as the United States and China lurch toward an impending conflict.

Meanwhile, Russia, Iran, and North Korea have all focused on improving their ability to target critical infrastructure, including underwater cables, water treatment facilities, and operational control technologies, such as those used by offshore energy platforms. Our adversaries believe that demonstrating the ability to compromise such infrastructure can achieve the goal of influencing foreign policy outcomes.

Meanwhile, the U.S. Government approach to cybersecurity has seen its share of challenges, from a lack of prioritization and chasing trends to its inefficient approach to the private sector and lack of accountability for government employees. To overcome these challenges, it is crucial for the government to recognize and prioritize risk as a fundamental component of its cybersecurity strategy. By prioritizing risk, the government can allocate resources effectively, adopt a proactive approach, and ensure accountability in its cybersecurity efforts.

Technology is rapidly developing and evolving. However, this does not mean that the government can erratically chase after the shiny object. Instead, the U.S. Government should find ways to close the detection gap. A recent IBM report highlights the average time to identify and contain a data breach is 287 days, with malware residing on systems for over 180 days.

More policies and more people are themselves not a solution. The model the government has embraced is flat-footed and clumsy. It is an approach that keeps them in a constant state of response and recovery, awaiting alerts from the private sector and then managing damage control messaging afterward. We must become forward-leaning and take meaningful steps towards addressing the risk and mitigating cyber threats to our critical infrastructure. This includes engaging with small businesses that are driving innovation.

Government procurement practices must evolve and foster innovation, especially in the tech sector. Identifying and authenticating users is a fundamental security control, yet, as we just heard, a recent DOI Inspector General report highlighted lackadaisical policies and procedures that enabled the cracking of 21 percent of active user passwords. The report demonstrated that the front door to the Department had been left open by its employees.

From a repercussion perspective, we all have a role to play in vigilance. And just like how resilience starts with the individual, so too does the responsibility of cybersecurity. The government needs to take a firm stance on accountability at the employee level.

U.S. Government employees are central, important, and have immense power. With that must come responsibility.

We must strike a delicate balance between harnessing the power of innovation and securing our digital infrastructure to counter the evolving threat landscape. To do this, Federal departments and agencies must focus on three things: first, they must prioritize infrastructure by risk; second, focus on closing the detection gap; and third, strengthen personal accountability at the employee level.

Thank you for the invitation to testify today, and I look forward to our discussion.

[The prepared statement of Mr. Cavanaugh follows:]

PREPARED STATEMENT OF BRIAN J. CAVANAUGH, VISITING FELLOW FOR CYBERSECURITY, INTELLIGENCE, AND HOMELAND SECURITY, THE HERITAGE FOUNDATION

My name is Brian Cavanaugh. I am a Visiting Fellow for Cybersecurity, Intelligence, and Homeland Security at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Chairman Gosar, Ranking Member Stansbury, and distinguished Members of the Subcommittee:

In today's digital era, where technology pervades every aspect of our lives, the critical importance of cybersecurity for federal departments and agencies cannot be overstated. As our government increasingly relies on interconnected systems, cloud computing, and data-driven decision-making, the very fabric of our national security, economic stability, and public trust hangs in the balance. The threats we face in cyberspace are relentless, sophisticated, and pervasive, posing a significant challenge to the integrity and resilience of our nation.

Cybersecurity is no longer a mere accessory or an afterthought; it is the cornerstone on which the functioning of our government rests. Federal departments and agencies store and handle vast amounts of sensitive and classified information, ranging from critical infrastructure blueprints and defense strategies to personal records and financial data. Any breach or compromise in these systems can have catastrophic consequences, undermining our national security, eroding public confidence, and jeopardizing the very foundations of our democracy.

The interconnectedness of our digital infrastructure means that a single vulnerability can ripple across multiple agencies, putting not only individual departments at risk but the entire government apparatus as well. The consequences extend beyond bureaucratic headaches; they can disrupt essential services, compromise emergency response systems, bring a halt to the economy, and undermine the trust citizens have placed in their government to protect their interests. The threats we face transcend borders and adversaries, requiring a unified and robust approach to fortify our cyber defenses.

Threat Landscape

The landscape of cyber threats is ever evolving, with adversaries constantly honing their tactics and exploiting vulnerabilities. Nation-states, organized crime syndicates, and even lone actors seek to breach our defenses, steal sensitive information, manipulate data, and wreak havoc on our systems. The realm of cybersecurity demands constant vigilance, adaptability, and a proactive stance to anticipate, detect, and respond to these threats in real time. We cannot afford to be reactive; we must be several steps ahead, pre-empting attacks and safeguarding our digital assets with an unwavering commitment.

The People's Republic of China (PRC) is an adversary of the United States. After a decades-long engagement strategy toward China, we find ourselves embroiled in a New Cold War with an even more capable adversary than the Soviet Union. The threat posed by China to U.S. infrastructure in terms of cyber is significant and complex. The Office of the Director of National Intelligence assesses China currently represents the broadest, most active, and persistent cyber espionage threat to the U.S. government and private-sector networks.

China has long been recognized as a major player in the realm of cyber espionage, and its capabilities and activities continue to evolve and expand. The Chinese government and affiliated entities have been attributed to a wide range of cyber activities, including intellectual property theft, espionage, and targeting critical

infrastructure sectors. China's cyber operations pose a serious concern to U.S. infrastructure due to several factors.

First, China has demonstrated a high level of sophistication in its cyber capabilities, employing advanced techniques and tools to breach networks, infiltrate systems, and exfiltrate sensitive data. Their focus on intelligence gathering, particularly related to economic and technological advancements, underscores the potential for significant economic and national security consequences.

Secondly, China's large-scale and persistent cyber campaigns are a cause for alarm. They have been accused of engaging in long-term, strategic cyber operations, targeting a variety of sectors, including government agencies, defense contractors, technology companies, and energy infrastructure. Most recently, Volt Typhoon, a PRC-sponsored hacking group, has been targeting the communications, manufacturing, utility, transportation, construction, maritime, government, information technology and education sectors in the U.S. The breadth and persistence of these campaigns demonstrate a sustained commitment to cyber operations, posing a persistent and evolving threat.

Moreover, China's ability to leverage its vast resources, both in terms of technology and human capital, enhances its cyber capabilities. The country possesses a highly skilled cyber workforce, often supported by state-sponsored initiatives, and has invested heavily in research and development to develop advanced cyber tools and techniques. This combination of talent, resources, and strategic focus amplifies the potential impact of their cyber operations on U.S. infrastructure, especially as the U.S. and China lurch toward an impending conflict over Taiwan and Chairman Xi's vision for a new world order.

While the Office of the Director for National Intelligence noted Russia's cyber operations during the Ukraine war fell short of the pace and impact they had expected, Russia continues to pose cyber threats to the U.S. Putin is particularly focused on improving Russia's ability to target critical infrastructure, including underwater cables and operational technologies. It appears that Russia's belief in demonstrating the ability to compromise such infrastructure during a crisis achieves the goal of influencing foreign policy outcomes.

Iran has demonstrated a willingness to conduct aggressive cyber operations on critical infrastructure, such as water treatment facilities, and their expertise is improving at an alarming pace. While their approach to cyberattacks remains opportunistic, it does not diminish the susceptibility of U.S. critical infrastructure owners, particularly as Tehran believes it must prove to itself that they can push back against the West.

Cyber operations from North Korea have matured and are capable of causing temporary, limited disruptions of some critical infrastructure networks and disrupting business networks in the U.S. The North Korean cyber program emphasizes cybercrime, focusing on financially motivated cyber operations, such as conducting cryptocurrency heists—with on such heist obtaining $625 million. However, cyber actors linked to North Korea have conducted espionage efforts against a range of organizations and continue to focus on cyber espionage geared toward advancing Pyongyang's military programs.

Another threat that often goes unmentioned is transnational organized criminals whose ransomware attacks continue to execute high-impact ransomware attacks, extorting funds, disrupting critical services, and exposing sensitive data. Critical infrastructure such as health care, schools, emergency services, and manufacturing continue to experience attacks aimed at disrupting services. The cost of ransomware attacks is taking its toll on insurance markets, price increases and a hesitation of new insurance carriers in the market are systemic of an out-of-control problem set.

What Is at Risk

The growing trend of digital transformation within federal departments and agencies brings immense benefits but also amplifies the risks. The adoption of emerging technologies such as artificial intelligence, Internet of Things, and cloud computing introduces new attack surfaces and vulnerabilities that must be addressed with utmost urgency. For its part, the Department of the Interior (DOI) houses enormous amounts of data on its digital infrastructure. Whether it relates to sustaining the health and productivity of public lands, the development of U.S. Outer Continental Shelf energy and mineral resources, or enhancing the quality of life of American Indians, Indian tribes, and Alaska Natives, the DOI must safeguard the data, resources, and infrastructure it utilizes to deliver its mission.

As noted in a recent Office of Inspector General (OIG) report, lackadaisical policies and procedures enabled the OIG to hack 21 percent of active user passwords at the DOI using basic and inexpensive means. Of the 18,000-plus accounts hacked, 362 accounts were senior U.S. government employees and 288 accounts had elevated

privileges. Identifying and authenticating users is a fundamental security control. The OIG was able to demonstrate that the front door to the DOI has been left unlocked by its employees.

With over 1,600 structures on the outer continental shelf (OCS) responsible for a significant portion of U.S. domestic oil and gas production and at least 187 offshore wind farms currently being developed for energy production, the Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) must proactively address cybersecurity risks. Modern exploration and production methods are increasingly reliant on remotely connected operational technology, a known vulnerability for cyberattack. A successful cyberattack on offshore energy infrastructure could cause physical, environmental, and economic harm. The effects of a cyberattack could resemble those that occurred in the 2010 Deepwater Horizon disaster or cause market-moving disruptions to energy production or transmission.

In the context of cybersecurity, the interconnected dependencies of critical infrastructure mean that a breach or compromise in one sector can have far-reaching consequences across multiple sectors. The ripple effect of such an attack can cause widespread disruption, economic losses, and potentially endanger public safety. The risk of interconnected dependencies lies in the fact that critical infrastructure sectors are often interdependent and share common underlying systems and technologies. This means that a vulnerability or compromise in one sector can be exploited to gain unauthorized access or disrupt operations in another sector. For instance, a successful cyberattack on a Bureau of Land Management system could potentially impact the operations of a U.S. Geological Survey system or even a Department of Commerce system.

Flaw in Current Approach

The U.S. government's approach to cybersecurity has its flaws, from a lack of prioritization and chasing trends and buzzwords, to its approach to the private sector and its soft response to U.S. government employees entrusted with access to systems and data. Addressing these four areas would represent a marked improvement for the government sector of critical infrastructure.

The lack of prioritization of risk within the U.S. government is a significant hindrance to its efforts in cybersecurity. Effective cybersecurity requires a strategic and risk-based approach, where resources and efforts are allocated based on the level of risk posed by various threats and vulnerabilities. However, when risk is not adequately prioritized, several detrimental consequences arise: resource allocation inefficiency, a reactive approach to threats, inadequate risk assessments, misallocation of efforts, and a lack of accountability.

To overcome these challenges, it is crucial for the U.S. government to prioritize risk as a fundamental component of its cybersecurity strategy. This requires a comprehensive understanding of the threat landscape, thorough risk assessments, and the establishment of clear priorities based on potential impacts and likelihood of occurrence. By prioritizing risk, the government can allocate resources effectively, adopt a proactive approach, and ensure accountability in its cybersecurity efforts, ultimately strengthening the resilience of its systems and protecting national interests.

One sign that the government is misallocating efforts is its willingness to chase after cybersecurity buzzwords or new trends. While it is no secret that technology is rapidly developing and evolving, this does not mean that the U.S. government can erratically chase after the shiny object. Instead, the U.S. government should find ways to close the detection gap, something alluded to by the IBM Security Cost of a Data Breach Report 2022. According to the report, the average time to identify and contain a data breach is 287 days, with malware being undetected for an average of 180 days on systems.

The U.S. government's model for addressing cybersecurity is a flat-footed and clumsy approach that keeps them in a constant state of response and recovery—awaiting alerts from the private sector and then managing messaging. Instead of waiting for the private sector to decide to share information, the U.S. government must become forward leaning, and take meaningful steps toward addressing the risk and mitigating cyber threats to our critical infrastructure. This includes engaging with small businesses and start-ups that are driving innovation in cybersecurity. Procurement practices must evolve and foster innovation, especially in the tech sector. Flexibility in requirements, streamlined and agile procurement-process adoption, and incorporation of pilot programs and testbeds would be a great start.

The risk of interconnected dependencies within critical infrastructure highlights the urgent need for robust cybersecurity measures, including personal accountability. From a repercussion perspective, we all have a role to play in vigilance, and just like how resilience starts with the individual, so, too, does the responsibility of

cybersecurity. The U.S. government needs to take a firm stance on accountability at the employee level. U.S. government employees are central, important, and have immense power. With that must come responsibility—with the expectation that they become lead adopters in proven security methods. Cyber and information technology policies need to be treated as seriously as those regarding the unauthorized disclosure of sensitive information.

A More Resilient Future

To address the threat posed by China and other cyber adversaries, the U.S. government must take proactive measures to enhance cybersecurity efforts. We must strike a delicate balance between harnessing the power of innovation and securing our digital infrastructure, employing robust encryption, multi-factor authentication, and comprehensive threat intelligence to counter the evolving threat landscape. Moreover, to address the critical importance of cybersecurity for federal departments and agencies, we must prioritize infrastructure by risk, focusing on closing the detection gap and strengthening personal accountability.

Investing in research and development of innovative cybersecurity technologies and techniques is crucial to stay ahead of evolving threats. This includes leveraging technologies such as artificial intelligence, machine learning, and behavioral analytics to detect and respond to cyber threats in real time. While investing in cutting-edge technologies and cultivating a highly skilled cybersecurity workforce, we must promote a culture of cybersecurity awareness and resilience at all levels of government.

Robust cybersecurity practices, threat intelligence sharing, investment in defense technologies, and collaboration with international partners are vital components of a comprehensive strategy to mitigate the risks posed by China's cyber activities to U.S. infrastructure.

The value of cybersecurity for federal departments and agencies cannot be underestimated. It is the shield that safeguards our nation's secrets, ensures the smooth functioning of our government, and preserves the trust and confidence of the American people. We must rise to the challenges that lie ahead, fortifying our defenses, embracing innovation securely, and forging a united front against the ever-present and evolving threats in cyberspace. Our future, our security, and the integrity of our democracy depend on it.

QUESTIONS SUBMITTED FOR THE RECORD TO BRIAN CAVANAUGH, FELLOW FOR CYBERSECURITY, INTELLIGENCE, AND HOMELAND SECURITY, THE HERITAGE FOUNDATION

Questions Submitted by Representative Gosar

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

Answer. 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.

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

Answer. 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.

Mr. COLLINS. I thank the witness there for his testimony, and the Chair now recognizes Mr. Cheng for 5 minutes.

STATEMENT OF DEAN CHENG, SENIOR ADVISOR, CHINA PROGRAM, UNITED STATES INSTITUTE OF PEACE, WASHINGTON, DC

Mr. CHENG. Good afternoon, Chairperson Collins, Ranking Member Stansbury, and other members of the Committee. My name is Dean Cheng. I am a Senior Advisor with the U.S. Institute of Peace, but my comments this afternoon are my own. My comments this afternoon are intended to provide some context for better understanding potential Chinese interest in cyber penetrating and attacking the Department of the Interior.

Broadly speaking, the PRC employs cyber and network penetration operations to gather intelligence, identify vulnerabilities, map out networks, and otherwise prepare to establish information dominance. The Department of the Interior's areas of responsibility span a range of issues that are of particular interest to the People's Republic of China, including mineral and oil leasing, infrastructure management, and relations with key Pacific Island nations.

The Department is, therefore, at great risk to Chinese cyber penetration and attacks.

From the Chinese perspective, what matters is information. Because the CCP sees the world today as living in the information age, information has become the key currency of power, both at the national and international level. Information feeds and supports all aspects of comprehensive national power and, therefore, all elements of information—military, economic, political, technical—contribute to a nation's power and, conversely, are potential elements that should be hacked because they are also elements of vulnerability.

The overall concept underlying Chinese activities is information dominance. It is [Speaking foreign language]: the ability to exploit information at times and places of one's own choosing, the ability to move and analyze information more rapidly and more accurately than competitors, and denying an adversary those same capacities.

The PRC and, in particular, the Chinese Communist Party, sees establishing information dominance as central to regime survival. In this regard, Chinese cyber operations are undertaken for a variety of purposes. This includes intelligence gathering.

And let me emphasize here this is not simply military and defense and intelligence community-related information. It also includes business activities in the private sector. And we have seen Chinese Government entities operate against private-sector entities. It includes mapping out networks. It includes political military targeting, but also industrial espionage. For example, we have heard reference to Volt Typhoon, which targeted U.S. infrastructure. We have also seen Chinese entities hack cloud storage systems.

As well as political intelligence gathering, notably here is the case of the OPM hack from several years ago. It is interesting to note, I suggest, that OPM servers were housed bureaucratically within the Department of the Interior. This goes to the broader aspect of Department of the Interior responsibilities, which includes management of public lands, including drilling and mining, fisheries, offshore public lands, offshore drilling operations. All of these are things that, from the CCP's perspective, need to be mapped, monitored, and potentially hacked.

For example, USGS is responsible for creating a critical minerals list. The latest version was undertaken in 2022. What has not yet occurred is a survey of critical minerals on public lands. USGS is undertaking such actions. From the PRC's perspective, not surprisingly, they would love to know the results of a survey of U.S. public lands and what critical minerals—including, for example, rare earths—might reside. And from there, what companies might be contracted to extract that, and what would be the infrastructure that would be built out to move ores to processing facilities.

Finally, it is important to note here that the Department of the Interior, through the Bureau of Insular Affairs, has responsibility for interactions with a number of Central Pacific Island countries, including the Republic of the Marshall Islands, Federated States of Micronesia, and Republic of Palau. Your counterparts on the Armed Services Committee can certainly go into significant detail on the importance of these islands for U.S. operations.

Federated States of Micronesia, for example, surrounds the island of Guam, one of our central geographic locations in the

Central Pacific. But the island of Kwajalein in the Republic of the Marshall Islands is a key part of our space and missile defense capabilities. So, with that in mind, I would suggest that it is, above all, important to recognize that, while the Department of the Interior's focus—by its title, of course—is domestic affairs, because of the various bureaucratic responsibilities, it is absolutely a high-priority target for the PRC.

Thank you very much for the opportunity to testify today.

[The prepared statement of Mr. Cheng follows:]

PREPARED STATEMENT OF DEAN CHENG, SENIOR ADVISOR, UNITED STATES INSTITUTE OF PEACE

My name is Dean Cheng. I am a non-resident Senior Fellow at the Potomac Institute for Policy Studies, and a Senior Adviser with the United States Institute of Peace. The views I express in this testimony are my own, and should not be construed as representing any official position of either the Potomac Institute or the United States Institute of Peace.

Chinese View of Information

Over the past half century, the leadership of the People's Republic of China (PRC) has increasingly emphasized the importance of information as it relates to national economic development and national security. Beginning in the 1970s, the proliferation of microelectronics, computers, and telecommunications technology has accelerated the ability to gather, store, manage, and transmit information. From the perspective of the Chinese Communist Party (CCP) leadership, information technology, including computers and telecommunications systems, have permeated all aspects of society and economies and become an integral part of a nation's infrastructure.[1] Chinese analysts have dubbed this process "informationization (*xinxihua*)," and see the world as shifting from the Industrial Age to the Information Age.

From the Chinese perspective,

> Informationization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard.[2]

In the face of this broad trend of economic, political, and social informationization, Chinese analysts have concluded that national economic development requires greater integration of information technologies into all aspects of the economy, while defending against threats to PRC national interests and security also must become informationized.

Economic development in the Information Age is built upon accessing, exploiting as well as analyzing and transmitting information. While manufacturing, transportation, and other traditional industries remain an essential part of a nation's strength, even those are increasingly digitized, whether in terms of the designs that they are producing or the electronic controls that govern the manufacturing equipment and power networks that sustain them. Information technology therefore permeates all aspects of the nation's economy, indirectly as well as directly.

The spread of information technology similarly means that potential adversaries have unprecedented access to each others' national economy, as well as the broader population and the top decision-makers. Just as the bomber and ICBM allows an opponent to directly strike a nation without having to first break through ground or naval defenses, information technology similarly outflanks traditional military forces. The proliferation of information technology into society and economics makes a nation broadly vulnerable to a range of new pressures and threats.

These threats extend beyond information networks (e.g., vulnerability to denial-of-service attacks) and component computers (e.g., computer viruses, malware).

---

[1] TAN Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology* (#5, 2009), p. 72.

[2] State Council Information Office, Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans (October 18, 2002), http://www.cia.org.cn/information/information_01_xxhgh_3.htm

Instead, the very information itself can constitute a threat, if, for example, its content erodes the morale of key decision-makers, popular support for a conflict, or the will of the military to fight. Consequently, China's interpretation of its national interests has expanded, in step with the expanding impact of information writ large on China.

More recent advances in information technology, including artificial intelligence and machine learning, the Internet of Things (IoT), big data and cloud computing, have further underscored the growing reach and capability of those able to exploit information networks through network warfare and cyber operations. These advances also affect both economic and security calculations.

PRC Employment of Network and Cyber Operations

Because of the growth of interconnectivity, the CCP is able to exploit its network and cyber capabilities for both economic and national security gains.

In the military and security context, PRC network and cyber operations are an integral part of intelligence gathering, just as they are for most other nations, including the United States. Undertaking such efforts is an essential part of the PLA's broader efforts to establish "information dominance," which PLA analysts view as an essential prerequisite to fighting and winning future conflicts. Because of the need to be able to rapidly exploit information more effectively than an adversary in wartime, it is necessary to undertake cyber and electronic reconnaissance of adversaries in peacetime. This includes not only amassing electronic signatures of enemy communications and weapons systems, but also surveying their networks, understanding their organization, and constructing the ability to attack those systems and defend against counter-attacks.

To this end, the Chinese People's Liberation Army (PLA) created a new service, the PLA Strategic Support Force (PLASSF), in the massive restructuring and reorganization announced on December 31, 2015. The PLASSF brings together China's electronic warfare (EW), network and cyber warfare, and space warfare forces into a single entity.[3] As all of these elements are linked to the gathering, exploitation, and transmission of information, the PLASSF is very much China's "information warfare force."

Of special importance here is the Network Systems Department (NSD) of the PLASSF. This component of the PLASSF incorporates element of what had previously been part of the PLA General Staff Department's 3rd Department, which had been responsible for a variety of cyber espionage activities. This includes the infamous Unit 61398, named in a 2013 Mandiant report and the first PLA unit publicly identified as a hacker force.[4]

The existence of Unit 61398 as a PLA unit also highlights a fundamental difference between Chinese and Western execution of cyber *economic* espionage. There are few reports of Western intelligence or military forces being tasked with economic espionage. By contrast, the PLA is part of a vast network of Chinese cyber forces that undertake economic as well as national security espionage. Five members of Unit 61398, for example, were indicted by the US Department of Justice for various cyber economic espionage activities over the period 2006–2014, including attacks on Alcoa, Allegheny Technologies Inc., and Westinghouse.[5]

As the Office of the Director of National Intelligence noted in their 2023 threat assessment, "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."[6] Similarly, FBI Director Christopher Wray observed in 2020 that Chinese espionage efforts are

> not just targeting defense sector companies. The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind turbines to high-end medical devices. And they're not just targeting innovation and R&D. They're going after cost and pricing

[3] For a more extensive discussion of the PLA SSF, please see John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, INSS China Strategic Perspectives #13 (Washington, DC: National Defense University, October 2018).

[4] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (February 2013) https://nsarchive.gwu.edu/document/21484-document-83

[5] Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," (May 19, 2014) https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[6] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community 2023* (Washington, DC: ODNI, February 2023), p. 10, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

information, internal strategy documents, bulk PII—anything that can give them a competitive advantage.[7]

These efforts in turn incorporate both military and civilian, governmental and non-governmental elements, such that they outnumber the FBI's cyber staff by 50 to 1.[8]

Targeting the U.S. Department of the Interior for Network Attacks

Given the roles and responsibilities of the United States Department of the Interior (DOI), at least some of this massive array of cyber and network attackers are likely targeted at the DOI. For example, the DOI has oversight of US public lands, including drilling and mining rights. Within this purview is oversight of development of leasable minerals, such as oil, natural gas, coal, phosphate, potassium, and sodium, as well as locatable (or hardrock) minerals, such as gold, silver, copper, and gemstones.[9] Such resources are clearly of economic importance.

As important, the United States government has identified an array of 35 critical minerals vital to national economic security, including cobalt, fluorspar, and niobium.[10] Until recently, there have been no surveys of public lands to determine how much, if any, of these critical minerals might be present. Under President Biden's Executive Order 14017, however, the DOI is encouraged to have the US Geological Survey, along with the Bureau of Land Management and the Department of Agriculture's US Forest Service, begin such surveys. For the PRC, accessing the results would provide useful insight into American reserves and potential production capacity for these critical minerals.

Similarly, the DOI has oversight over leasing of both onshore and offshore sites for oil drilling. Knowing the location of potential new energy reserves, including offshore sites, would be strategically valuable, as it could help the Chinese determine which companies, in turn, to monitor and even penetrate through cyber and other means. As important, sites that are tapped will require the construction of substantial networks of pipelines and other infrastructure to extract and move those resources. As a 2021 Joint Cybersecurity Advisory, coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), noted, state-sponsored Chinese actors have repeatedly targeted U.S. oil and natural gas (ONG) pipeline companies in the past.[11]

ONG companies may have their operating software attacked. Alternatively, as with the May 2021 Colonial Pipeline incident, the companies may be targeted for ransomware attacks, where the data is made inaccessible (but is not destroyed). Although Colonial Pipeline's networks moved oil from refineries to customers, other parts of the overall energy supply chain, including from fields to refineries, could also be targeted.[12]

Finally, as the DOI is part of the overall US government bureaucracy, it offers potential access to a range of systems not necessarily related to its purview. The DOI, for example, housed the data center for the Office of Personnel Management (OPM). This was the center that was accessed when OPM was hacked in 2015, exposing the records of some 4 million current and former federal employees. Notably, hearings into the hack indicated that DOI had some 3000 "critical and high risk vulnerabilities."[13]

---

[7] Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat," Remarks at the Department of Justice China Initiative Conference, Center for Strategic and International Studies (February 6, 2020) https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

[8] Lauren Feiner, "Chinese Hackers Outnumber FBI Cyber Staff by 50 to 1, Bureau Director Says," CNBC (April 28, 2023) https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html

[9] Congressional Research Service, *Federal Lands and Related Resources: Overview and Selected Issues for the 118th Congress*, CRS Report R43429 (February 24, 2023) https://crsreports.congress.gov/product/pdf/R/R43429/42

[10] US Geological Survey Communications and Publishing, "US Geological Survey Releases 2022 List of Critical Minerals," (February 22, 2022) https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals

[11] "Chinese Gas Pipeline Intrusion Campaign, 2011–2013" (July 21, 2021) https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

[12] "About Shell Pipeline," https://www.shell.us/business-customers/shell-pipeline/about-shell-pipeline.html

[13] "Thousands of Cybersecurity Vulnerabilities Uncovered at Interior Department," FedScoop (July 15, 2015) https://fedscoop.com/after-opm-hack-interior-cybersecurity-audit-finds-thousands-of-critical-vulnerabilities/

Oversight of Pacific Island States

Another reason for concern about Chinese network attacks and cyber intrusions into the Department of the Interior is that the Department is responsible for overseeing US relations with several of the microstates of the central Pacific. One example is the Republic of the Marshall Islands (RMI), an independent nation tied to the United States by a Compact of Free Association. It comprises 5 islands and 29 atolls, with a population of some 58,000 people. While only possessing some 70 square miles of dry land, these islands and atolls are spread across 750,000 square miles of central Pacific territory.[14] As such, they straddle waters that link the American west coast with the east Asian littoral.

This strategic position was made clear during the Second World War, when U.S. forces "island hopped" through the Marshall islands, on their way to the Marianas and eventually to Japan. Indeed, the battles for Kwajalein and Eniwetok provided invaluable experience for later battles on Guam, Iwo Jima, and Okinawa.

In the wake of the Second World War, the United States was granted trusteeship over various central Pacific territories, including the Marshall Islands. The Republic of the Marshall Islands (RMI) gained its independence in 1986. Under the original and subsequently amended Compact of Free Association (CFA), RMI citizens can work, live, and study in the United States, as non-immigrants.[15] As of 2019, there were some 27,000 Marshallese in the United States, a substantial portion of the RMI population.[16]

In addition, under the terms of the CFA, the United States provides RMI with economic support and aid. The United States provides RMI with some $70 million annually in various forms. This includes a jointly managed trust fund. US government agencies and offices, such as the Federal Communications Commission and US Postal Service, also provide services to the Marshall Islands. This aid is scheduled to end when the current amended Compact expires in 2023.

In exchange, the United States is granted exclusive and full authority to RMI lands and waterways for security and defense purposes, although RMI is free to conduct its own foreign relations. A key element of both economic and security ties is the leasing of land and lagoon space to the U.S. Army on Kwajalein atoll under the Military Use and Operating Rights Agreement. The missile and space facilities there are the second largest employer in the RMI.[17]

RMI's Role in American Defense Efforts

Throughout the post-war period, the Marshall Islands have played an important role in America's defense, especially in the context of nuclear deterrence.

In the immediate post-war period, the United States conducted an array of nuclear tests in the Marshall Islands. The 67 nuclear tests conducted there between 1946 and 1958 included Castle Bravo, the largest American nuclear test involving a 15 megaton device.[18] It is worth noting that this test was nonetheless dwarfed by four Soviet tests, which ranged from 20–50 megatons.

With the Limited Test Ban Treaty of 1963, which effectively banned above-ground nuclear tests, the islands have no longer been rocked by nuclear explosions. RMI has continued to play an important role, however, in maintaining America's nuclear deterrent posture. Especially important has been the role of Kwajalein and the Ronald Reagan Ballistic Missile Defense Test Site (RTS).

The RTS provides key support to US defense efforts in several ways. The credibility of the American nuclear deterrent is sustained through a program of regular tests of Minuteman III missiles. As recently as August 2021, the US fired a Minuteman III with a Hi Fidelity Joint Test Assembly re-entry vehicle onboard towards Kwajalein.[19] Such tests demonstrate to all observers, including America's adversaries, the continuing functionality and reliability of the American nuclear

---

[14] 14 U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[15] U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[16] Susanne Rust, "They Came Here After the U.S. Irradiated Their Islands. Now They Face an Uncertain Future," *Los Angeles Times* (December 31, 2019) https://www.latimes.com/world-nation/story/2019-12-31/marshall-islands-uncertain-future-us-marshallese-spokane

[17] U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Marshall Islands," (July 15, 2018) https://www.state.gov/u-s-relations-with-marshall-islands/

[18] Lawrence Livermore National Laboratories, "Brief History of Nuclear Testing in the Marshall Islands," (July 28, 2021) https://marshallislands.llnl.gov/testhistory.php

[19] Air Force Global Strike Command Public Affairs, "Minuteman III Test Launch Showcases Readiness of U.S. Nuclear Forces' Safe, Effective Deterrent," (August 11, 2021) https://www.stratcom.mil/Media/News/News-Article-View/Article/2727368/minuteman-iii-test-launch-showcases-readiness-of-us-nuclear-forces-safe-effecti/

deterrent. This is becoming an ever more pressing issue due to the aging of the Minuteman III, first introduced in the 1960s.

The fact that these test shots cover some 4200 miles further enhances the credibility of the American deterrent. Russian ICBM tests from the Plesetsk Kosmodrome to the Kura test range in Kamchatka cover some 3800 miles.[20] Longer test flights provide more opportunity for measurements of flight characteristics.

Moreover, given the size of the Kwajalein lagoon (which is one of the largest in the world at over 600 square miles), one can target warheads and dummy payloads into it, and thereby prevent their recovery by other actors. In 2016, Chinese sailors seized an American unmanned underwater vehicle (UUV) from international waters.[21] There should be little doubt that the Chinese, among others, would very much like an opportunity to examine a dummy US nuclear warhead.

The facilities at Kwajalein also support missile defense efforts. The various radars and facilities provide American missile defense planners and engineers with data to help improve missile interception capability. This is of growing concern, as both Russia and China modernize their own nuclear arsenals.

Nor are missile defenses only relevant to the nuclear side of the deterrence equation. The PRC, for example, has deployed anti-ship ballistic missiles, such as the DF-21 and DF-26. Both of these are clearly intended to neutralize American aircraft carriers and other maritime strategic platforms. Missile defenses would degrade Chinese confidence that they can sink or damage American carriers, which in turn would help deter China from using force against various neighbors, from Japan to Taiwan to the Philippines.

In November 2020, an American SM-3 Block IIA missile successfully intercepted an ICBM-type missile, launched from Kwajalein.[22] This was the first time that the SM-3, which can be deployed aboard an AEGIS-equipped destroyer or cruiser, had destroyed such a target.[23] This radically improves not only American deterrence, but that of any allied nation that has comparable AEGIS-type systems in their fleet. The SM-3 is already part of the Phased Adaptive Approach for NATO defense against Russian missile threats. It is deployed in the ground-based site in Rumania, and will be deployed to the site currently under construction in Poland. Meanwhile, Japan has chosen to rely on its fleet of AEGIS destroyers to provide missile defense for the Home Islands, against North Korean and Chinese threats. The success of the SM-3 Block IIA test means that this key US ally will be more secure in coming years. The facilities in the Marshall Islands have played a key role in improving American and allied security.

Finally, the facilities in the RMI, including on Kwajalein, play a central role in space surveillance. The United States Space Force currently tracks some 26,000 objects in space. Because of the high speed of objects in orbit, even a bolt or a screw can do enormous damage to the International Space Station or an orbiting satellite. The recently built Space Fence on Kwajalein provides the Space Force with the ability to monitor objects as small as a marble.[24]

This capability is of growing importance as America's competitors and adversaries develop ever more capable space systems, many of which are believed to be anti-satellite systems. The Russians, for example, have deployed sub-satellites from larger satellites, much like submunitions from a dispenser. In 2017, Kosmos-2519 launched Kosmos-2521, a sub-satellite while in orbit. Kosmos-2521 subsequently launched a sub-satellite of its own, Kosmos-2523. Both Kosmos-2519 and Kosmos-2521 maneuvered in orbit.[25] Meanwhile, China's new reusable space plane apparently released an object while in orbit, and engaged in rendezvous and proximity

---

[20] Joe Saballa, "Russia to Test Launch Advanced intercontinental Ballistic Missile," *Defense Post* (May 5, 2021) https://www.thedefensepost.com/2021/05/05/russia-to-test-launch-ballistic-missile/

[21] Terri Moon Cronk, "Chinese Seize U.S. Navy Underwater Drone in South China Sea," *DOD News* (December 16, 2016) https://www.defense.gov/News/News-Stories/Article/Article/1032823/chinese-seize-us-navy-underwater-drone-in-south-china-sea/

[22] The Department of Defense, "U.S. Successfully Conducts SM-3 Block IIA Intercept Test Against an Intercontinental Ballistic Missile Target," (November 17, 2020) https://www.defense.gov/News/Releases/Release/Article/2417334/us-successfully-conducts-sm-3-block-iia-intercept-test-against-an-intercontinen/

[23] The War Zone Staff, "The Navy Has Finally Proven It Can Shoot Down an Intercontinental Ballistic Missile," *The Drive* (November 17, 2020) https://www.thedrive.com/the-war-zone/37685/the-navy-has-finally-proven-it-can-shoot-down-an-intercontinental-ballistic-missile

[24] Sandra Erwin, "Space Fence Surveillance Radar Site Declared Operational," *Space News* (March 28, 2020) https://spacenews.com/space-fence-surveillance-radar-site-declared-operational/

[25] Gunter D. Krebs, "Kosmos-2519/Kosmos-2521/Kosmos-2523," *Gunter's Space Page* Retrieved October 17, 2021, https://space.skyrocket.de/doc_sdat/kosmos-2519.htm

operations (RPO) with at least one other object over the past year.[26] All of these actions are difficult to track, especially while also maintaining situational awareness over 26,000 pieces of other debris. Russia has since launched other satellites that have behaved in a similar fashion, launching their own sub-satellites.[27] US space surveillance capabilities must maintain watch over all these objects, if America's own satellites are to be preserved.

The ground-based Space Fence radar on Kwajalein is an essential part of the American space surveillance network. It plays a key role in helping the U.S. detect and track potential threats to its satellites, including its missile early warning, strategic communications, and reconnaissance platforms.

In addition to RMI, the United States has comparable special relationships with the Federated States of Micronesia, and the Republic of Palau. Relations with both of these states are also overseen by the DOI. Both of these states are slated for additional US military construction, but have also been courted by Beijing.[28]

For the PRC, which has been seeking inroads into the central Pacific and to build expanded ties to the various states, gaining insider knowledge of American positions, aid packages, and general policy toward those states would be of enormous strategic advantage. Moreover, as both RMI and the Republic of Palau maintain ties with Taiwan, rather than the PRC, Beijing is intensely interested in gaining any leverage it can to shift their diplomatic alignment.

QUESTIONS SUBMITTED FOR THE RECORD TO DEAN CHENG, SENIOR ADVISOR, CHINA PROGRAM, UNITED STATES INSTITUTE OF PEACE

Questions Submitted by Representative Gosar

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

Answer. There may be issues of reallocation of money within a budget, and whether Congressional authorizations allow such reallocations. For example, it may be that money cannot be shifted from, say, Bureau of Land Management to Department of the Interior (DOI) information services without prior authorization.

More importantly, however, is even within the DOI's information services budget, how money is programmed. More money spent on cybersecurity will almost certainly mean less money spent on some other aspect of information management and information services within the DOI. It may mean fewer updates of the web-site, or a lagging purchase of new computers. So long as the information technology/information services budget is (relatively) fixed, additional tasks will be a matter of "robbing Peter to pay Paul."

One consideration, however, may be to determine better metrics of information security, in order to assess the effectiveness of dollars spent on information security. How well is DOI currently doing in terms of securing its information systems?

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

Answer. Measuring effectiveness and determining efficiency of cyber security is extremely difficult to measure, because it is essentially assessing dogs that do not bark. For example, how does one assess effectiveness of deterrence measures, other than "no war occurred"?

Assessing cybersecurity initiative measure effectiveness might be facilitated by conducting "tiger team" or "red team" attacks. Indeed, this might provide USCYBERCOM with an opportunity to engage in cross-departmental cooperation by staging "attacks" against DOI. Alternatively, asking USCYBERCOM to help assess threats and security capacity of DOI's information security would potentially help both departments improve their level of operation.

---

[26] Andrew Jones, "China's Mysterious Spaceplane Releases Object into Orbit," *Space News* (November 2, 2022) https://spacenews.com/chinas-mystery-spaceplane-releases-object-into-orbit/, and Joseph Trevithick, "Chinese Spaceplane Docked with Another Object Multiple Times Data Indicates," *The Drive* (May 9, 2023) https://www.thedrive.com/the-war-zone/chinese-spaceplane-docked-with-another-object-multiple-times-data-indicates

[27] Neel V. Patel, "The U.S. Says Russia Just Tested an 'Anti-Satellite Weapon' in Orbit," *Technology Review* (July 23, 2020) https://www.technologyreview.com/2020/07/23/1005568/us-space-command-russia-test-anti-satellite-weapon-orbit-kosmos-2543/

[28] Kirsty Needham, "Pacific Islands a Key U.S. Military Buffer to China's Ambitions, Report Says," Reuters (September 20, 2022) https://www.reuters.com/world/asia-pacific/pacific-islands-key-us-military-buffer-chinas-ambitions-report-2022-09-20/

Questions Submitted by Representative Grijalva

Question 1. In May 2023, a Chinese Government hacking group successfully launched a malware attack on telecommunications systems in Guam and other parts of the United States. What were the consequences of this breach and what can we learn from it to strengthen our cybersecurity posture, especially in the Indo-Pacific region.

Answer. I believe several lessons have emerged.

- One of the most basic is that the same cybersecurity threat groups are often given different names by different cyber-security firms, making it harder to assess how extensively the threat entity has operated, where it has performed prior penetrations, etc. The group "Volt Typhoon" is also known as "Bronze Silhouette" among other names. Encouraging cyber-security firms to not only share data (they often do), but to either use the same nomenclature would improve overall security by facilitating a common understanding of the threat.
- The threat is constantly shifting. "Volt Typhoon" attacks do not require downloading malware, but exploit existing lines of attack. As important, it apparently involves exploiting cyber security firms as an attack pathway.
- There should be little question that the PRC will engage in disruptive attacks against critical infrastructure in time of conflict, and most likely in time of crisis. This is consistent with known People's Liberation Army (PLA) writings, and suggests that policies and courses of action predicated on the assumption that the PRC and PLA will ***not*** conduct such attacks are badly mistaken. It is therefore essential to plan now for both mitigation and response strategies in the likely event of such attacks and ensuing disruptions.

Mr. COLLINS. Thank you, Mr. Cheng. The Chair now recognizes Ms. Siers for 5 minutes.

STATEMENT OF RHEA SIERS, SENIOR ADVISOR (CYBER RISK), TENEO, WASHINGTON, DC

Ms. SIERS. Mr. Collins, Ranking Member Stansbury, and Committee members, thank you for the opportunity to discuss cybersecurity challenges. My name is Rhea Siers, and I have worked over 30 years in both the government and private sectors, witnessing the cyber threat to our national security and economic well-being growing exponentially.

I will use a practitioner's approach, as someone who sees the daily realities of defending our networks and responding to cyber incidents.

The cyber playing field has evolved. Initially, cyber was the primary domain of state actors. But to understand the totality of the cyber threat challenge, we must acknowledge the role and activities of non-state actors, as well. Computer technology is now easily available to non-state actors, such as organized criminals and hacktivists. They procure cyber tools from state sponsors or the cybercrime underground: a robust, full-service operation.

Years ago, the hallmark of state cyber actors was their persistence, tenacity, innovation, and exploitation of human error. Now, some of these non-state actors are displaying similar performance and tactics.

Of great concern is the increasing impact of actors that self-identify as non-state actors, but are controlled or resourced by states. These groups often employ cybercrime tactics, but their objectives align with their sponsor's strategy. These groups are supported by our traditional adversaries, such as Russia and

China, and our newer cyber adversaries, such as North Korea and Iran.

Two examples: The Russian Sandworm group linked to Russian military intelligence is a very sophisticated cyber presence. In 2017, they caused a shutdown at the global maritime giant, Maersk, leading to significant monetary losses and disruption to the worldwide supply chain. The Lazarus Group is a North Korean-sponsored hacking syndicate. They have pursued numerous attacks on an array of sectors worldwide. Their objective is supplying the North Korean regime with funds with the dual purpose of disruption in world markets and financial transactions. Their cyber mentor in building capabilities, of course, was China.

What are our adversaries after? They want access to confidential data. Thus, their efforts to penetrate government and private sector networks.

This isn't just spy versus spy. The government holds a great deal of sensitive data that can give adversaries a very good idea of our security vulnerabilities, from the financial sector to oil pipelines.

This is not just about data. We see more threats against industrial control systems, the instrumentation that operates the industrial processes, from manufacturing plants to power grids. There is potential for operational disruption and damage. One recent example: the Chinese government-supported hackers who targeted multiple U.S. oil and gas pipelines over the past decade, mapping the industrial controls for potential future operations.

Future cyber challenges are also emerging, from efforts to infiltrate the supply chain of information technology, such as the Russian SolarWinds operation, to the potential to alter algorithms that are increasingly running our operational technology.

So, how do we defend against traditional and newer adversaries with the finite resources we have in the public and private sectors?

What we don't want is something I call Chicken Little cybersecurity. Recall the story of Chicken Little. He gets hit in the head by some acorns, and he decides the sky is falling. Every day we are hit with a barrage of bad cyber acorns, threats, malicious software, data breaches. To keep the sky from falling, you must assess the specific risks to your organization, public or private. Your cyber defense ultimately depends on your ability to do so.

The response to state and non-state cyber threats is to focus and strategize; find the key vulnerabilities and risks; realize that no government agency or private company is an island unto itself. We cannot claim that we can repel any cyber attack or neutralize all our cyber adversaries. Instead, we must aim for cyber resilience, collaborative preparation, and agile response that doesn't stop at the public-private boundary.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Siers follows:]

PREPARED STATEMENT OF RHEA D. SIERS, SENIOR ADVISER, TENEO

Subcommittee Chairman Gosar, Ranking Member Stansbury and distinguished Members of the Subcommittee, thank you for the opportunity to appear before to discuss the cyber threats to our national security from State adversaries and their proxies. My name is Rhea Siers and I have spent over thirty years in this area, both in government and in the private sector and have watched the cyber threat to our national and economic well-being grow exponentially. I approach this topic from a practitioner's standpoint, as someone who has seen on a daily basis the challenges of protecting our nation's critical infrastructure and government and business operations from the inside and outside. Those challenges are the direct result of our digital world given the vast amount of personal, proprietary and operational information flowing through all our networks. Frankly, it is a treasure trove of information and potential disruption available to our adversaries worldwide.

Prior to my current position as a Senior Advisory on Cyber Risk to Teneo, I served in a variety of senior operational positions at the National Security Agency including Deputy Assistant Director for policy; since my retirement from the US Government Senior Executive Service, I have worked as an attorney and advisor on Cyber Incident Response, and as a Senior Cyber Defense Strategy Executive at Bank of America. I am also on the faculties of George Washington and Johns Hopkins Universities where I have developed and taught courses on Cyber Threats, Strategy and Policy for the past fifteen years. My approach today is a pragmatic one—not just discussing the changes in cyber threats but the importance of planning for emerging threats as technology continues to develop so rapidly. My advisory focus is not just the response to crisis cyber situations but the very critical need for advance planning to ensure resilience to attacks, disruption or even worse, destruction of data and operational technology in our networks. I'm all about demystifying cybersecurity and helping my students and clients ask the right questions about their cyber defense in the wake of daily hostile cyber activity.

In my testimony today, I will discuss the following issues relating to state and other cyber threats to our national security and economic stability:

1. Cyber Actors: The Playing Field Evolves
2. Potential Implications: Who is Hacking and What Are Their Objectives?
3. Responding to the Cyber Threat Challenge: Avoiding the "Chicken Little Cybersecurity" Syndrome

1. The Cyber Playing Field Has Changed:

I admit, given my background, taking a bit of a long and evolutionary view of cyber threats. When I started in this field, cyber was very much the primary domain of state actors—intelligence services and the military held the keys to cyber operations and were the most successful adversaries. They dominated the activity, the attacks, the use of cyber to penetrate networks to gain a national security advantage, to collect intelligence and to seek economic advantage. They possessed the technological resources to conduct electronic surveillance and warfare both domestically and overseas. While that's certainly still very true today, the cyber playing field has leveled out a bit and the attribution—the "who dunnit" of cyber operations—has become a bit murkier.

If we want to understand the totality of the cyber threat challenge, we must acknowledge the role of non-state actors. Significant technological advances actually make computer network resources more widely available. Thus, nonstate actors, such as organized criminals, and 'hacktivists' are now taking full advantage of available cyber capabilities. Certain tools are readily available—either from state sponsors or the cybercrime underground, which features a full service, one-stop shopping for tools such as ransomware—that hold data hostage until a ransom is paid.

There is a growing and increasingly impactful category of actors that self-identify as nonstate actors but are controlled or resourced by states. They often employ cybercrime tactics and techniques, but their objectives align with the State's strategy against adversaries. One can call them a blended or hybrid threat, but ultimately many are state-sponsored and supported. Of even greater concern, the nonstate cyber actors are improving all the time. Years ago, the hallmark of state cyber actors was their persistence, tenacity, great use of technology and exploitation of human error. Now these state proxies are displaying the same persistence and use of more advanced cyber tools and techniques. These proxies allow states to build further capacity and also aid in the state's efforts to hide some of its cyber activity.

Just a few recent examples illustrate the challenge of state sponsored cyber groups:

- The Russian Sandworm group, which is linked to Russian military intelligence, has been quite active. Sandworm is a sophisticated cyber presence and is believed to have conducted the 2015 BlackEnergy cyber attack against Ukraine's power grid as well as the 2017 attack on the global maritime giant, Maersk. Maersk's booking system and loading systems were impacted. Maersk and all its global shipping were shut down resulting in significant monetary losses and great impact on the worldwide supply chain. Sandworm has been active against Ukraine recently as well in an effort to damage the industrial control systems that run high voltage substations there—i.e. shut off power.
- The Lazarus Group is a North Korean sponsored hacking syndicate—they are known to have been involved in the attack on Sony Motion Picture Entertainment here in the US and have pursued attacks on the financial and pharmaceutical sectors worldwide. While their key objective is supplying the North Korean regime with funds, they also often have a dual purpose of disruption in world markets and financial transactions.
- More recently, the Department of Justice indicted a number of Iranians affiliated with the Iranian Islamic Revolutionary Guard Corps (IRGC) for ransomware activities "threatening the physical security and economy of the United States". These activities included the targeting of critical infrastructure with ransomware.

As if the playing field wasn't complicated enough—there are no shortage of targets for malevolent cyber actors. While certainly government agencies at all levels are in the crosshairs of hostile cyber states, the private sector in the US controls about 90% of cyberspace; of even greater concern is the protection of our critical infrastructure. For example, the Cybersecurity and Infrastructure Security Agency (CISA) notes that "more than 80% of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses and other sources of energy that are integral to growth and production across the nation".

2. Who Is Hacking and Why? Potential Implications

To understand impact on the natural resources sector, it is important to understand three different and multiple cyberattack objectives—i.e., what benefits the cyber attacker is expecting to gain from a successful intrusion or attack.

All of these objectives operate across the three main **target areas** of commercial, industrial, and government sectors. A single operation can also seek to affect multiple targets and have multiple purposes. The fact that different targets share similar vulnerabilities only strengthens the necessity for collaboration (not just information sharing) across the entire cyber environment, regardless of whether the target is a public or private entity.

Objective 1: Collection of and Access to Confidential Data

You name it, every commercial, industrial, and governing entity is a potential treasure trove of information to the right attacker. This isn't just "spy vs spy". Remember that the government sector holds a great deal of sensitive data beyond plans and strategies including intellectual property, personal and proprietary data. It also includes data related to control systems, such as dams or water treatment facilities—these are potential vulnerabilities that must be protected. In some highly regulated industries, companies are required to report their cyber and physical security strengths and weaknesses to the government. Unauthorized access to those reports by one of our adversaries is obviously a serious concern. This is not only about data being accessed; there is the potential for data being altered with a negative impact on operations and safety.

Of course, these attacks also focus directly on the private sector. Just a few months ago, both the Department of Energy and the US Intelligence Community warned of "custom made" malware targeting the control systems for both electricity and natural gas. The warning indicated that this hacking operation, probably conducted by Russian state supported groups, were mapping the US energy infrastructure. "Mapping" is a key step in intelligence gathering—the precursor to an ability to potential disrupt and even destroy energy industry or other equipment.

Objective 2: Financial Gain

This second cyberattack objective is largely the motive of cybercriminals seeking unauthorized access to funds, personal information that can be used to pose as a victim and obtain funds, or information about pending transactions or deals that can be used to engage in such activities as insider trading.

One recent area of concern: criminal, ransomware and data extortion targeting the industrial sector. We are seeing more and more threats against Industrial Control Systems (known as ICS). ICS are the different types of systems and instrumentation that operate or automate industrial processes, anything from manufacturing plants to power grids. Previously, ransomware used to focus on information technology and data access but has now expanded to this operational technology. An intrepid cybercriminal, including state sponsored groups, can threaten to stop the production line, turn off the power, or in several recent cases, turn off the oil or gas pipeline. They can do this simply by threatening administrative or enabling functions. It doesn't take a lot of imagination to see the potential harm to business and of course, to a utility's customers and operations.

Example:

Colonial Pipeline (2021): Just the threat of a potential release of data by the Cyber Crime group DarkSide caused Colonial Pipeline to shut down its East Coast pipeline delivery system for gasoline, jet fuel, and diesel. And the cybercriminals didn't even target the actual pipeline; they went after its corporate data, encrypting it and demanding a ransom. Unable to bill its customers, Colonial Pipeline turned off the spigot, resulting in a significant shortage of gasoline. This also demonstrated that blended threat that I referred to earlier when cybercriminals conduct activity, sometimes tolerated, and sometimes encouraged, by a nation state that views the attacks a serving their interest, in this case, Russia.

Objective 3: Operational Disruption/Damage

Attacks attempting to disrupt or even destroy operational controls and technology have targeted the entire spectrum of commercial, industrial, and governmental targets and have used the full range of cyber techniques and even cyber weaponry to achieve their goals. The targets include commercial, industrial and government entities that are heavily reliant on their computer network for operations. There has been a steady increase in attacks on industrial control systems that run manufacturing or utilities.

Methods: Disruptive operations often require more advanced tactics including the collection of extensive intelligence and setting up a presence in the target's network for a prolonged period of time without detection. Most recently, ransomware has sometimes been added to the attacks.

Example: Chinese government supported hackers targeted an array of US oil and gas pipelines over the past decade, seeking "strategic access to industrial control networks that run the pipelines for future operations rather than for intellectual property theft".

3. Responding to Cyber Threats:

I have briefly outlined state and state-associated cyber threats and the potential dangers to our national and economic security—but it's time for some practitioner pragmatics—the big "so what?"

You may have heard, especially about a decade ago, people referring to cyber threats by states as a potential "**Cyber Pearl Harbor**," a catastrophic cyberattack on critical infrastructure, like power grids, that would cause physical damage and injuries or death to our citizens. Have we had a Cyber Pearl Harbor? Thankfully not. Is one theoretically possible? Yes, but it is critical to give context to what the threats mean without turning to untethered panic. This debate is also a red herring; it sets a threshold for damage from a cyberattack that is quite high, forgetting that lower-level attacks can cause significant problems in everyday life as well as to our national and economic security, a kind of death by 1000 cuts. And just a cursory look at recent hacks of private-sector companies and government agencies should remind us that smaller-scale intrusions can be disruptive, dangerous and very costly even without catastrophic outcomes.

I tend to think of both the cyber and national security environment as a set of concentric circles. That means simply that this is not just an issue of direct impacts by direct attack on a specific target. Rather this means that cyber state and non-state attackers aim at not just their primary target, such as gas or energy distribution, but the enabling functions often supplied by third party partners. When attackers are frustrated by their primary targets, they turn to those concentric enabling circles—suppliers who have some access into the network or even the

physical plant of the target. They gather intelligence, conduct reconnaissance, gather organizational and structural information and they search for the backdoor for unauthorized access. States historically were most proficient at this intelligence work; but that is no longer exclusively true. Once again, state supported non-state actors have proven themselves agile learners at collecting intelligence about their targets and taking the time to penetrate their targets' networks to map them and assess them for further attack.

This is also a problem that I like to call "**chicken little cybersecurity**." You might recall the story of Chicken Little: he gets hit in the head by a couple of acorns and decides the sky is falling. We are all hit with a daily barrage of bad news about cyberattacks and intrusions—new malicious software, a new advanced persistent threat (APT) group, or new backdoors into our networks. Not every cyber event or newly discovered vulnerability applies to every company, government agency or entity. Throwing money at your cyber problem without incisive analysis and context is not going to keep the sky from falling on you. If you cannot assess or link the specific risk to your organization or to your sector, public or private, you are in serious danger of being overwhelmed. If the risk is not fully assessed and related to actual operations or potential fallout, you are limiting the efficacy of your cyber defense.

The response to state and non-state cyber threats is to focus; find the key vulnerabilities and risks; realize that no government agency or private company is an island onto itself. We cannot claim, nor should we, that we can repel any cyber attack or intrusion; instead, we must aim for cyber resilience—collaborative preparation and well-practiced response.

Thank you.

QUESTIONS SUBMITTED FOR THE RECORD TO RHEA SIERS, SENIOR ADVISOR (CYBER), TENEO

Questions Submitted by Representative Gosar

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

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

Answer. Both of Representative Gosar's questions deal directly with the specific details of the DOI budget. I am unfamiliar with DOI budget details such as mandated vs discretionary spending, the conditions for the reprogramming vs transfer of funds, or whether provisions exist that might limit the movement of funds to new cybersecurity programs or activities. I realize that these represent difficult choices and prioritizations but cannot offer specific guidance.

With that caveat, I want to focus on the reality of funding cybersecurity in federal agencies (and often in private entities). As previously noted, successful cyber resilience necessitates not only sufficient funding but consistent funding. In addition to the monetary costs, there is also the challenge of finding human resources—people with the right cyber and technology skills to institute best practices, stay on top of technological advancement and to move with agility and speed as necessary. Lack of funding and resources result in gaps in our ability to protect today's threats; lack of resources negates our ability to prepare strategically, operationally and coherently for new threats and future risks. It is difficult to make our networks and systems resilient when our resources are so limited that we can, at best, put out fires and try to fend off the latest hack. I'm not arguing for unlimited cyber funding; that would be unrealistic. I am advocating consistent, prioritized funding that is built on a multi-year program without interruptions, annual funding swings or "salami slice" cuts lacking a sound rationale.

Questions Submitted by Representative Gallego

Question 1. Ms. Siers, in your testimony you use the phrase "Cyber Pearl Harbor." Can you elaborate on what this means and the likelihood of such a threat occurring?

Answer. "Cyber Pearl Harbor," a catastrophic cyberattack on critical infrastructure, like power grids, that would cause physical damage and injuries or death to our citizens. It could hypothetically disrupt our daily lives, our welfare and our economy. The use of the term was more prominent a decade ago as we began to

understand the potential ramifications of cyber activity and attacks. It certainly attracted much-needed attention to cyber threats at that time. Have we already experienced a Cyber Pearl Harbor? Thankfully not. Is one theoretically possible? Yes, but it is critical to give context to what the threats mean without turning to untethered panic.

This debate is also a red herring; it sets a threshold for damage from a cyberattack that is quite high, ignoring that lower-level attacks can cause significant problems in everyday life as well as to our national and economic security, a kind of death by 1000 cuts. And just a cursory look at recent hacks of private-sector companies and government agencies should remind us that smaller-scale intrusions can be disruptive, dangerous and very costly even without catastrophic outcomes.

Question 2. You've detailed a number of existing threats in your testimony and responses. What are some of the future threats of concern in cyber security?

Answer. Given the pace of technological advancement, there is clearly much potential for future threats in the cyber realm. I'll focus on only two to provide examples of potential cyber risk. First, a supply chain cyber attack—usually when your adversary targets a trusted third-party vendor who supplies software or other services to your agency or company. The Russians hacked by deploying malicious code in management software used by thousands of government agencies and private companies. The hack gave the Russians great access into many public and private networks and is certainly a threat that could be repeated in the future. Even when companies or agencies manage their cybersecurity well, some of this is beyond their control because it resides with software developed outside their own enterprise.

The second is a newer concern—relating to the use of Artificial intelligence and machine learning that relies on data to make predictions and decisions. It's what's used in self-driving cars or translation tools for example. This is called "data poisoning" in which the attackers tamper with the data used to build the models—and "poisons" the data, rendering it unreliable or inaccurate.

Question 3. In September 2022, the U.S. activated the 3rd Multi-Domain Task Force in Hawaii to support the U.S. Indo-Pacific Command and the operations of the first task force activated in the region in 2017. To what extent does cyber play a role in our multidomain operations in the Indo-Pacific region?

Answer. Cyber is a critical part of our military operations—not only via US Cyber Command but in electronic warfare functions, intelligence and integrated into battle plans. The third multi domain task force brings together cyber, electronic warfare and intelligence. This activation supports the national security prominence of the Pacific Theater. Cyber is critical for both readiness and interoperability for all operations.

Question 4. To what extent is a cyber-attack a threat to our military operations and national security posture in the Indo-Pacific region? What are some potential consequences of such an attack?

Answer. In terms of a cyber attack—it would depend largely on the nature of the attack. First, we should note that there is a very good level of cyber preparedness by our military and a good amount of contingency planning to deal with the cyber threat. However, this preparedness does not inoculate forces in the region from disruption; nor can we say with absolute certainty how cyber attacks might lead to a serious escalation even beyond the Indo-Pacific region. There are many potential consequences of such an attack—for example, if the PRC Government makes the ill-advised decision to attack Taiwan, it will have to disrupt our military (and our allies') communications—so that threat is real and present. If an escalation ensues, there will be significant economic consequences with global impact.

Questions Submitted by Representative Grijalva

Question 1. The Offce of the Inspector General Audit found that several DOI components lacked sufficient authorizations, and the DOI did not conduct quality control reviews or submit those systems to FISMA audits. These DOI offices included the National Park Service, which manages Americans' transactions and reservations to national parks through recreation.gov, and the Bureau of Trust Funds Administration, which manages over $5 billion in trust for Native Americans. Please describe how a breach at these two offices might have real consequences for individuals.

Answer. These data breaches can provide unauthorized access to Personal Identifiable Information (PII)—depending on the type of transaction, anything from credit card numbers to birthdays to social security numbers to passport numbers. The real consequences often occur when this type of information is found on what is called "the Dark Web"—kind of the "Star Wars Bar" of cyber criminals where lots of information can be procured. The information can be used for scams, to procure other credit cards, and for any of us who have experienced this form of identity theft—it is quite a hassle and can cause considerable stress. In many cases, the victim has to replace their credit cards or even other forms of identification such as driver's licenses or passports. Victims may have their credit frozen for important transactions like home mortgages or choose to freeze their credit while investigations are being conducted. The other consequence is what the breach does to the reputation of the office/organization that was hacked—there are major reputational issues including a loss of trust by clients/customers.

Question 2. Federal agencies like the Department of the Interior increasingly rely on non-federal entities for services. For example, Booz Allen Hamilton, a major consulting form, runs recreation.gov. What are best practices for protecting federal assets that contractors have access to when the federal government does not control the contractor's cyber infrastructure?

Answer. There are already a number of requirements for contractor cybersecurity especially in the Defense sector, such as those provided by the Defense Federal Acquisition Regulation Supplement (DFARS) and the Cybersecurity Maturity Model Certification (CMMC). These provide good practices and are based on the National Institute of Standards and Technology (NIST) 800-171 (Controlled Unclassified information). General best practices are familiar ones—including such items as Multi-Factor Authentication, certain types of perimeter and endpoint protection and internal penetration and vulnerability scans. I would add that the federal agency itself must take proactive steps to monitor compliance by contractors when possible and establish firm and clear deadlines, accountability and requirements for notification in the case of a contractor breach.

Question 3. There are concerns that the significant budget cuts included in the recent debt ceiling deal would limit funding available for federal cybersecurity, much like how the cuts to agency funding recently proposed by Republicans could negatively impact our ability to fulfill NEPA requirements. What impact does funding insecurity and uncertainty have on an agency's ability to address cybersecurity threats?

Answer. Cybersecurity and cyber resiliency are not inexpensive—and this is not only a matter of dollars. In addition to the monetary costs, there is also the challenge of finding human resources—people with the right cyber and technology skills to institute best practices, stay on top of technological advancement and to move with agility and speed as necessary. Lack of funding and resources result in gaps in our ability to protect today's threats; lack of funding negates our ability to prepare strategically, operationally and coherently for new threats and future risks. It is difficult to make our networks and systems resilient when our resources are so limited that we can, at best, put out fires and try to fend off the latest hack. It is difficult to ensure cyber resilience when we put off replacing legacy systems or do it in a piecemeal fashion. I'm not arguing for unlimited cyber funding; that would be unrealistic. I am advocating consistent, prioritized funding that is built on a multi-year program without interruptions, sudden funding swings or "salami slice" cuts lacking a sound rationale.

Mr. COLLINS. Thank you, Ms. Siers. The Chair now recognizes Dr. Clancy for 5 minutes.

STATEMENT OF T. CHARLES CLANCY, SR., SENIOR VICE PRESIDENT AND GENERAL MANAGER, MITRE LABS, AND CHIEF FUTURIST, THE MITRE CORPORATION, McLEAN, VIRGINIA

Dr. CLANCY. Mr. Collins, Ranking Member Stansbury, Committee members, thank you for inviting me to testify before you today on this topic of critical national importance. My name is Charles Clancy. 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, or FFRDCs, on behalf of the U.S. Government. We provide deep cybersecurity expertise across the executive branch and the Federal judiciary.

Before joining MITRE, I led cybersecurity research and development programs as a professor at Virginia Tech, and as a scientist at the National Security Agency.

Over the past 5 years, the cyber threat environment has continued to change. Organized crime continues to target enterprise network environments with ransomware, including those used by the U.S. Government. China and Russia have elevated their offensive cyber programs into strategic instruments of statecraft.

The Director of National Intelligence's annual threat assessment concludes that China could almost certainly disrupt oil and gas pipelines and rail infrastructure in the United States, and would do so to deter U.S. military action by impeding our decision-making, inducing societal panic, and disrupting military mobilization. It also assesses that Russia is focused on attacking U.S. undersea cables and industrial control systems.

But let's, I guess, focus in a bit more on some of the enterprise networks that have been germane to the discussion so far today. I guess I want to differentiate that a bit from the critical infrastructure that Department of the Interior has oversight authority over.

So, starting with the internal enterprise networks that DOI operates, they are all governed by requirements stemming from the Federal Information Security Modernization Act, or FISMA, which was originally passed in 2002 and has gone through a number of legislative updates. This Act emphasizes a risk-based approach to cybersecurity with protections commensurate to the level of data that needs to be protected by those agencies.

Helping agencies implement FISMA is a number of key standards from NIST. So, NIST provides their security control baselines, known as Special Publication 853, and the Risk Management Framework, or RMF. These all cover the things we talked about in the earlier panels, including password complexity and multi-factor authentication, and are best practices across the entire executive branch.

The White House has also taken steps to move beyond these tools and require Federal agencies to implement zero trust architectures, which was part of an executive order 2 years ago. DOI would be well served by developing and executing a plan to implement the NIST Risk Management Framework, or RMF, and the new and emerging Federal Zero Trust cybersecurity principles that go beyond MFA, in terms of securing enterprise networks.

Shifting gears to look at the privately-operated critical infrastructure that the Department of the Interior has some oversight over, this is sort of a different set of authorities, a different set of levers that might be pulled to improve cybersecurity. So, critical infrastructure is most often operated by private organizations, subject to some form of regulations.

Sector risk management agencies, or SRMAs, have been mentioned a couple of times in passing so far during the hearing, are

responsible for the cybersecurity of those named critical infrastructure sectors. SRMAs typically promote the use of the NIST cybersecurity framework, another NIST document that is really focused on cybersecurity for privately-operated critical infrastructure systems.

While much of this ecosystem today relies on voluntary compliance and information-sharing, the National Cybersecurity Strategy that was published earlier this year by the White House seeks to establish minimum cybersecurity requirements, rather than a voluntary compliance regime for U.S. critical infrastructure.

Recent reports from the GAO highlight cybersecurity concerns with offshore oil and gas industry. While not designated an SRMA, the Bureau of Safety and Environmental Enforcement, or BSEE, does oversee security for this industry. The Bureau 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 that is consistent with the National Cybersecurity Strategy.

Major operators of offshore energy and their corresponding onshore transportation infrastructure could implement an integrated strategy for securing both, which the intelligence community assesses as specifically under threat from China.

Recent cyber attacks against Guam attributed to China are also concerning. 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, DOI and DOD could develop a closer partnership on securing the infrastructure upon which both the U.S. military and citizens of Guam depend. This could include leveraging DOD's cyber protection teams and other assets to collaboratively perform a cybersecurity vulnerability assessment of Guam's infrastructure and systems.

Implementing any of these requirements come down to workforce. Certainly, we have talked a bit about the competitive nature of the cybersecurity talent base. I will point out that the Department of the Interior does not have a current permanent chief information security officer, and I would recommend filling that position as soon as possible. Other departments and regulatory commissions have consolidated organizations focused on cybersecurity and resilience within the industries that they regulate.

One option could be to establish a cybersecurity cell within the Office of the Secretary that is focused on coordinating cybersecurity strategy and policy across all segments of DOI's regulatory and oversight apparatus.

Thank you. And with that, I look forward to your questions.

[The prepared statement of Dr. Clancy follows:]

PREPARED STATEMENT OF DR. CHARLES CLANCY, SENIOR VICE PRESIDENT, MITRE

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.

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

---

[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

[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

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.

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 Enforcement (BSEE) does oversee security for the offshore energy industry. BSEE could leverage its rulemaking authorities, in

---

[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

[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

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 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.

QUESTIONS SUBMITTED FOR THE RECORD TO T. CHARLES CLANCY, PHD, SENIOR VICE PRESIDENT AND GENERAL MANAGER, MITRE LABS

Questions Submitted by Representative Gosar

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

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

Answer. 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.

---

[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/

[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

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 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.

Mr. COLLINS. Thank you, Dr. Clancy.

I want to thank all the witnesses for their testimony. We are going to move into Member questions, and I am going to recognize myself for 5 minutes.

Dr. Clancy, I want to kind of pick up on what you were just talking about. And I may bounce around. I hope we have time for several questions from Members. It looks like there are two of us, so we may.

Government agencies and interacting. You said, if I heard you right, that that may be an answer to find someone to interact with all of these agencies. Is that right?

---

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

Dr. CLANCY. Yes, the Department of the Interior has many different pieces of the critical infrastructure apparatus over which they have authority. And having a single point to coordinate across the Department, I think, would be helpful, and also coordinate up with the Office of the National Cyber Director.

Mr. COLLINS. Mr. Cavanaugh, can you add to that? Do they already talk within this agency, or is there any——

Mr. CAVANAUGH. Sir, to answer that question, I think the structure exists for that communication, as they are able to participate in their sector-specific coordinating councils, whether it be government facilities for the vast majority of the Department of the Interior, or if it is the energy sector, or food and Ag, even for the fisheries.

The challenge has been staffing at the Department of the Interior, and identifying the appropriately staffed individual or individuals that can cover those meetings and represent the Department.

Mr. COLLINS. So, pretty much, that is what you would say would be the barrier that is keeping them from sharing——

Mr. CAVANAUGH. Being more proactive in that engagement process. The structure is there, but it has not been a primary focus for the Department.

Mr. COLLINS. And I don't know if any of you all can answer any of this, or how much you delve into the DOI, but when we were asking the first panel some of the questions, we were talking about passwords. And I find it amazing that we have a government agency that is just now identifying maybe changing passwords to passphrases. I am in the private sector. We did that years ago.

Hardware and software, does anybody keep an inventory as to what needs to be upgraded, what hasn't been upgraded?

I mean, are we still using TRS 80 model 2s, or where is the problem at in DOI?

Dr. CLANCY. I guess I will say that, under FISMA there is a set of requirements to specifically identify systems. And based on the Inspector General's testimony, it sounds like there are tens of such systems across the Department of the Interior that have sort of separately received their authority to operate, or ATO, which basically says that they have, among other things, appropriate cybersecurity safeguards.

I believe the way it would work is they would go through each one of those individual accredited systems and look at what the gaps are for implementing some of these more sophisticated cybersecurity protections, because each one likely is different, could be run by different agencies or parts of the Department.

Mr. COLLINS. Right. But it just seems like to me that, ultimately, as Mr. Cheng was alluding to, that we would be moving to a cloud-based system, where that is where you would really clamp down on your multi-factor authentication, and that shouldn't be a problem.

Mr. CHENG. Sir, one of the aspects that is, unfortunately, in play here is the software and the hardware that runs it that is embedded in a lot of the infrastructure itself, the supervisory control and data acquisition systems, or SCADA. These are, essentially, very small programs that make sure that the pipelines run, et cetera.

They have operating systems. In many cases, they are still running off of Windows——

Mr. COLLINS. Don't say 98.

Mr. CHENG. Well, a little better, but Windows 7. And the problem is that the chips that are running them, essentially mini-computers, if you will do not have the capacity to be upgraded. It is not like you can go in. You literally would have to rip out the entire machinery, and put a new one in that would be able to run Windows 10, Windows 11. But Microsoft has stopped upgrading and security updating for Windows 7.

So, in addition to the specific computer issues that have already been touched upon, there is that crossover to the literal infrastructure side of what is the level of security that is even possible on systems that were never designed to be updated, and certainly had not expected to be hacked.

Mr. COLLINS. I would agree, I just don't understand how we have agencies in the Federal Government that are that far behind. That doesn't really make sense to me.

Dr. CLANCY. I would say, from my perspective at MITRE, we see the IT infrastructure of much of the entire executive branch, and there are many agencies with 40-year-old systems still running today.

Mr. COLLINS. I know I am out of time, but one last question. I think it was Mr. Cavanaugh, you said hold employees accountable. We don't hold employees accountable for not following safety protocols, as far as even logging in?

Mr. CAVANAUGH. Having almost 13-plus years experience in the Federal Government, there is minimal accountability outside of being remediated by additional training. So, if you had a password issue, you were just assigned to take more security training. There was no actual accountability beyond training for employees.

Mr. COLLINS. I would have thought Colonial Pipeline at least would have been a huge wake-up call.

Ms. SIERS. Sir, let me add to this a little bit. We are successful, and in Federal agencies where there is success and accountability, it is because at the leadership level and the manager level it essentially becomes part of your contract. So, that has the way of changing the culture, focusing people.

I have personally, however, seen people lose their jobs over issues where there is a pattern of poor password usage and other abuses. So, I don't believe there is one answer for the entire Federal Government, but I do also really believe it is a leadership issue.

Mr. COLLINS. All right, thank you. I know my time has expired. I recognize the Ranking Member, Ms. Stansbury, for 5 minutes.

Ms. STANSBURY. All right. Thank you so much, Mr. Collins. I want to follow up on some of the testimony that all of you have given already.

The first is this set of folks who have been involved in hacking and cyber attacks who are kind of in the interspace between state actors and private actors. And I know Ms. Siers, you talked a little bit about this in your oral testimony here today. But tell us more about what kind of organizations are we talking about. Are these professional criminal organizations? Are they shops that have been

set up by state actors that are in a sort of quasi-private space, but doing contract work for them?

And what is their motivation? Why are they attacking the United States, and our systems, and our institutions?

Ms. SIERS. I would say it is a little bit of all of those. Let me just talk more about the purely criminal organizations.

This is an incredibly well-organized effort. You can buy anything you need on the Dark Web, which is kind of the cyber version of the Star Wars criminal bar. And you find all kinds of tools, you find negotiators to negotiate ransom with any victim. So, that is one category.

Then, of course, you have hacktivists, who generally claim to have political purposes and oppose certain operations or certain organizations.

And then you have this other group that we are not entirely sure on occasion where they come from, but we know a couple of things. One is they are either physically present or availing themselves of servers in specific states, and it is the usual suspects, to be honest: Russia, China, Iran, North Korea. And they are at least given tacit approval to do what they do at one end of the continuum. And at the far end of the continuum, they have direct state support. And sometimes that even includes—and we have seen this in Russia—moonlighting intelligence officers, who actually go there after hours and assist these groups.

We have also seen these patriotic hacktivist groups. Russia has used them on a number of occasions. They are using them now, they used them against Estonia. That is to afford them some kind of plausible deniability, so that they are really unable to point to a specific government figure.

So, you have this whole panoply. It makes attribution, which is kind of our whodunit in cyber, sometimes somewhat difficult, and it makes strategies to respond sometimes a little bit difficult, as well.

Ms. STANSBURY. Well, if there is one thing this hearing has been, it is terrifying to really understand the full breadth of the kinds of organizations and activities that are happening out in the world here.

And Mr. Cheng, as you were testifying today, and I know in your written testimony, as well, you mentioned the attack on Guam and its telecommunication systems, and sort of touched a little bit about the implications for a Chinese extension of its sphere of influence in the South Pacific. I wonder if you could talk a little bit more about that, and the implications for the United States and for our strategic and global position in the South Pacific, and our relationship with China.

Mr. CHENG. Absolutely, ma'am. As the People's Liberation Army has expanded its array of missile capabilities, operations within what is sometimes termed the First Island Chain, stretching from Japan through Okinawa, Taiwan, the Philippines, and down to the Straits of Malacca, have become much more problematic. Whether or not U.S. air bases, U.S. aircraft carriers, et cetera will be able to operate in those waters is becoming more difficult.

So, the Department of Defense is intent upon establishing, essentially, a fallback position in the Central Pacific through what is

sometimes termed the Second Island Chain, which would stretch through Guam, the Republic of the Marshall Islands, et cetera.

Notably, the Chinese have been working very hard to invest and to develop infrastructure across this region, but they are also monitoring what is going on there.

The other aspect to keep in mind is, especially on the island of Kwajalein, which is part of the Republic of the Marshall Islands and therefore within the DOI's remit, is an array of key defense facilities, including the Ronald Reagan Ballistic Missile Defense test site, a key site where we test our ICBMs, which is essential to nuclear deterrence, but also the establishment of the space fence, so that we can see what is coming, basically, over the horizon.

These are key targets for Chinese espionage, but as important in time of crisis or conflict would be facilities that would be targeted, ideally, through cyber means simply because of the distance from Chinese military forces. So, all of these are essential to maintaining American dominance through the Central Pacific region, and are primary targets for Chinese kinetic and non-kinetic means of attack.

Ms. STANSBURY. Well, thank you for sharing all that. One of the things that our Committee is doing, and you mentioned this in your testimony, while our Committee is primarily over the domestic functions of the Department of the Interior, this is the Committee that also oversees and does oversight over our relationship with many of the associated states and territories that are in that region. And we have just stood up a bipartisan task force to look at many of these issues, which myself and others are serving on.

I do have one more follow-up, which is really about the last two questions I asked. And Dr. Clancy, I didn't realize when I read your testimony initially that you had worked in the national security space outside of the private sector. So, I was really interested to hear that in your introduction.

You touched on this a little bit in your oral testimony, but since you do have that background, I wonder if you could talk a little bit more about what are some of the things that you see Congress and our agencies can do to beef up that relationship with DOD, and to make sure that we are really protecting these critical, critical assets and pieces of infrastructure on the cyber side so that we are not vulnerable to the kinds of attacks and espionage that we have been talking about.

Dr. CLANCY. Yes. I think, specific to Guam, I think there is a great opportunity for partnership with DOD, given they are a major component of the ecosystem there.

The example I said in my testimony is leveraging DOD cyber protection teams to go out and work collaboratively with the privately-operated Guam utilities to help identify potential vulnerabilities and beef up security.

Other things could be for the Department of Defense to start including language in the contracts that they have with local utilities for power, water, other sorts of things, requirements that they meet additional cybersecurity requirements. And while that would likely increase the cost of those services to DOD, it would also pro-

vide resources back to those utilities to help beef up the security, given there is such a dependence on that.

I will note that it is not just Guam, though. Hawaii is another big opportunity for DOD collaboration with local utilities, and some of the other territories, as well.

Ms. STANSBURY. Thank you very much. And we will be working on the NDAA in the coming months, and I think this is something we would really love to work with the Majority on, is to figure out how to make sure we are beefing up all of these resources.

So, thank you, Mr. Chairman, and I yield back.

Dr. GOSAR [presiding]. I thank the gentlelady, and she is right on, because we have the Holman Rule, so we can go line item by line item to make those priorities.

And Mr. Cheng, can you elaborate on the fundamental difference between Chinese and Western execution of cyber economic espionage? What is the fundamental difference between the two?

Mr. CHENG. The fundamental difference, sir, is that the West, for most purposes, is dominated by private industry. There aren't too many state-owned enterprises, state-run entities, and there is also a real separation of powers. Posse Comitatus title 10 versus title 50 are just some of the examples of how, in our system, the military is circumscribed in what it can do.

So, the idea that a Western government would put its cyber military elements out there to, say, steal data about X industrial or economic process creates fundamental issues, beginning with can the government order you to do that, to how would you even disseminate that data. If you gave data on new cars to Chrysler, Ford and GM would be unhappy. If you gave it to all three of those companies, you have probably told everyone in the world that you are engaging in cyber economic espionage.

In the case of China, every one of those aspects is different. The Chinese economy has substantial state-owned enterprises, which means that you can share data directly within the government because oil companies, steel companies, shipbuilding, those are part of the government.

And the Chinese have publicly in their own writings noted that the People's Liberation Army, which is a party army, it is not a national military, it is part of the Chinese Communist Party, it is supposed to do what the party needs it to do. And if that means the party needs it to go and steal economic information, intellectual property, map out private company data, establish, you know—that is a legitimate order for the PLA to acquire that data, which can then be shared within the Chinese system because these state-owned enterprises, the main beneficiaries, are part of the government, as well.

So, we are talking about a fundamentally different ecosystem, a fundamentally different view of the role and responsibilities for the armed forces. And let me note here that Chinese description of their cyber forces—again, from their writings—is the military, non-military governmental entities, but also non-governmental entities ranging from universities to private companies. The CCP is able to reach out and employ a whole-of-society approach within which, therefore, Chinese cyber economic espionage occurs. This is a very different model than anything we see in the West.

Dr. GOSAR. Wow. How much has the Chinese cyber capabilities improved over the past 10 years? And have they outpaced the United States in these capabilities?

Mr. CHENG. We are watching the Chinese steadily improve their cyber capabilities. Pre-2015 a lot of their cyber penetrations often left fingerprints. The Mandiant Report on APT1 back in 2013 was able to determine a PLA unit 61398 cyber activities because they were able to identify who some of these players were, who in turn had essentially left digital fingerprints of who they were.

Since 2016, they have become much tighter. It is harder to identify. But I would defer to either other members of this panel or people from our intelligence community who can provide much greater detail.

Dr. GOSAR. We have also heard today about staffing challenges with IT professionals in the Department and government-wide. What would prevent the Department from using its contracting authority to overcome some of these challenges? Could that be a potential short-term alternative?

Dr. Clancy and Mr. Cavanaugh, could you answer that?

Dr. CLANCY. I think, certainly, it is a function of budget. Many agencies and departments leverage outside contractors for IT work all the time. Certainly, MITRE, as an operator of federally funded research and development centers, we are turned to often by many of those agencies for such tasks. It is often just a function of having budget in order to do that.

Dr. GOSAR. OK.

Mr. CAVANAUGH. And from my perspective, the NIST cyber risk framework provides a great opportunity for them to direct a contractor to address some of those outstanding needs that they have.

But I would caution that right now the tendency across government is to chase after shiny objects and things you are hearing in the cyber community: Zero Trust architecture, polymorphic malware. We have spent a long time and a lot of energy and money building walls around our systems, and not a lot of time understanding what is on our systems and how to observe if anything is there, capturing the point of the fingerprints being left behind in other scenarios. It has just not been a priority.

So, we need to prioritize the infrastructure that has the highest likelihood and highest consequence for impact, and in that process also start closing the ability to detect when something is on our system.

Dr. GOSAR. So, is the procurement process part of the problem?

Mr. CAVANAUGH. I would argue, yes. Right now, there is a tendency to lean heavily in contract bundling, which doesn't always net the outcomes that you are hoping for. The current process makes it very hard for small businesses to engage, and a lot of your innovation in the tech sector is being driven by start-ups and small companies that are understanding the edge of technology.

I would risk that the Internet of Things that we have talked about for a few years now is now becoming the leading edge of where cyber vulnerabilities will exist. And the companies that are most apt to understand that and be able to address those needs may not be your larger corporations and Big Tech; it will most

likely be small companies that have understood that, and are addressing only that, and not being driven by their corporate priorities.

Dr. GOSAR. I am going to ask this last question for each one of you to answer. What, if anything, is preventing the Department from prioritizing cybersecurity in their annual budget process?

I will start with you, Mr. Cavanaugh.

Mr. CAVANAUGH. I think the point we have seen today is maybe prioritization within staffing and leadership. So, they don't have a CISO, Dr. Clancy?

Dr. CLANCY. Correct.

Mr. CAVANAUGH. Yes, that is a huge challenge. So, not having a CISO and not having someone at the leadership level guide and direct strategies are pointless without leadership buy-in.

In terms of capturing how they get there today and appropriately budget for it, they need to have a strategy that identifies and prioritizes. They need to understand what it is they want to close down on and where they want to look.

We spoke a little bit about offshore oil and gas. I would also surmise that offshore wind, which is going to become a growing thing, is going to be equally vulnerable as oil and gas. Iran has already successfully proven that they are targeting wastewater and water treatment facilities.

Dr. GOSAR. Mr. Cheng?

Mr. CHENG. Sir, if we look at a corporation, and it is anything other than a cybersecurity company, IT security is an overhead problem. It is not a profit center. And I would suggest that, essentially, the same is going to be true not only for the Department of the Interior, but the Department of Commerce, even DOD and elsewhere, which is to say IT security is not seen as the primary mission of the agency. It is part of yes, I have to hire people, yes, I have to keep the lights on, I have to buy new desks for people, et cetera.

As I believe it was the GAO witness testified, 83 percent of the budget, when it comes to IT, is operations and maintenance. It is keeping the computers running. Antivirus software may be part of it, but it is largely, "I have the blue screen of death, how do I get my computer to turn back on?" not "Are the Chinese rummaging through my files?"

So, making it a priority, I guess part of the issue is going to be which part of the other responsibilities that are part of DOI on its web page, are you going to ask us to lower in priority or deprioritize? Is it managing the national parks? Is it overseeing offshore pipelines? Because unless you elevate it to—and that would have to be true across a lot of departments—"This is job two", it is going to be other duties as assigned.

Dr. GOSAR. Ms. Siers?

Ms. SIERS. Well, let me talk about this a little bit from the private sector. It is not a profit center until you are hacked, seriously. And then everything changes. And that is usually a good thing.

But the real problem, having listened to the term "legacy systems" used continuously by the first panel, which, of course, raises many concerns, the real issue is we are fighting fires every

day. So, we focus on the tactical, and we don't talk about what Mr. Cheng referred to as the strategic issues down the road.

So, when our funds are limited, we are putting out the fires but we are not trying to consider what might happen, for example, with some of the improvements in AI, and how that is going to impact us. We are generally woefully unprepared for that, because it is human nature to respond to the first thing on your plate.

That involves leadership, again, and a certain form of management in terms of your cyber and your infrastructure. And in order to do that, you have to have a very disciplined budget process, as well, that takes every part of your budget and projects it 3, 4, 5 years ahead to see where the impact is going to be, and see what risk it is really going to help with.

Dr. GOSAR. Mr. Clancy?

Dr. CLANCY. I think that is a great point there. The legacy system issue is, I think, also coupled in with the cybersecurity issue. If you spend a whole bunch of money on cybersecurity Band-Aids to put on top of legacy systems, you may be throwing good money after bad. So, it might be better to think about a broader IT modernization effort that includes improving cybersecurity as part of it to get a more systemic set of solutions.

Also, I want to note that that is specifically with respect to their enterprise IT infrastructure. That is different than having the right experts to help with the regulatory aspects of overseeing the cybersecurity of the private sector-operated infrastructure like the offshore oil and gas.

Many critical infrastructure sectors, specific agencies have workforce shortages there. I think after the Colonial Pipeline hack we realized how ill-staffed TSA was to help respond. Same thing with the Florida wastewater attack a couple of years ago, where EPA, again, was caught flat-footed without a robust team of people who were really paying attention to this.

So, I think there are sort of two different strategies. There is a broader IT modernization strategy, I think, that is needed for the enterprise infrastructure, but also getting the right experts in to help with the regulatory and oversight component.

Dr. GOSAR. So, I am going to ask one thing. What was the question that you wanted asked, and it wasn't asked, and what is the answer? What keeps you up at night?

We are going to go back in reverse order. Mr. Clancy.

Dr. CLANCY. I guess I will just note that I think with China and Taiwan, we are in sort of a couple-year window here to figure out how to combat large-scale cyber attacks against U.S. critical infrastructure. And that window is getting shorter and shorter, and I think we need to take aggressive action to speed this up across all sectors.

I mentioned that, specifically, electric power, rail, oil, and gas are all being specifically targeted by China to incapacitate them so that, if they take action in Taiwan, we are unable to respond effectively. And this is a scenario that is only a few years down the road, potentially.

And the offshore oil and gas production is part of that ecosystem, and is as vulnerable or more vulnerable than many of the other aspects.

Dr. GOSAR. Ms. Siers?

Ms. SIERS. I think the question I would have liked is what are the consequences, truly, of hacking into a Federal agency. I mean, what really happens to you? I am not talking about the person who messes up the passwords.

And I think there are several levels of consequences we have to think about. The first is standard law enforcement indictments. We have seen a lot of them against the usual suspects. They are useful in some ways.

And lately, we have also seen efforts, though, to disrupt vulnerabilities writ large. And what it simply means is we are not just focusing on a vulnerability that affects a Federal agency, something wrong with a Microsoft application, for example. We are seeing vulnerabilities challenged, information being provided, patches being provided by government entities for everyone to use.

And the third part of this, which I think is probably the most important, I think the Ranking Member referred to the takedown of Hive recently, a Russian group. In essence, the U.S. Government, the FBI, hacked into it and took it down. It also provided the keys to a whole group of victims of Hive, both, I would believe, government and private sector.

So, I think we have to be clearer about what the consequences are, and I think we have to develop that as we develop this kind of culture in the Federal Government that cybersecurity becomes a priority mission.

Dr. GOSAR. Thank you.

Mr. Cheng?

Mr. CHENG. Actually, I guess I had two. My first question that I wish had been asked, and I don't have an answer to at all, is the extent to which, when there is a CISO at the Department of the Interior, how often do they interact in particular with Cyber Command and with the rest of the intelligence community, not simply from a law enforcement perspective, but broader, being informed about the nation state actors, the gray zone actors, et cetera.

And then the other part of this would have been to ask, actually, the two previous witnesses, are your agencies engaging in two-factor authentication? Do you have, personally, passphrases as opposed to passwords?

And what about the rest of the government? Is the Department of the Interior unique, or is the Department of the Interior actually not so bad because they only could penetrate 20 percent of the passwords? Commerce, Treasury, Energy, Education, et cetera. How well do they do?

Dr. GOSAR. Mr. Cavanaugh?

Mr. CAVANAUGH. For myself, I think the question I would have liked to have been asked is the vulnerability aspect. But I can address that in a couple of terms real quick here, which is things that keep me up at night.

Spending 3 years in the National Security Council as a Senior Director for Resilience, the first phone call from the Sit Room was usually to me before they woke other people up. So, I have seen a lot of things that kept me up at night. But I will say the pervasiveness of the nation state actors and the ends to which they will

be willing to go, it is a very cost-effective measure, which is very expensive to defend against. So, for them, this is a way to bleed people out. They can instill a million paper cuts while you try and take care of all your paper cuts. It is going to cost a lot of money.

And with that in mind, the things we could be doing differently is looking at our vulnerabilities through three lenses. From a software perspective, are we closing the detection gap in our software? Do we see what is on our software that shouldn't be there? And it gets back to the hashes, and it gets back to some of the encryption capabilities. It is not a hard lift, and I am sure there are companies out there that are exploring this, and we just haven't seen it yet.

On the hardware side, I think the CHIPS Act is a pretty strong move to get a good understanding of supply chain, and understanding what semiconductors mean to that supply chain. So, I think there were some efforts in the NDAA last year toward semiconductors. The ones that most worry me are essential or legacy semiconductors, because they are the most pervasive semiconductor in our systems, which I think they account for 75 or more percent of semiconductors.

And then lastly, the human factor, which is going back to the accountability piece, which we discussed earlier today, is how do we instill accountability at the employee level with the government employees who we entrust so much with.

Dr. GOSAR. Well, I just have to tell you, we ask that question because that helps us generate more questions, but it gives us a better understanding.

So, I want to thank the panel. It has been an absolute pleasure. I wish more Members would have attended, because it is incredible, what we learned today.

The members of the Committee may also have some additional questions for the witnesses, and we ask that you respond to them in writing. Under Committee Rule 3, members of the Committee must submit those questions to the Subcommittee clerk by 5 p.m. on June 12. The hearing record will be held open for 10 business days for those responses.

If there is no further business, without objection, we are adjourned.

[Whereupon, at 4 p.m., the Subcommittee was adjourned.]