Committee on Natural Resources
Subcommittee on Oversight and Investigations
Oversight Hearing
June 7, 2023

Responses to Questions for the Record
Rhea Siers, Senior Advisor (Cyber) Teneo

Questions from Representative Gallego

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?

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.

<u>This debate is also a red herring</u>; 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.

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?

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.

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?

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.

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?

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 from Representative Grijalva:

1. The Office 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.

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.

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?

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.

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?

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.

Questions from Subcommittee Chair Gosar:

1. Is anything stopping the Department of the Interior from allocating a greater percentage of its existing budget to cybersecurity initiatives?
2. How can DOI better prioritize cybersecurity initiatives with its existing budget?

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.