Testimony of Rhea D. Siers
Before The
United States House of Representatives Committee on Natural Resources
Subcommittee on Oversight and Investigations
"Examining Ongoing Cybersecurity Threats within the Department of the Interior and the Nexus to State Sponsored Cyber Actors"
June 7, 2023

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 non-state 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.