TESTIMONY OF MR. SAM CHANOSKI
TECHNICAL RELATIONSHIP MANAGER, IDAHO NATIONAL LABORATORY

before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY & COMMERCE
OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE

concerning

"EXAMINING EMERGING THREATS TO ELECTRIC ENERGY INFRASTRUCTURE"

JULY 18, 2023

Introduction

Chairman Griffith, Vice-Chair Lesko, Ranking Member Castor, and members of the Committee, I thank you for holding this hearing and inviting Idaho National Laboratory's (INL) testimony on emerging threats to our electric energy systems. Our nation's electric energy infrastructure is the foundation for societal health, a vibrant economy, and national security – and it has become contested space in the perpetual competition against those who would bring us harm.

I am a technical relationship and program developer at INL. In this capacity, I provide technical leadership, expertise, and strategic insights to Cybercore's portfolio of critical infrastructure security and resilience programs sponsored by the U.S. Department of Energy, Department of Homeland Security, and Department of Defense. Prior to INL, I spent 15 years working for investor-owned utilities, the North American Electric Reliability Corporation (NERC) and the Electricity Information Sharing and Information Center (E-ISAC), and as the global product security incident response team leader for a major grid equipment manufacturer. During this time, I also had the privilege to serve as a U.S. Army Reserve officer, providing intelligence support to defensive cyberspace

operations. My experience has given me an uncommonly broad and sometimes deep perspective from which I have seen and studied the evolution of threats to our electric grids.

Testimony

Before jumping to the enumeration and characterization of particular risks, it's helpful to establish a shared mental model to understand risk. In security disciplines, a common risk expression is: "A threat exploits vulnerabilities to impose consequences." While arithmetic symbols are often used in an attempt to explain risk as a formula or equation, it is important to recognize that this is a conceptual qualitative expression and not a strict quantitative formula. However, the general principles of multiplication are nonetheless accurate here, as a change in one element will cause a roughly proportional change in the overall risk. Consistently decomposing and communicating security risk in this manner facilitates effective risk management.

External sources of harm are often beyond our direct control.. In cybersecurity, threats are sentient human individuals and organizations, and for all-hazards approaches threats also include severe weather, economic conditions, animals, vandals, and so on. For a threat to credibly exist it must have the intent and ability to inflict harm in a particular manner, and the opportunity to do so.. For some threats, the opportunity is constant but for others there are particular conditions required for the threat to take action. Natural threats don't require intent; hurricanes and macroeconomics are not sentient, of course.

Vulnerabilities are weaknesses that a threat can take advantage of to inflict harm in a particular manner. In cybersecurity, vulnerabilities are frequently associated with technical flaws in software, commonly documented in a CVE (Common Vulnerabilities and Exposures notice) and usually remediated through patching or upgrades. While these technical flaws are certainly good examples as a class, they are not the only type of vulnerabilities. Threats also exploit latent weaknesses in larger technical systems as they actually exist, which usually has drifted over time from their initial on-paper design intent and as-understood state. Vulnerabilities also exist due to natural human fallibility manifested as individual error or poor organizational choices, and due to operational and

business processes with weaknesses that fail to reliably produce only their intended outcomes.. Sentient threats can and do deliberately exploit these vulnerabilities in people, process, and technology, while all-hazards threats act through the laws of physics, engineering, and human behavior.

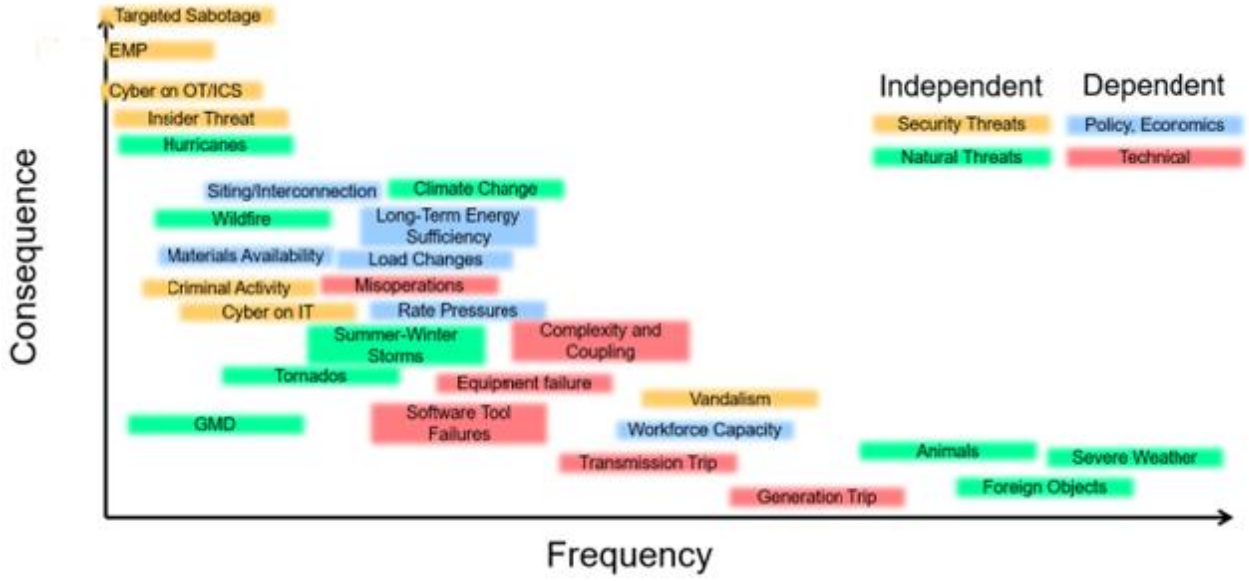
Taken together in the context of a particular risk, threat and vulnerability represent likelihood. Again, this is a conceptual and not a quantitative formulation, but it is nonetheless useful to help understand cybersecurity risks alongside and as a component of overall business risk. Since likelihood is dependent on timeframe and given enough time most risks will eventually be realized, it is easier to think in terms of frequency and how often a particular risk is realized.

Consequence is the third aspect of risk; it is the extent of the harm that could be inflicted. It is a combination of magnitude and duration, and there is often significant nonlinearity in consequence. Higher magnitude impacts that are of a short duration may ultimately be of considerably lower consequence than a lesser impact that persists over a long time.

With this risk expression established mental model established, it is helpful to understand how each of the three elements can be influenced to mitigate the risk.

- An asset owner typically can't directly influence a threat, so the threat's capabilities, opportunities, and intent, must be understood.
- Latent weaknesses and vulnerabilities must be found and remediated. We can and should also take proactive measures to minimize the introduction of new vulnerabilities and weaknesses into people, processes, and technology. Unlike threats, an organization should largely be able to control its own vulnerabilities, subject to resource constraints and external dependencies.
- Consequences are minimized, focusing on either the ultimate magnitude or the duration. It's also helpful to understand how magnitude and duration interact for each particular risk. They are not always linear.

My testimony focuses on security threats, and as part of that it's helpful to consider the consequence and frequency of security threats relative to other threats facing our electric energy systems. There are no single universally accepted practices to name or broadly categorize threats, so I've chosen to use plain-language recognizable names (even where this is counter to the risk expression described earlier) and group them as Security, Natural, Policy and Economics, and Technical threats. While the different threats are shown as discrete points below, they are more of a convex-to-the-origin range of consequences and frequencies. The graph below is not quantitatively precise, but I believe it is qualitatively accurate, to my experience and knowledge.



Threats on the vertical asymptote are commonly labeled as high impact, low frequency[1] (HILF), with Black Swan consequences so severe that they might be expected to "kill the organization." Surviving these consequences should they ever occur is the goal here., Strategies to reduce consequences and remediate vulnerabilities are appropriate here. Without entering a lengthy debate over terminology, this is sometimes referred to as resilience.

[1] See DOE and NERC's 2010 "HILF Report" at https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf

Threats on the horizontal asymptote are low impact, high frequency risks that are realized as a regular part of everyday business, with consequences that could be categorized as "annoyances," "routine trouble" or "a cost of doing business." Even in aggregate, the consequences of these realized risks do not jeopardize the organization's status as a going concern. Thriving in these expected everyday conditions while absorbing the consequences of the accepted and realized risks is the goal here, sometimes referred to as robustness. Leveraging automation and standards-based approaches are well-suited for managing these risks.

At the knee of the curve is an interesting group of threats whose impacts are high enough to merit attention but well short of catastrophic, and which occur frequently enough to identify and understand trends but short of being able to establish any statistical significance. Learning from and reducing the aggregate impacts of these realized risks is the goal here, similar to the concept Nassim Nicholas Talib describes as antifragility[2]. Doing so over time will change the shape of the curve to be more convex and may help prevent a confluence of realized everyday risks from spiraling into the catastrophic consequences of what Charles Perrow explains as "normal accidents."[3]

While a deep discussion of each security threat is beyond the scope of this hearing, I want to touch on some points to consider when those detailed analyses and discussions take place:

- Many of these risks have interactive dependencies with one or more of the other risks; some of these dependencies are well understood, others are not. These couplings should be deliberately explored when designing mitigations for a particular risk, to prevent unintended consequences.
- In many cases, there are forces holding different threats at their current frequency or consequence, e.g., NERC Critical Infrastructure Protection (CIP) Standards regulation helping hold cyber threats against OT/ICS to lower realized consequences, or deterrence holding EMP to a frequency of "it hasn't happened

[2] Taleb, N. N. (2013). Antifragile. Penguin Books.
[3] Perrow, C. (1984) Normal Accidents: Living with High-Risk Technologies. Basic Books, New York.

yet."

- Natural threats change on seasonal to generational timeframes and with more predictability, but security threats can evolve much faster and with more surprise. The timing of a security threat taking overt action may be influenced by facts and circumstances driven by natural threats, such as a targeted sabotage timed to take place when the grid is under stress from extreme weather.
- Artificial intelligence and machine learning, and other future game-changing technologies, will provide new capabilities to threats and also new opportunities for defenders and operators. It is challenging to foresee the eventual impacts of these advancements at early stages.
- While policy and economic risks are not direct security concerns per se, malign influence and misinformation campaigns can exploit our differences and disrupt efforts to improve grid security, introduce or sustain weaknesses into systems, or simply hamper our focus and resolve.
- The value chains on which our electric energy infrastructure depends are global, and their security requires consideration of individual and shared roles and responsibilities across the ecosystem.[4]

As one of DOE's 17 national laboratories, and the lead nuclear energy laboratory, INL's mission is to conduct research, development, and demonstration of solutions that will assure the advancement of nuclear energy, clean energy, and critical infrastructure protection technologies – all with the objectives of assuring the energy, economic, and national security of the U.S. As such, INL is at the forefront of U.S. and international control systems cybersecurity and grid resilience research. We support DOE in developing and implementing initiatives to research, develop, and test new methodologies and technologies to protect and add reliability to energy infrastructures as we evolve toward a cleaner fuel mix; add new energy sources, storage, and consumers; and manage the risks of malicious cyber and physical activity, electromagnetic pulse (EMP), and other natural and man-made phenomena. Two programs are of particular relevance to this testimony and hearing:

[4] World Economic Forum (2020). Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain. https://www3.weforum.org/docs/WEF_Securing_the_Electricity_Value_Chain_2020.pdf

- By including cybersecurity as a core element of engineering risk management, Cyber-Informed Engineering (CIE) ensures that inherent risks of digital technology are considered and mitigated in the earliest possible stages of the design lifecycle. CIE is applied within each lifecycle step for engineered systems, from early concept to implementation. CIE facilitates a mindset and culture for designing engineered systems through which all parties involved in critical functions (particularly engineering personnel) consider how cyber risk could be mitigated through purposeful design. Adversarial considerations and the engineering process combine to improve existing functions or build a system that has significantly reduced possibility of critical failure or compromise via cyber means. CIE emphasizes engineering out potential risk in key areas, as well as ensuring resiliency and response maturity within the design of the engineered system.
- Consequence-driven Cyber-informed Engineering (CCE) puts CIE's cybersecurity in engineering concepts into practice at an organization by considering their most critical functions from an adversarial perspective. CCE begins with an assumption that a sophisticated and determined adversary will compromise an organization, but that it is possible to determine which functions could cause critical impact if manipulated and plan high-impact defensive measures against an adversary's interference.

INL is proud to take on this challenge in partnership with Congress, DOE and other government and private sector partners to protect our energy systems. I sincerely thank you for the opportunity to provide testimony on this important issue, and I look forward to your questions and insights.

Summary of Key Points

- Security risk is expressed as a threat exploiting vulnerabilities to impose consequences. Threats are external sources of harm, vulnerabilities are weaknesses in people, process, and technology that a threat can take advantage of to inflict harm, and consequence is the harm expressed as magnitude and duration.

- Risks can be mitigated by a combination of understanding threats, finding and fixing vulnerabilities, and taking actions to reduce or limit consequences.

- Threats to electric energy infrastructure can be categorized as security, natural, policy and economics, and technical threats. Moving generally from high consequence and low frequency to low consequence and high frequency, security threats can be further subdivided into targeted sabotage, EMP, cyber attacks on operational technology and industrial control systems, insider threats, criminal activity, cyber attacks on information technology systems, and vandalism.

- Strategies to manage high-consequence, low-frequency (HILF or Black Swan) threats aim for survival and resilience, where automation and standards-based approaches delivering robustness are well-suited for lower consequence high-frequency threats where the objective is to not just survive but to thrive despite the lower-level threat noise. Threats at the knee of the curve, which are consequential enough to gain attention and warrant response but still frequent enough to perceive trends from, are where we learn how to reduce the consequences of future threats; this is how we can improve from where we are today.

- INL's Cyber-Informed Engineering (CIE) approach and mindset, as applied through the Consequence-driven Cyber-Informed Engineering (CCE) methodology, are high-impact programs to counter existing and emerging threats to critical functions and infrastructures, including electric energy systems.