STATEMENT OF
MR. BRENT J. STACEY, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
SUBCOMMITTEE ON ENERGY
COMMITTEE ON ENERGY AND NATURAL RESOURCES

JULY 12, 2016

Mr. Brent J. Stacey, Associate Laboratory Director, Idaho National Laboratory National and Homeland Security Division

U.S. Senate Hearing to receive testimony on S.3018, the Securing Energy Infrastructure Act, and to examine protections designed to guard against energy disruptions

Introduction

Chairman Risch, Ranking Member Manchin, and distinguished members of the Subcommittee; I want to thank you for holding this hearing and inviting testimony from the Department of Energy's Idaho National Laboratory, also known as INL. As a fellow citizen of Chairman Risch's home state of Idaho and the Associate Laboratory Director of INL's National & Homeland Security Directorate, I am honored to participate with this most distinguished panel in the national discussion on the role of technology and research in assuring the security of the energy sector, one of the lifeline sectors within the 16 sectors of our critical infrastructure. I request that my written testimony be made part of the record.

S.3018 "Securing Energy Infrastructure Act"

INL extends its gratitude to Senator King, Senator Risch, Senator Collins, Senator Heinrich, Senator Crapo and Senator Mikulski for the leadership and dedication demonstrated in sponsoring S.3018 – with the goal of establishing a pilot program to develop a cyber-informed engineering strategy that defends our energy infrastructure from the most serious of security vulnerabilities. Electricity and the grid are essential in all sectors of our infrastructure, including transportation, communications and water.

The grid plays a central and unique role in our national security and public safety. Components within S.3018 support the objectives of ongoing and proposed research, development and testing within the Department of Energy (DOE) laboratories. Additionally, this bill has elevated the public discourse on a number of factors, including: 1) the benefits of how digital control systems and communications improve safety, reliability and efficiency; and 2) the security risks of cyberattack on individual components, systems and interdependent infrastructure.

This public discourse also has included discussions regarding slowing or stopping the implementation of advanced technology within certain, highly selective elements of the energy sector to eliminate the risks of cyberattacks that could result in high-consequence events from sophisticated adversaries who are focused and capable of conducting targeted attacks on power systems.

Outside of the policy debate, INL views this bill not as taking a step to limit the implementation of advanced technologies, but rather an opportunity to perform the research, development and testing necessary to explore, innovate and validate, with science-based data, the ground truth on credible, high-consequence vulnerabilities and the best way to mitigate these vulnerabilities.

We understand that the solutions resulting from this science-based ground truth on vulnerabilities and mitigation will include advanced technologies and all other practical solutions that can be proven and practically implemented to protect our national energy sector. We believe that our understanding also is consistent with the intentions and

perspectives of many peers in government and industry. My colleague, Mike Assante, the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) Security, said this: "*Beyond enhancing our cyber defenses, our goal is to unlock the greatest benefits that technology offers, but not go so far as to ignore the select need to establish responsible limits and alternatives.*"

Consistent with the language in the legislation, this is a role that is most appropriate for national labs. INL, as well as many other laboratories, partner on the research and implementation of a breadth of solutions with public utilities and control system vendors. This research, detailed later in this testimony, is sponsored by and coordinated with DOE's Office of Electricity Delivery and Energy Reliability, DOE's Office of Nuclear Energy, the National Nuclear Security Agency's Office of Defense Nuclear Nonproliferation, and DOE's Office of Intelligence and Counterintelligence.

Based on the ubiquitous nature of industrial control systems, their protocols, and often their automated operational functions, there is an economy-of-scale benefit of this research across all 16 sectors of critical infrastructure, the Department of Defense, Department of Homeland Security and many other federal, state and local governments. The integration and coordination of this cross-sector work is becoming significantly more important as we seek to address the challenges of preventing catastrophic, cascading, high-consequence events from sophisticated, highly adaptive cyber adversaries.

Idaho National Laboratory's role in Infrastructure Security

INL has the mission to discover, demonstrate, and secure innovative nuclear energy and critical infrastructure solutions. To achieve our mission and vision for securing critical infrastructure, INL provides the nation with the scientific capabilities, world-class research expertise and unique experimental infrastructure to conduct the complex research, development, demonstration and testing that are needed to protect the energy sector's infrastructure. INL's national security R&D emphasizes physical protection against ballistics, explosives and natural phenomena, such as solar storms, as well as the cyber protection of advanced digital controls, embedded and wireless communication systems.

INL's leadership and partnership with other federal agencies and industry in the protection of the nation's infrastructure is grounded on an accumulated history of innovations in risk and vulnerability assessment; infrastructure interdependency modeling and simulation; technical threat analysis; scaled testing of physical and cyber threats; and the deployment of information and technology solutions that assist public and private stakeholders in preventing, mitigating and recovering from natural and man-made threats.
Examples include:

1) The "Aurora project test," which was performed for the Department of Homeland Security (DHS), during which an electrical generator was destroyed by exploiting a cyber-physical vulnerability.
2) The completion of more than 100 cybersecurity assessments on vendor and asset-owner control systems in support of the DOE Office of Electricity Distribution and Energy Reliability's National SCADA Test Bed.
3) First-of-a-kind, grid-scale, ground-induced current tests for the Department of Defense and DOE to establish a scientific baseline for understanding the threat to the power grid from geomagnetic disturbances (GMD).

4) Multitudes of industrial control system cyber threat reports and advisories, on-site cyber assessments, interdependency analyses, and training sessions with government and industry for the Department of Homeland Security Industrial Control System Cyber Emergency Response Team (ICS-CERT), DOE, and Department of Defense.

Our U.S. utilities have been efficient and effective in engineering and maintaining the electric sector's infrastructure for functionality, reliability and safety – and in raising their cybersecurity hygiene through the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards. Yet, with the advent of sophisticated and adaptive cyber adversaries, such as seen during the attack against the grid in Ukraine, we are now faced with the need to enhance our critical infrastructure's efficiency, reliability and safety by implementing effective security features that can detect, resist and respond to the most sophisticated cyberattacks.

Principles and Trends

INL is committed to perform our national laboratory's role to advance scientific knowledge and to help transform the security of our national infrastructure. Our vision for control systems cybersecurity research is grounded upon the following principles and threat trends:

1) Cyber risks to critical industrial control systems and networks are serious and are taken seriously by industry and government.
2) The U.S. and our allies are playing catch-up in research investments and validation of assessment results given the complex co-dependencies of technology, engineering, and process.
3) The speed of technological innovation is outpacing our traditional approach to solve the problem by using standards and policies.
4) Determined, sophisticated and patient adversaries will be successful in penetrating an infrastructure's digital systems.
5) A disciplined adversary likely will know the dynamics of industrial control system (ICS) technology better than the asset-owner. Since the asset-owner will know their engineering and operational/business processes better than the adversary, we need to leverage our detailed engineering and process knowledge for a higher level of cyber protection.
6) While we are catching-up with incremental improvements to harden our defenses and better detect and respond to a cyberattack, we also can make progress if we identify and focus protections on the few areas where we have made engineering and business decisions that leave us exposed to high national security level risks. These areas of high risks are where we can re-design and develop engineered barriers or cyber-informed human responses as last lines of defense to remove the possibility of a significant consequence.
7) Cyber authorities, system defenders and research efforts are spread across multiple government, academic and industry organizations. Access to this dispersed advanced control systems security talent is limited and does not facilitate response in a coordinated and integrated manner to prioritize resources on high-consequence vulnerabilities. Additionally, robust and resilient security solutions to address threats to functional cyber-physical systems require access to multidisciplinary operational and engineering teams and realistic at-scale experimentation environments. We have observed that unique integrated staff and facilities for research and protection of our

infrastructure reside within the DOE laboratory complex and within a few select organizations across the federal government and industry.

8) Technology advances for automation and digital control are inherently embedded into our energy infrastructure. The opportunity to go back decades to implement large-scale manual control and response is unfeasible relative to the benefits from diversifying our energy supply with renewables, providing service and reliability into rural regions, and managing costs by balancing supply and loads.

Consequence-Driven Cyber-Informed Engineering

INL is piloting a transformative approach. Consequence-driven Cyber-informed Engineering (CCE) reprioritizes the way the nation looks at high-consequence risk within the control systems environment of the most essential infrastructure assets. Our goal is to provide both private and public organizations with the tangible steps and tools required to examine their environments for high-impact events/risks; identify implementation of the most likely digital devices and components that facilitate that risk; illuminate specific, plausible cyberattack paths for these digital devices; and develop concrete mitigations, protections and tripwires to address the high-consequence risk. The ultimate goal of the CCE effort is to help organizations take the steps necessary to thwart cyberattacks from even the most highly resourced, top-tier adversaries that would result in a catastrophic physical effect.

The CCE framework research is built upon three generally recognized realities of control systems cyber space:

1. Asset-owners must recognize the difference between targeted and indiscriminate attacks, and accept that if targeted by an advanced cyber adversary the asset-owner will be compromised.
2. Traditional IT security defenders primarily are focused on cyber hygiene which, while critical to an overall cybersecurity strategy, is only sufficient to repel non-targeted attacks, rather than the cyber-physical effects of a high-consequence event. Minimizing these effects, along with the potential impacts of an advanced persistent threat, depends upon the highly technical skills available through government assistance.
3. Control systems are most often designed to meet functional engineering and safety requirements, not security requirements. As such they are designed and programmed around failure mode analysis of the function rather than incorporating improved risk-based and synergistic security profile.

When INL pilots this CCE approach with utilities and government organizations, we work with them to tackle the challenge by advancing through four distinct phases:

1. Consequence Prioritization. The entity and government partner identify the highest-consequence event that would pose a risk to national security - for example, loss of electricity to a large segment of a utility's customers for eight days or longer.
2. System-of-Systems Breakdown. The entity evaluates its infrastructure and operational processes to identify critical functions and services that are linked to the highest-consequence event. This process can be thought of as an engineering analysis process.
3. Consequence-based Targeting. This phase builds on how an adversary achieves a specific impact against a target system. The entity and INL cooperatively share information to answer this question: "Is there anyway an adversary can achieve a negative impact through cyber to this function?" Using the ICS Cyber Kill Chain (a

high-level model that emulates the steps used by an adversary), the entity can identify steps necessary for an adversary to be successful against a specific system(s).

4. Mitigations and Protections. The goal of this phase is to intelligently improve the security posture based on development and implementation of physical, infrastructure, digital, engineering or operational change(s) that interrupts the attack vector against credible target systems.

INL is currently validating this approach in several sectors through pilot projects. Some lessons being learned as critical to the future success of this approach are:

1) We will benefit from more effective translation of classified threat information about the specifics of threat actors' technology readiness capabilities and intentions to do damage into "actionable intelligence," information that is specific, prioritized and implementable into changes in an asset-owner's systems and processes.
2) We can benefit by optimizing and coordinating research, expertise and information-sharing forums to gain economy-of-scale in solving high priority ICS cybersecurity challenges. There is much commonality among the control systems and their protocols that generally are ubiquitous across the sectors of critical infrastructure. Hence, much of the technical threat and technical solution information developed for a high priority vulnerability will be useful to many others.

Partnership is Critical

The challenge of protecting our energy infrastructure is vital and complex. By complex I mean that it is technologically complex, institutionally complex and politically complex. Our energy infrastructure is an integrated system that must be protected on multiple fronts. Our country needs short term tactical solutions, but it also needs foundational work that provides longer-term holistic system solutions. Reducing risk through the energy infrastructure will require the rallying of government organizations, national laboratories, industry and industry trade groups, other research organizations, and academia working together as a team towards a common outcome. This teaming will require commitment, trust, resources, and leveraging of each partner's unique roles and strengths. The nation needs increased investment in long-term over-the-horizon research and development addressing holistic solutions that fundamentally reduce the system risk to our energy infrastructure.

An example of a significant step forward in partnering within national laboratories to address the national control systems cybersecurity challenge, INL, Pacific Northwest National Laboratory, and Sandia National Laboratories are teaming to lead a research initiative that holistically addresses control system cybersecurity. This initiative will: 1) provide a forum to focus government and other research investments on solving the control systems cybersecurity research challenges found within the most common control systems that have great potential for high-consequence; 2) advance the fundamental science and engineering needed to develop and implement cybersecure control systems; and 3) integrate research, training and education to develop the national technical expertise and workforce capacity to support government and industry.

This initiative's success in enhancing the protection of critical infrastructure is dependent upon broad national support that enables the future priorities and resources for research programs; creates a current, anticipatory and actionable collaborative information-sharing environment; and implements adaptable, forward-leaning technologies, standards, policies and regulations.

Summary

I thank the Committee's members and fellow panel members for the honor of serving as a witness on this complex challenge, one that requires comprehensive action across technology, policy and regulation. Protection of the energy sector, as well as the other sectors of critical infrastructure, deserves our attention and commitment to assure our economic prosperity, national defense and public safety. INL welcomes its role in serving the nation as a unbiased technology 'broker' for protection of our critical infrastructure by developing and validating credible threats and their consequences; developing, testing and demonstrating the effectiveness of innovative security technologies; conducting experimentation that establishes the science- and engineering-based data to support policy; and performing the threat analyses and risk assessments that support industry's implementation of protective measures and regulatory actions.

The pace of the evolution of the threat balanced against the economic factors accelerating the implementation of advanced technologies calls for a unified team of stakeholders interested in addressing the challenge. This teaming includes government, researchers, vendors, asset-owners and regulators.

Your commitment to this hearing, the high quality of peers as my fellow witnesses, and your proposed legislative actions and appropriations for research, demonstrate that the nation is actively engaged in addressing this challenge.

Thank you for inviting me today to testify, and I look forward to your questions.