STATEMENT OF
MR. ZACHARY D. TUDOR, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES

OCTOBER 26, 2017

Mr. Zachary D. Tudor, Associate Laboratory Director, Idaho National Laboratory National and Homeland Security Directorate

U.S. Senate Hearing to receive testimony on advanced cyber technologies that could be used to help protect electric grids and other energy infrastructure from cyberattacks.

Chairman Murkowski, Ranking Member Cantwell, and distinguished members of the Committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on advanced technologies to protect the U.S. power grid and energy infrastructure from cyberattack. I appreciate the opportunity to address this Committee and express my utmost respect and gratitude for your leadership and continued interest in this topic.

I request that my written testimony be made part of the record.

I am the associate laboratory director for National and Homeland Security at Idaho National Laboratory, also known as INL. INL is responsible to the Department of Energy (DOE) to create, cultivate, and deliver future technology solutions that enable the realization of this nation's strategy for secure energy production and delivery. INL's role within the DOE laboratory complex provides great opportunities for influencing and executing an extensive government and industry portfolio of research, development and demonstration programs that address the cyber threats to the stability, reliability, and resilience of the nation's energy infrastructure. Also, with my role as a member on the Board of Directors of (ISC)^2 – the International Information Systems Security Certification Consortium – I have the opportunity to influence the strategy, governance, and oversight of certification for information security professionals around the world – some of whom are protecting the information and control system networks within our electric infrastructure.

The cyberattacks in 2015 and 2016 on the Ukraine power grid demonstrated that attacks on energy infrastructure can move very quickly and impact a wide variety of interdependent systems across a region. With recent high-profile events like Nuclear 17 and Palmetto Fusion within the U.S., it is obvious why utilities and regulators are concerned with increasing burdens caused by more sophisticated and frequent cyber events – during which they must have capabilities and skills to detect and respond to an attack before it causes an unacceptable impact. Due to the multifaceted interdependencies of the grid with other critical infrastructure, the breadth of technologies and systems that make up our energy infrastructure, and the speed and sophistication of a cyberattack, protection of the grid and energy infrastructure from cyberattack is one of our most complex technical and operational challenges. To increase confidence in our ability to protect the grid and energy infrastructure, the U.S. must continue to pursue research and development, demonstration at scale, and deployment of solutions from all sources of innovation, including industry, universities, and national laboratories. *These solutions will be realized through deployment of advanced technologies, implementation of enhanced engineering and operational processes, and development of a highly skilled and well-informed workforce.*

The U.S. requires unique capabilities to solve the most complex technical research and development challenges. The nation owns and invests in the Department of Energy's national laboratories to provide expertise and unique research and development capabilities to solve these difficult technical challenges. A recent example that illustrates our reliance on the Department of Energy and its national laboratories for protection of the grid and energy infrastructure is the March 14 letter from Senators Cantwell and Wyden to President Donald Trump urging the President to maintain the Department of Energy's leading role in defending our critical energy systems and networks as codified in the Fixing America's Surface Transportation Act (Public Law 114-94). Similarly, Senator King and co-sponsors Senators Risch, Heinrich, Collins, and Crapo drafted S. 79, the Securing Energy Infrastructure Act – legislation that emphasizes the development of a cyber-informed engineering strategy with the Department of Energy and national laboratories to defend energy infrastructure from vulnerabilities and exploits.

INL is the nation's lead nuclear energy national laboratory and is recognized as a national and international leader in control systems cybersecurity and grid resilience. INL advocates that effective grid and energy infrastructure protection will be achieved with not only advanced technology solutions, but with innovative engineering approaches, and a deep pool of top-tiered cyber defenders, scientists, and engineers. As such, INL is committed to and engaged in conducting the research, development, demonstration, and deployment of a broad range of holistic solutions that will have transformational and sustainable impact on the reliability and resilience of the grid and energy infrastructure. INL's commitment is showcased in an INL strategic initiative – the Cybercore Integration Center. The Cybercore Integration Center is focused on creating enduring national capabilities for control systems cybersecurity innovation with long-term objectives to:

- Transform the cyber-informed science and engineering within national research and innovation programs that solve the most complex cybersecurity challenges resulting from the convergence of cybersecurity with control systems, power, and wireless among critical infrastructure and national security systems.
- Develop multi-organizational partnerships to share research capabilities and real-time threat information on the most difficult national security challenges.
- Build the nationwide, multidisciplined expertise needed to sustain a superior control systems cyber workforce.

Successful implementation of the Cybercore Integration Center strategy includes partnerships and collaborations to leverage the researcher talent pool and unique research infrastructure within the national laboratories, industry, and universities. As an example, my national laboratory and industry peers who are participating in this hearing (i.e., Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and New Context) provide many unique capabilities, including those that are making technology breakthroughs in situational awareness, sensors, automation, modeling, simulation, and visualization.

A critical factor in achieving grid and energy infrastructure protection and resilience is taking a balanced approach to projects for advanced technologies, engineering processes, and workforce development. A balanced portfolio includes near-term, urgent solutions that can be rapidly developed, tested, and deployed for industry use, and the long-term, complex advanced technologies that must transition through the scientific peer-review process and technology maturation levels before they can be deployed. Whether solutions are developed for the near term or long term, research for protection of the grid and energy infrastructure should be based on real-world operational requirements and cybersecurity gaps.

INL has unique insight into these real-world operational requirements, because on any given day, INL experts can be found in multiple locations across the U.S. working with industry to protect the grid and other critical infrastructure. Multidisciplinary teams of cybersecurity, control systems, wireless, power management, and threat analysis are deployed to work collaboratively with power utilities, industrial product vendors, or other infrastructure asset owners. These teams enable discovery and analysis of gaps, such as the need for tools that provide effective and immediate assistance for incident response and recovery. Other gaps may lead to better defined requirements for a long-term solution that would eliminate future vulnerabilities and threats. INL's experts also uncover requirements during threat analysis briefings, cyber exercises and cyber training when we identify needs for improvements in information sharing and skills development.

With this technical and operational insight into near-term and long-term technology requirements, INL's Cybercore Integration Center is positioned to implement a research and development strategy that encompasses a broad spectrum of solutions for grid and energy infrastructure security. This strategy emphasizes that there is no single silver bullet solution; rather, solutions must address technologies, processes, and people. Cybercore Integration Center's priorities are a holistic research and development strategy, which pursues advanced solutions that, when deployed, enable stakeholders to implement sustainable, cyber-informed decisions that harden infrastructure against the most sophisticated cyberattacks and the most unacceptable consequences.

Advanced Technologies: Examples of INL's progress in research and development of advanced technology solutions for grid and energy infrastructure protection and resilience are provided in the following bullets. These technologies emphasize opportunities to employ multiple technology disciplines (sensors, information and decision science, wireless, network architectures, etc.) to provide the benefits of machine-to-machine speed and automation in responding to cyber intrusion or attack.

- Automated threat response for industrial control systems can result in improved capabilities to prioritize threats and exploits, reduce the time to discover and recover from illicit behavior, and increase resiliency of the electric grid. In collaboration with Lawrence Livermore National Laboratory, New Context, and the other industry partners of the California Energy Systems for the 21st Century (CES-21) Program, INL is conducting research with machine-to-machine automated threat response (MMATR) concepts and technologies. One essential concept within MMATR research is machine-readable Indicator and Remediation Language (IRL) generation. This concept will enable control system devices to have capabilities for early detection of abnormal behavior, and then with machine-speed, remediate an exploit before the exploit has an impact. This concept, as well as others for automated response capabilities are currently being tested on physical test beds consisting of actual utility grid controls and security equipment. INL's experimental infrastructure to test and demonstrate at-scale provides unique capabilities to measure and understand a new technology's performance through normal operations, equipment malfunctions, system degradations, and failure events.

- To address increasing demand for real-time cyber intrusion monitoring and immediate cyber event response, INL is pursuing a variety of autonomous technology solutions for protecting operational technology (OT) systems and networks (e.g., industrial control systems (ICS), programmable logic controls, supervisory control and data acquisition systems (SCADA), etc.). One of INL's innovations in cybersecurity automation includes the INL Autonomic Intelligent Cyber Sensor (AICS). AICS is an example of an OT tool that can be used to protect the grid and energy infrastructure by enabling system owners to more easily design, implement, and monitor cyber secure control system networks. AICS uses autonomic computing techniques and a service-oriented architecture to: a) automatically discover network entity information, b) automatically deploy deceptive virtual hosts (dynamic honeypots), and c) automatically identify anomalous network traffic with very high accuracy. The continued advancement of AICS towards deployment through DHS's Transition to Practice Program is an excellent example of maturing an INL Laboratory Directed Research and Development Program (LDRD) research project through the levels of technology readiness.

- The U.S. grid, energy infrastructure, and electric vehicles are evolving rapidly to rely more heavily upon wireless communication technologies. This increased reliance on wireless technology introduces the potential for vulnerable access points for malware intrusion into the electric grid and energy infrastructure. To explore potential wireless vulnerabilities and eliminate consequences from a wireless cyberattack, INL is performing wireless cyber research on a protection technology, WiFIRE, through our Laboratory Directed Research and Development (LDRD) Program. Researchers are making significant progress in the early stage research and proof-of-principle testing of a prototype for real-time monitoring of radiofrequency spectrum use and characterization of communication protocols. WiFIRE has the potential to serve as an early warning sensor for wireless-based cyber intrusion to assure the confidentiality, integrity, and availability of wireless communications. WiFIRE is being designed for the protection of approved for current and future radiofrequency spectrum allocations such as the allocations assigned for Smart Grid communications networks, electric vehicle wireless charging systems, and vehicle-to-vehicle (V2V) technologies. This technology also will have capabilities for next-generation wireless communication systems and the detection of illicit use of spectrum.

Advanced Engineering Processes and Operations: Examples of our progress in research and development of cyber-informed engineering protections of the electric grid and energy infrastructure are provided in the following bullets. These advancements enable asset owners and the operational defenders of critical infrastructure to assess their systems and operations to optimize their operational technology cybersecurity posture within their current and future systems by engineering in cyber secure designs and barriers, and engineering out vulnerabilities and attack pathways.

- Many asset owners are burdened with the unsustainable, day-to-day responsibility of detecting and responding to an increasing load of cyber exploits on their information technology (IT) and operational technology (OT) networks. Hence, INL developed Consequence-driven, Cyber-informed Engineering (CCE) to assist asset owners in understanding the actions they can take that will have the most beneficial impact in reducing risk to assets, operations and services/products. CCE provides asset owners with a methodology to implement an effective and efficient cyber investment strategy that is based on sound engineering principles and credible threats. The CCE guided methodology leads an organization through the steps required to protect their most essential processes from the most capable cyber adversaries. CCE fully leverages an organization's deep engineering expertise, including intimate systems and process knowledge, to engineer out the cyber risk with greatest consequence. The unique value of CCE is achieved when stakeholders complete the four-phase process: a) identify the highest consequence events; b) conduct a system of systems breakdown to identify all digital components and systems within the target environment; c) perform an ICS Cyber Kill Chain analysis to identify likely attack vectors and end effects, including assessment of current threat actors' capabilities; and d) prevent the high consequence event through cyber-informed engineering mitigations that disrupt the kill-chain. INL recently completed the initial pilot study of this advanced engineering process with a major U.S. electric power utility through a Cooperative Research and Development Agreement (CRADA). The pilot study was completed to mature the methodology and determine the potential value of CCE to assist utilities with assessing vulnerabilities and implementing solutions to cyber threats. With the discoveries and lessons learned of this first CCE pilot, INL is evaluating pathways to increase exponentially the availability and use of CCE through publications, train-the-trainer courses, and industry licenses. CCE results were briefed to the Section 9 electric utility partners and key U.S. intelligence community representatives. Intelligence threat analysts are evaluating the pilot study's findings, recommended mitigations, and lessons learned to determine if there are opportunities to enhance future threat analyses to protect grid and energy infrastructure.

- In support of the Department of Energy Office of Electricity Delivery and Energy Reliability's (DOE-OE) efforts to enhance grid and energy infrastructure security, INL is participating in multiple research initiatives with utilities. The goal is to enhance the value of cyber threat information sharing, and to expand information sharing for protection of operational technology (OT) networks. These initiatives focus on new analytical tools and information sharing approaches for the grid and energy infrastructure operators to determine what to monitor, how to collect and process data, and how to share sensitive data while protecting privacy. The results from these pilots will inform the development of a repeatable, standard approaches that the utilities across the entire electric grid enterprise can use for operational threat data sharing and analysis.

- The Controller Area Network Bus (CAN Bus) protocol integrates the controls for powertrain, battery charging, transmission, antilock braking, air bags, etc., for automobiles, air, rail and marine transportation. To advance secure use of the CAN Bus protocol for electric vehicle connections to the power grid, battery storage systems, and vehicle-to-vehicle (V2V) networks, INL researchers are performing research to improve the cybersecurity of CAN Bus hardware and software. Success with innovations in CAN Bus will significantly reduce the cybersecurity risks associated with the automated control systems within automobiles, heavy transportation vehicles, aviation systems, and large electric generators – particularly when these new protections remove risks inherent to vehicles connecting with the electric grid. INL researchers are transitioning CAN Bus innovations towards deployment as part of research supported by DOE's Grid Modernization Laboratory Consortium and DOE's Technology Commercialization Fund.

<u>Advances in Workforce Development:</u> INL experts seek novel approaches to improve the effectiveness of knowledge transfer and information sharing by developing novel immersive learning environment methods and tools. Within our program portfolios for DOE, Department of Homeland Security (DHS), and other federal organizations, INL experts are in high demand nationally and internationally to provide education and training to elevate cyber skills and provide cyber awareness through sharing real-world knowledge and experiences. Examples demonstrating the progress in advancing the Cybercore Integration Center's objective for developing highly skilled, multidisciplinary cyber defenders and researchers, include the following:

- In response to a DOE-OE request for INL to provide critical knowledge transfer to utility operators related to the Ukraine power grid cyberattack, INL researchers designed, developed, and prototyped unique hands-on training devices. These "Ukraine-Event-in-a-Box" devices are designed to challenge course participants to defend against cyberattack on the equipment these participants routinely encounter within their power generation systems and power distribution substations. INL is exploring opportunities to make these training systems readily available for university engineering laboratories and industrial control room simulators.

- As part of collaborative university research in control system cybersecurity with the University of Tulsa, INL researchers developed a specialized educational tool. The credit-card-sized board is used as a cyber-skill teaching and assessment tool. This board includes various environmental sensors, data storage, input mechanisms and screen display features to develop expertise in forensic analysis. To increase access to students, INL is evaluating the potential for open source release of the board's proprietary control software.

- INL and DHS provide the ICS-CERT ICS Cybersecurity (301) control systems technical level training course for industry, government, and university participants. For over a decade, this first-of-its-kind course has provided over 4,000 participants with hands-on training to discover who and what is on the network, identify vulnerabilities, understand how those vulnerabilities may be exploited, and learn defensive and mitigation strategies. This course includes a Red Team/Blue Team exercise that takes place within an actual control systems environment, and continuously evolves to address new learning methods, evolving threats, and protections.

- INL is partnering with educational institutions across the state of Idaho to build a pipeline for the future control systems cybersecurity expertise. INL, in collaboration with Idaho's three research universities, conducted a Cybercore summer camp – a three-day camp that provided high school students with hands-on experience using various ethical hacking techniques and methods. INL also assisted the University of Idaho in creating a graduate certificate in Critical Infrastructure Protection. This new graduate certificate, available in fall 2017, will educate current and future technology management, engineering, and computer science students on the challenges of protecting U.S. critical infrastructure.

The examples described within this testimony are provided to emphasize INL's progress in developing and deploying advanced technology solutions and to emphasize the key principles of the INL Cybercore Integration Center's holistic research and development strategy for control system cybersecurity innovation. These principles emphasize solutions focused on the development of the technologies, processes, and people required to protect electric grids and other energy infrastructure from cyberattacks. The principles include: a) multiple advanced technology innovations are needed when we are threatened by a sophisticated cyber-threat actor; b) advanced technologies that focus on autonomous detection and mitigation will be more readily accepted when stakeholders benefit from reductions in the costs and labor of cybersecurity, and the solutions provide timely and effective detection and mitigation of cyberattacks; c) advanced engineering technologies should enable cyber-informed design of processes, operations, and systems that have engineered-in cyber protections and engineered-out cyber vulnerabilities; d) advanced solutions must support the building of a nationwide, multidisciplined control systems cybersecurity workforce; and e) effective solutions should be based upon peer-reviewed science, use sound engineering principles and standards, and be tested and validated at-scale. INL encourages collaborations and partnerships because advanced technology solutions will arise from all sources – industry, entrepreneurs, academia, government, and laboratories.

I thank the Committee's members for this opportunity to share our strategy and provide examples of the progress we are making in meeting the dynamic evolution and technical complexity in identifying and mitigating threats to the electric grids and energy infrastructure. Your strong support for discussions of the opportunities and benefits of long-term research and development will result in effective and sustainable solutions. The written examples of our progress along with continued technology development from many others will lead to the solutions needed to protect the U.S. power grid and energy infrastructure from cyberattack. You have my commitment that INL will continue to pursue the realization of DOE's and INL's mission and strategy to meet the national objectives for protection of the grid. Thank you.