**STATEMENT OF**

**MR. ZACHARY D. TUDOR**

**ASSOCIATE LABORATORY DIRECTOR**

**NATIONAL & HOMELAND SECURITY**

**IDAHO NATIONAL LABORATORY**

**BEFORE THE**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**ENERGY AND COMMERCE COMMITTEE**

**SUBCOMMITTEE ON ENERGY**

**March 14, 2018**

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

**U.S. House of Representatives Hearing to receive testimony on "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response"**

Chairman Upton, Ranking Member Rush, and distinguished members of the committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on the Department of Energy (DOE) cybersecurity and emergency response. I greatly appreciate the opportunity to address this committee and thank the members for your commitments and legislative decisions to assure that our national energy supply is reliable, resilient and protected.

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 one of 17 DOE national laboratories and is DOE's 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. In my role at INL, I have the pleasure and responsibility to lead, influence and execute a broad portfolio of research programs which address the cyber and physical protection, and emergency response for critical infrastructure, with an emphasis on the Energy Sector.

In passing the Fixing America's Surface Transportation (FAST) Act in 2015, Congress provided authorities for the DOE to be the Sector-Specific Agency for cybersecurity for the Energy Sector. The impact of your actions and your priorities that called for today's hearing reflects our mutual understanding that our nation faces persistent, capable, well-resourced, and highly motivated cyber adversaries. These adversaries continue to develop the skills, technical capabilities, and opportunities for potential compromise of the equipment, systems, networks, and facilities that constitute our nation's power grid and energy infrastructure. The potentially unacceptable consequences of a sophisticated cyberattack create an imperative for us to do all we can to demonstrably reduce cyber risk.

Beyond cyber, our national grid also is challenged with the complex realities of real-time operations and the accelerated introduction of intelligent and interconnected technologies. These technologies enable: a) integration of bulk power generation with distributed renewables; b) automated management of electricity transmission and distribution systems that support our cities and rural communities; and c) network communications to balance supply and demand, and support recovery during disasters. These innovations are critical to managing a modern and resilient operational environment, yet also increase the risks to the critical control systems throughout the Energy Sector.

After two years in my leadership role with a national laboratory, I have seen first-hand the

critical capabilities DOE is providing for the nation to reduce these risks and execute as the Energy Sector-Specific Agency for protection, coordination and response. These critical capabilities include a broad array of science and engineering programs, extensive teams of multidisciplinary national laboratory researchers, unique user facilities and test beds for experimentation "at scale," and a breadth of collaborative public-private relationships with industry, universities, and federal agencies. Because of these capabilities, DOE will continue to reduce the risks for the Energy Sector and support other federal authorities when their assigned sector has high potential for significant consequences due to the Sector's dependencies upon energy systems (e.g., oil and gas pipelines, transportation fuels, dams, defense manufacturing, etc.)

INL supports the DOE in achieving the intentions of the FAST Act's legislative direction to coordinate with the Department of Homeland Security (DHS), other federal organizations, and critical electric infrastructure stakeholders in *"…providing, supporting, and facilitating technical assistance and consultation for the Energy Sector to identify vulnerabilities and help mitigate incidents…*" We do this through performing cutting-edge energy system research, developing and sharing cyber and physical threat information, and conducting cyber and physical security assessments – all with the objectives of assuring our energy security and reducing risks to our critical infrastructure.

Often, our experts work with industry to implement solutions and provide guidance in partnership with government and private stakeholders who are encountering the realities of keeping real-world systems functioning while defending against significant risks. These "eyes-on-target" experiences allow INL to prioritize better the building of capabilities and focus research on the most relevant challenges. These priorities are continuously validated and updated as a result of discussions with DOE, our research partners, and a wide range of infrastructure stakeholders. Some recent discussions included: a) Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) from the Section 9 utilities and the California Energy Systems for the 21st Century; b) cybersecurity researchers at universities such as the state of Idaho's three research universities, Texas A&M University, the University of Texas at San Antonio, the University of Tulsa, New Mexico Tech and North Carolina State University; c) peers at national laboratories such as Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories; and d) senior government officials from DOE, Department of Defense (DoD), and DHS.

With the remainder of today's testimony, I will update you on some of the progress INL continues to make with innovations that have opportunities for immediate and sustainable impact in reducing security risks. I will highlight INL's support, synchronized with other DOE national laboratories, that will enable the success of the new DOE Office of Cybersecurity, Energy Security and Emergency Response (CESER) in achieving its mission to improve the Energy Sector's preparedness for and ability to respond to cyber and physical threats. I also will discuss examples of the partnerships and collaborations that will support the development of coordinated strategies for science and technology research and operational preparedness and response among DOE, DHS, and other stakeholders.

With regard to reducing cyber risks, I, and many of my colleagues at other national laboratories, am keenly focused on sharing threat and vulnerability information with

stakeholders by developing analytical reports and advisories that confirm the status of threats to our power grid and energy infrastructure. Through INL's Cybercore Integration Center, referred to as Cybercore, we perform research, development, testing and evaluation of technologies that can prevent, detect, and mitigate vulnerabilities and intrusions. These technologies can create barriers that minimize attack pathways, mitigate the consequences of an attack, and effectively restore functionality. Cybercore inherently differentiates itself from individual programs and specific products by focusing on holistic emphasis of integrated, engineered solutions focused on cyber-informed technologies and processes, and cyber-prepared people.

Examples of Cybercore and other relevant technology advancements that are reducing risks for energy systems include and are not limited to:

- With DOE and multiagency support, INL experts supported recovery and information sharing following the cyberattack on the electric grid in the Ukraine in 2015 and 2016. As a result of our post-event analyses and discoveries, INL developed and is conducting "Cyber Strike" Workshops for U.S. asset owners and operators to provide awareness and operations training that foster better protection of electrical utilities from similar attacks. During the next few months, with DOE Office of Electricity Delivery and Energy Reliability sponsorship, INL staff will conduct Cyber Strike Workshops for over 400 individuals who work at electrical utilities in Florida, Georgia, and California. This information-sharing effort harnesses INL's proprietary training equipment and face-to-face interactions with our leading researchers and analysts to prepare these private utilities with the tools and techniques to guard against and respond to cyber events. In the future, this outreach will include more energy system stakeholders, including organizations within the oil and gas industry. An example of the typical feedback received from an industry attendee of a Cyber Strike Workshop: *"…It really highlighted the importance of not only having a very solid cybersecurity program, but also the vigilance that is needed from employees to help prevent unwanted intrusion. Everyone said this training was very eye-opening and has changed the way they think about protecting their information in the cyber world…*"

- INL developed and completed an initial pilot study of our proprietary Consequence-driven, Cyber-informed Engineering (CCE) methodology with Florida Power and Light (FPL) through a Cooperative Research and Development Agreement (CRADA). CCE was developed to address the realization that constantly "chasing" threats and vulnerabilities, rather than getting ahead of these problems, is not sufficient to secure our critical systems. CCE is designed to assist asset owners in understanding the most effective and immediate actions they can take to eliminate the opportunity of the "worst-case" cyber-physical impacts from an attack by the most capable cyber adversaries. CCE leverages an organization's knowledge and experiences with their systems and processes to "engineer out" the potential for the highest consequence events. This study was completed to mature the methodology and demonstrate the potential value of CCE to assess vulnerabilities and implement solutions. Briefings of the study's results were shared by a team of researchers and executives from INL and FPL for the Section 9 electric utility partners, and key government leaders. These briefings included separate sessions with U.S. Senate and House of Representative staffers from the energy and

intelligence committees of the Senate, and with the DOE Office of Electricity Delivery and Energy Reliability senior official Pat Hoffman and Assistant Secretary Bruce Walker. A second pilot study of CCE is underway with a military organization, and INL is advising the National Security Council on approaches to implement CCE to a broader set of participants across the U.S.

- Over the last 12 months, INL teamed with DHS in providing technical threat analyses, mitigations, advisories, and field assessments. Hundreds of products and assessments were performed to reduce cyber risks across all 16 critical infrastructure sectors, including Energy, Water and Wastewater, Dams, Commercial Facilities, Government Facilities, Critical Manufacturing, Transportation, and Food and Agriculture. INL supported DHS in the development and advancement of an interagency Aviation Cyber Initiative (ACI) to identify and mitigate cyber vulnerabilities in the nation's aviation systems. Cybersecurity assessments with airlines, airports, and avionics manufacturers have been underway for over two years, including cooperation with the Federal Aviation Administration's Next Generation Air Transportation System (NextGen) cyber risk analysis efforts.

- INL's capabilities also are being applied to provide solutions to a broader range of physical and electromagnetic threats. Recent experimentation conducted through our Laboratory Directed Research and Development projects and DOE-sponsored exploratory science projects provides opportunities for new solutions in: a) protective armor for defending substations against high-caliber ballistic threats similar to what occurred at the Metcalf Transmission Station in California; b) high-fidelity modeling and visualization of grid response and interdependent infrastructure behavior during intermittent renewable generation and natural disasters; and c) transformer survivability during electromagnetic pulse attack or geomagnetic disturbance events.

INL is one of several national laboratories collaboratively contributing technical information and strategic planning guidance to assist DOE leadership in the early stages of developing the structure, capabilities and processes for the DOE Office of Cybersecurity, Energy Security and Emergency Response (CESER). Guidance is focused on the coordinating and integrating research, development, and incident response capabilities among the multiple programs and organizations within the DOE and other federal organizations. Examples include:

- *Providing principles for establishing a CESER RD&D portfolio that delivers impactful solutions in response to cyber and all hazard threats.* These principles can guide CESER in focusing on the development and operationalization of next-generation cyber and situational awareness tools for real-time response by leveraging the cutting-edge energy research for transmission, distribution and storage resulting from the DOE Office of Electricity Delivery and Energy Reliability Grid Modernization Laboratory Consortium.

- *Providing principles for including security-informed design into future grid infrastructure.* CESER will be able to reduce future cyber risks to energy infrastructure by coordinating and integrating "engineered-in" cyber-physical protections into future advanced energy systems (e.g., DOE Office of Nuclear Energy research on advanced reactor designs and

fuel cycle facilities; DOE Office of Energy Efficiency and Renewable Energy programs for electric vehicles connecting to the grid, etc.).

- *Providing guidance on best practices for developing processes and procedures for coordination with incident response* with the DHS U.S. Computer Emergency Readiness Team, the DHS National Cybersecurity and Communications Integration Center Hunt and Incident Response Team, U.S. Cyber Command, etc. Recent recovery efforts in Puerto Rico; responses to the Ukraine grid attack, Nuclear 17, and Palmetto Fusion; and participation in national exercises (e.g., GridEx, Liberty Eclipse, etc.) provide CESER with access to a tremendous pool of expertise to advance the realism and effectiveness of our future efforts for preparedness and response.

INL's track record of successful development and deployment of technical innovations is a result of an emphasis on collaborating, partnering, and sharing of experts and experimental facilities. This approach accelerates the maturation of technologies and methodologies from the conceptual to deployment stages; optimizes the benefits of leveraging investments in expertise, research programs, and technology development infrastructure; and creates effective environments for immediate information sharing of discoveries and emerging threats. Based upon our experiences, we included the formation of new multiorganizational partnerships as a major priority to achieve the Cybercore vision of creating the enduring national capabilities for control systems cybersecurity innovation. Examples of current partnerships that are enhancing national capabilities are:

- INL, Pacific Northwest National Laboratory, and Sandia National Laboratories comprise the three laboratory Cybercore collaboration, CyberPARC (Partnership for Advancing Resilient Controls), which is creating a collaborative environment among the labs to advance the science and engineering of cyber-physical systems to create resilient, self-healing control systems.

- In collaboration with the electric industry partners of the California Energy Systems for the 21st Century Program, INL and Lawrence Livermore National Laboratory are conducting research with machine-to-machine automated threat response (MMATR) concepts and technologies.

- Cybersecurity for the Operational Technology Environment (CYOTE), a DOE-OE pilot project supported by INL, facilitates situational awareness in operational technology (OT) networks, and information sharing and coordination among industry partners and stakeholders, while providing an adaptable forum for development and testing of scientific innovations that have potential to advance grid resilience and security.

The examples I have described demonstrate that DOE and INL are making significant progress in reducing the risks to our nation's energy infrastructure. Although we can minimize but not eliminate the risk, we must redouble our efforts in technology innovation; multiorganizational cooperation, coordination, and integration; and prioritization of funding and focus for research programs. Therefore, I emphasize that based on our current understanding of the threats to our Energy Sector infrastructure, we must aggressively continue to pursue programs to assure our energy, economic and national security. I thank the committee

members for this opportunity to discuss national cybersecurity challenges and to share the burden in creating a path forward that protects the U.S. Thank you.