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

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
SCIENCE SUBCOMMITTEE ON ENERGY
AND
SCIENCE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OCTOBER 21, 2015

Chairman Weber, Chairwoman Comstock, Ranking Member Grayson, Ranking Member Lipinski, and distinguished members of the Committees; I want to thank you for holding this hearing and inviting testimony from Idaho National Laboratory, also known as INL.

INL is acutely aware of the important national challenges facing critical infrastructure, especially the infrastructure vital to securing our energy supply. For over a decade, INL has developed and built capabilities focused on the control systems employed by our nation's critical infrastructure. This includes conducting research in the science and engineering of our electric power transmission and distribution systems. INL has the strong benefit of completing full-scale, real-world tests of technology solutions to validate and improve grid modeling and simulation.

I would like to highlight a few examples, out of many, which represent how INL has contributed to the security of our infrastructure:

1. The 2006 Department of Homeland Security's (DHS) Aurora project test, destroying an electrical generator connected to INL's power grid, was significant in proving a cyber-physical vulnerability in the electric power system.
2. For DOE Office of Electricity Distribution and Energy Reliability (DOE-OE): As the lead laboratory, along with Sandia National Laboratory, for the National Supervisory Control and Data Acquisition (SCADA) Test Bed, INL completed more than 100 assessments on vendor and asset owner control systems to identify and resolve cyber vulnerabilities.
3. For the Department of Defense: INL contributes research experimentation results and provides access to our full scale power grid test bed to characterize and improve models for understanding and mitigating the impacts of geomagnetic disturbance.
4. For DHS: INL provides control systems and critical infrastructure experts in support of DHS programs, including the Industrial Control System Cyber Emergency Response Team (ICS-CERT) Program and Regional Resilience Assessment Program (RRAP). This includes analysis of threat information, training of critical infrastructure owners and operators, assessing the security and resilience of infrastructure systems, and identification of infrastructure dependencies/interdependencies within a region.

INL has been and remains committed to the complex national security challenges that face our nation. As we lean forward pushing the limits of science and engineering for control systems security, we see a number of trends that offer insight into the direction for future research and development.

These insights include:

1) The presumption that a control system is "air-gapped" is not an effective cyber security strategy. This has been demonstrated by over 600 assessments.
2) Intrusion detection technology is not well developed for control system networks; the average length of time for detection of a malware intrusion is four months and typically identified by a third party.
3) As the complexity and "interconnectedness" of control systems increase, the probability increases for unintended system failures of high consequence - independent of malicious intent.
4) The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy.
5) The demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.

In a world in which we are rapidly migrating to the Internet of Everything, these insights, and others, highlight a seemingly unmanageable, exponentially increasing burden of vulnerabilities, attack surfaces and interdependencies.

INL views this burdensome and dynamic cyber-physical landscape, at its most basic level, as a three-tiered pyramid of defense. The base level is hygiene – the foundation of our nation's efforts, composed of the day-to-day measure and countermeasure battle. Elements of this level include important routine tasks such as standards compliance, patching, and password management. The hygiene level is and has been primarily the role of industry, with both vendors and asset owners participating. The second level of the pyramid is advanced persistent threat - composed of the more sophisticated criminal and nation state persistent campaigns. This level requires a strategic partnership with industry and government and, as such, it is important to note that these roles are still evolving. At this level, ICS-CERT provides critical surge response capacity and issues alerts of current vulnerabilities to the government and asset owners. At the top of this pyramid are the high impact low frequency events - catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from. This level is primarily the responsibility of the government. At INL, we are focusing our future research on the top two levels, striving for a two to four year research-to-deployment cycle. Our objective with this research is to achieve transformational innovations that improve the security of our power infrastructure by reducing complexity, implementing cyber-informed design, and integrating selected digital enhancements.

As the recognized leader in this field, it is our opinion that the risks and benefits of cyber exploitation of control systems require that the U.S. build and maintain a strategic, coordinated, technologically superior capability and capacity for control systems research, development, demonstration and deployment. To help catalyze the nation to meet this requirement, INL continues

to invest in control systems innovation. Evidence of the high demand for this capability is demonstrated by the large variety of strategic partners – all agreeing that the nation has an immediate need for high performance research and response teams. Our focus is on experts, students, and trainees continuously mastering control systems cyber skills through learning, experimentation, operation, and competitive experiences. Of particular emphasis is the INL's focus on specialization in solutions based on cross functional teams (e.g. cyber, safety, operations, power, communications, etc.), 'out-of-band' innovations, and cyber-informed engineering designs. As an example, INL is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets. Using INL's significant power and communications infrastructure to analyze technology and infrastructure interdependencies, teams will explore the viability of: 1) insertion of analog attack surface disruption zones, such as custom analog circuits printed at low cost with 3D printer technology, inserted between the control network and the ultimate physical process system being targeted; and 2) pruning down unnecessarily complex systems to the bare minimum process requirements, thereby dramatically reducing the attack surface open to attackers.

In conclusion, I would like to thank the Committees' members for this opportunity to share our insight on the capabilities, experiences, and vision for cybersecurity and the protection of our nation's power grid. The dynamic evolution and technical complexity of the threats demand visionary, multifaceted science and leadership solutions. Your interest in understanding cybersecurity threats with an emphasis on the reliability of our national power grid is commendable and gives me confidence that there is strong support from our legislators for research leading to innovative solutions. One of my intentions today with this testimony is to instill reciprocal confidence that INL, in concert with DOE and other DOE laboratories, will continue to apply our intellectual talent and research to address these challenges. In honoring the time allotted for my statement, I request that my full written statement be entered into the record. Thank you.

SUMMARY

STATEMENT OF
MR. BRENT J. STACEY, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY
IDAHO NATIONAL LABORATORY
BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
SCIENCE SUBCOMMITTEE ON ENERGY
AND
SCIENCE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OCTOBER 21, 2015

As the recognized leader in this field, it is our opinion that the risks and benefits of cyber exploitation of control systems require that the U.S. build and maintain a strategic, coordinated, technologically superior capability and capacity for control systems research, development, demonstration and deployment. To help catalyze the nation to meet this requirement, INL continues to invest in control systems innovation. Evidence of the high demand for this capability is demonstrated by the large variety of strategic partners – all agreeing that the nation has an immediate need for high performance research and response teams. Our focus is on experts, students, and trainees continuously mastering control systems cyber skills through learning, experimentation, operation, and competitive experiences. Of particular emphasis is the INL's focus on specialization in solutions based on cross functional teams (e.g. cyber, safety, operations, power, communications, etc.), 'out-of-band' innovations, and cyber-informed engineering designs. As an example, INL is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets. Using INL's significant power and communications infrastructure to analyze technology and infrastructure interdependencies, teams will explore the viability of: 1) insertion of analog attack surface disruption zones, such as custom analog circuits printed at low cost with 3D printer technology, inserted between the control network and the ultimate physical process system being targeted; and 2) pruning down unnecessarily complex systems to the bare minimum process requirements, thereby dramatically reducing the attack surface open to attackers.