STATEMENT OF

MR. ANDREW A. BOCHMAN, SENIOR CYBER AND ENERGY STRATEGIST
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES

APRIL 4, 2017

Mr. Andrew A. Bochman, Senior Cyber and Energy Strategist, Idaho National Laboratory National and Homeland Security Division

U.S. Senate Hearing to receive testimony on examining efforts to protect U.S. energy delivery systems from cybersecurity threats

Chairman Murkowski, Ranking Member Cantwell, and distinguished members of the Committee, I thank you for holding this hearing and inviting Idaho National Laboratory's testimony on the protection of our energy delivery systems. This topic is highly relevant and your attention to this issue will have a long-term impact on our energy, economic, and national security. I am the Senior Cyber and Energy Security Strategist at Idaho National Laboratory, also known as INL, and in this capacity I provide guidance to Department of Energy, or DOE, and INL leadership on matters related to protecting the nation's energy infrastructure against mounting cyber and physical threats. These threats include current threats of which we are aware and future threats that we envision and anticipate. I am honored to participate and request that my written testimony be made part of the record. .

As one of DOE's national laboratories, INL is missioned to be a leader in technology research, development, demonstration, and deployment for critical infrastructure protection. As such, INL is at the forefront of U.S. and international control systems cybersecurity and grid resilience research. We also 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 to the Smart Grid; add new energy sources, storage, and consumers; and encounter potentially high consequence impacts from the effects of Geomagnetic Disturbance (GMD), Electromagnetic Pulse (EMP) and other natural and man-made phenomena.

I am just returned from a United States Agency for International Development-funded trip to Estonia where I joined a team of U.S. state-level energy regulators, led by the National Association of Regional Utility Commissioners (NARUC), training Baltic & Black Sea energy commissioners on cyber security issues.

As you may know, Estonia is first country to suffer a large scale cyberattack against its critical government and commercial infrastructures. Estonia is located within a region where several other countries have been victims of cyberattacks on critical infrastructures. Recently, INL provided experts on the U.S. delegation that assessed the cyberattack on the Ukraine power grid and assisted the SANS training institute issuing of a summary report on the attack and subsequent recommendations for further protections. The possibility of attacks like these or worse have been the focus of DOE, INL, and some of your colleagues. Senators Cantwell and Wyden, who in a March 14 letter to President Donald Trump, urged the President to maintain, as the Fixing America's Surface Transportation, or FAST Act, to codify - DOE primacy over grid

security matters. And earlier, heightened concerns over cyberattacks on energy systems motivated Senators King and co-sponsors Senators Risch, Martin, Collins and Crapo to draft S. 79, the Securing Energy Infrastructure Act.

The average person may wonder: "Why all this activity now?" I would state that it's being driven by what has happened in the past, including the now-daily drumbeats of successful cyberattacks on U.S. government and private sector systems. But, in particular it is also about what cybersecurity experts see looming in the future. Manufacturers' zeal to embed new technology in industrial products, a trend which goes by the name Industrial Internet of Things (IIoT), and an eagerness to buy and install these products in energy infrastructure applications, means that, despite the cybersecurity community's best reactive efforts, attackers are going to penetrate energy systems, and utilize the complexities of "bolt on" cybersecurity measures to develop more attack path options than ever before. Cyber risk futurists, myself included, are experiencing a palpable sense of foreboding, never more so than when I study the current state of cyber-measure and cyber counter-measure activities. In the mix are market forces which may value efficiency, automation and autonomy to the detriment of security.

Even while acknowledging all of this contextual background, I can assure you that in my role with the Department of Energy, I daily gain confidence in our capability and capacity to overcome this condition and resolve significant energy infrastructure cybersecurity challenges. DOE, INL and our peer national laboratories are working these challenges via multiple strategy, policy and programmatic pathways. Though not exhaustive, I will describe a few of the relevant and impactful examples in which INL is serving DOE as a strategic and technical leader in the protection of the nation's energy infrastructure:

- DOE's Office of Electricity Delivery and Energy Reliability (DOE-OE) cyber threat intelligence and information sharing program, Cybersecurity Risk Information Sharing Program, or CRISP, is currently in place at dozens of U.S. utilities and efforts are underway to substantially improve both the timeliness and effectiveness of the security warnings they receive. Also, the DOE-supported California Energy Systems for the 21st Century (CES-21) program's Machine-to-Machine Automated Threat Response (MMATR) project has strong potential to accelerate alerts for specific categories of threat information to near real time.

- DOE-OE is investing over $15M in a new power grid test bed at INL focused on research, testing, and demonstration of technologies intended to protect substations and power transmission systems from both physical and cyber threats. As part of this investment, public utilities are adding more than $500K of additional equipment for further research as part of the DOE Grid Modernization Laboratory Consortium (GMLC) and Cybersecurity for Energy Delivery Systems (CEDS) programs. These investments enable cooperative cybersecurity research with universities and industry. Recent examples include cyber vulnerability discovery research with the University of Louisiana Lafayette on an electric vehicle charging station and development of cyber protection

devices with auto manufacturers.

- The DOE Office of Nuclear Energy (DOE-NE) has initiated research projects focused on nuclear energy cybersecurity, performing research intended to produce the scientific data serving as the basis for cost effective cybersecurity technologies and practices. These projects will enhance cybersecurity within our current and future nuclear power plant fleet, research reactors, future reactor designs and nuclear fuel cycle facilities. These research projects include INL, three other national laboratories (Sandia National Laboratory, Pacific Northwest National Laboratory and Brookhaven National Laboratory), the Electric Power Research Institute (EPRI), and several universities (including competitive awards granted at North Carolina State University, the Ohio State University, and Tulsa University). DOE-NE also has awarded three Phase I and one Phase II nuclear-cybersecurity grants within the DOE Small Business Innovative Research Program.

- In the spirit of Senator King's Securing Energy Infrastructure Act, INL and industry partners are on the home stretch of a threat-informed, engineering-centric assessment and mitigation activity at a very large U.S. utility. We call this approach Consequence-driven Cyber-informed Engineering, or CCE for short. The methodology reprioritizes the way we look at high-consequence risks within control systems environments. Lessons harvested from this initial pilot will be shared with research partners to greatly expand the nation's ability to "engineer out the cyber risk" from our most critical energy infrastructure networks and systems. Further reducing risk will require government, research and industry working toward a common goal complemented by investment in over the horizon research and development.

- INL supports the North American Electric Reliability Corporation and its biennial multi-sector North American Grid security exercise, GridEx, by creating extremely realistic "inject" artifacts that show energy systems operating incorrectly due to cyberattacks. INL experts routinely participate in many other national exercises, including the recent Cascadia Rising.

- Recent internal INL research investments include more than $5M in investments over the last two years in cybersecurity equipment, laboratories, and research related to energy security issues. Research topics address a wide range of energy-cyber relevant topics, such as: vehicle cybersecurity for battery charging, vehicle command and control communication protocols, and vehicle-to-vehicle automation communications; threat actor analyses; grid cybersecurity, geomagnetic disturbance (GMD) and electromagnetic pulse (EMP) threats against the grid; interdependency analysis; futuristic cyber-resilient systems and architectures; cyber reverse engineering; and cyber forensic tools. Aligned with these internal investments, the State of Idaho recently approved up to $90M for two new research facilities on the INL campus. One of those facilities, the Cybercore Integration Center, will support INL and Idaho universities' cyber and information

sciences research, education and training for DOE, other government, university and industry.

- DOE-OE's Infrastructure Security and Energy Restoration (ISER) organization, is the seat of the department's Sector Specific Agency (SSA) authority for all hazards, including cyber, to energy infrastructure. INL and PNNL are supporting the buildout of ISER's Incident Response & Coordination capabilities in conjunction with the Department of Homeland Security, North American Electric Reliability Corporation's Energy Information Sharing and Analysis Center (E-ISAC) and other grid security stakeholder organizations.

- Lastly, INL has supported ISER as it convenes the energy sector's Section 9 energy companies -- those previously identified in the 2013 Executive Order on Improving Critical Infrastructure Cybersecurity -- as serving, "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effect on public health or safety, economic security, or national security." Among specific capabilities requested are some of the items I just described. In addition, there is a call for a multi-lab environment where energy sector systems, both legacy and next generation, can be analyzed from a threat-informed cybersecurity vantage point, with specific mitigation actions shared securely, not merely among the labs and equipment suppliers, but with the asset owning utilities as well.

Before closing, I would like to emphasize a couple of DOE and INL grid protection leadership principles shared during prior testimony of INL representatives. Specifically:

- 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.

- 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. DOE, INL and other national laboratories identified this challenge and are making great strides in assembling and implementing long-term leadership and research plans to address the highest consequence scenarios, while building the expertise and experimental infrastructure to deliver sustainable, long-term capacity, and solutions.

- While we are catching-up with incremental improvements to harden our defenses and better detect and respond to a cyberattack, we will make progress to 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.

- At INL, we believe that unexplored options exist for taking consequences off the table. To this end, INL is accelerating our implementation of a transformative methodology we call “Consequence-driven Cyber-informed Engineering” that seeks and identifies high-consequence risks within the cybersecurity-industrial control systems environment. This process starts with identifying the highest impact, most severe consequences and then discovers the best process design and protection approaches for engineering out the cyber risk.

Thank you very much for the opportunity to provide testimony on this critical issue. INL is proud to take on this challenge and has much gratitude in similar resolve and commitments we see from you, DOE and our collaborative partners to protect our energy systems. Thank you for inviting me today to testify, and I look forward to your questions.