Statement of Carl Imhoff
Manager, Electricity Market Sector
Pacific Northwest National Laboratory

Before the
United States Senate
Committee on Energy and Natural Resources

October 26, 2017

Good morning. Thank you, Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee. I appreciate the opportunity to appear before you today to discuss advanced cyber technologies to protect the electric grid and other energy infrastructure from cyber-attacks, and issues and opportunities in this area.

My name is Carl Imhoff, and I lead the Grid Research Program at the Pacific Northwest National Laboratory (PNNL), a U.S. Department of Energy (DOE) national laboratory located in Richland, Washington. I also serve as the Chair of DOE's Grid Modernization Laboratory Consortium, a team of national labs that, along with industry, industry groups such as the Gridwise Alliance and the Electric Power Research Institute, and university partners, supports the Department's Grid Modernization Initiative. The consortium members include PNNL, the National Renewable Energy Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, Idaho National Laboratory, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, the National Accelerator Laboratory at Stanford, National Energy Technology Laboratory, Oak Ridge National Laboratory, Sandia National Laboratories, and Savannah River National Laboratory.

I will address two main points today:

1. PNNL and industry, via the North American Electric Reliability Corporation (NERC) Electricity Information Sharing and Analysis Center (E-ISAC), have made important progress in establishing information sharing capabilities for grid business information technology (IT) infrastructures, which provides cyber risk situational awareness for utilities and covers 75 percent of U.S. electricity generation. This effort will continue to broaden grid situational awareness for both the operational technology (OT) control systems of utilities in combination with IT systems, ultimately delivering enhanced, complete cyber situational awareness for the power system.

2. Fundamental science and technology offer important opportunities to complement cybersecurity situational awareness with improved defensive tools spanning the growing challenges at both the grid edge and core grid operations.

Background

For more than two decades, PNNL has supported power system reliability, resilience and innovation for Washington State, the Pacific Northwest, and the nation. During this period, the laboratory has:

1. Led DOE-industry collaborations in developing and deploying synchrophasor technology to help avoid blackouts. Phasor measurement unit networks are designed to enhance situational awareness of wide area systems. This new grid tool has demonstrated value by detecting impending system control and equipment faults for system operators, thus avoiding major outages. California estimates $360 million in annual savings to customers due to avoided outages, plus $90 million in annual savings in improved utilization of existing generation and delivery systems. This high performance monitoring system provides the basis for a new tool, developed in partnership between the Electric Reliability Council of Texas (ERCOT) and DOE, to better analyze complex blackout scenarios to that lead to improved design of resilient grid upgrades that resist cyber and other threats.

2. Gained significant experience leading effective public-private partnerships. For example, PNNL led a collaboration with utilities and vendors to develop and demonstrate transactive control concepts on the Olympic Peninsula in Washington State and for the Pacific Northwest Smart Grid Demonstration project – the largest of its kind – to validate smart grid benefits and new control approaches that engage demand and distributed resources at scale. Example outcomes include Avista Corporation implementing distribution automation and smart metering pilots that delivered a 10-percent reduction in customer outages, reduced consumer outage durations by 21 percent, and resulted in 1.5 million avoided outage minutes between April 2015 and April 2016.

3. Innovated and implemented new, novel predictive data analysis. PNNL delivered the first applications of high performance computing to grid tools such as interconnection-scale contingency analysis, reducing run times from days to under two minutes. PNNL also applied high performance computing and phasor measurement unit data to deliver the first real-time dynamic state estimation to open the door to the future world of predictive grid tools. This parallelized state estimator tool enabled PNNL to deliver assessments of system risk at the interconnection scale on the Western Interconnection in less than two minutes versus the traditional 24 hours. This provides operators with more powerful tools to mitigate the risk of potential cyber-attacks and other risks. Moving from reactive to predictive data-driven analysis methods is essential to effectively managing cybersecurity challenges on the grid.

4. Designed and implemented meaningful national exercises that address critical electrical grid resiliency and cybersecurity challenges. PNNL assisted NERC and DOE with design and implementation of a series of national GridEx exercises designed to link industry with government and law enforcement agencies to conduct cyber-attack exercises.

GridEx III, held in November 2015, engaged 364 organizations and more than 4,000 participants in scenarios designed and operated with support from PNNL. GridEx IV will be held in mid-November, with additional support provided by PNNL.

These examples illustrate the high return on investment possible when combining advanced technology innovation designed to improve cybersecurity with public-private validation and deployment.

Lastly, the DOE Grid Modernization Initiative is an important source of innovation for national efforts to modernize energy infrastructure. Improved grid resilience and security for cybersecurity is a major objective of the overall effort. The Initiative is a DOE-wide effort across multiple program offices to accelerate the development of technology, modeling analysis, tools, and frameworks to enable grid modernization adoption. As a key component of this Initiative, the Grid Modernization Laboratory Consortium – co-led by PNNL and the National Renewable Energy Laboratory – is working closely with partners in industry, academia, and cities and states to deliver new concepts, tools, platforms, and technologies to better measure, analyze, predict, and control the grid of the future – resulting in improved resilience, reliability, and productivity. Public-private collaboration in field validation accelerates the development of lessons learned and data that support states and utilities to develop business cases for their grid modernization efforts.

Current and Emerging Advanced Grid Cyber Security Technologies

Cyber Situational Awareness: In order to monitor and effectively manage the security and resiliency of the grid, PNNL and DOE developed and deployed the Cyber Risk Information Sharing Program (CRISP). This voluntary situational awareness program identifies cyber threats to utilities and shares that information with utilities, which collectively generate over 75 percent of the nation’s electricity. Today, PNNL works with the NERC E-ISAC and DOE to ensure rapid exchange of information across industry and government entities to provide timely alerts and response to cybersecurity risks posed to power industry infrastructure. This effort continues to expand coverage and improve the speed and accuracy of situational awareness of threats for the industry. In addition to expanding the system to include additional utilities, PNNL is developing advanced analytics that can handle terabytes of data daily.

PNNL is now extending cyber situational awareness to increase attention on the grid control systems internal to the utilities, also called operational technologies (OT), and the interdependent infrastructures such as fuel delivery (e.g. natural gas pipelines) and communications. We believe that the nation must develop an integrated, real-time view of cyber risk across the IT and OT elements of the power system to significantly improve our cyber resilience.

NERC standards already require significant sensing of the OT environment to ensure NERC Critical Infrastructure Plan (CIP) compliance. As such, PNNL is applying science and advanced technology tools to enhance the analytics of these data streams to deliver cyber situational awareness for these grid control systems. These analytics depend on the fundamental science of high performance computing, statistics, and a reemerging field of "deep learning." Deep learning refers to advances on the artificial intelligence concepts of the 1990s that are delivered on new high performance computing platforms and leverage the ultra large data sets that are emerging in the power system. These ultra large data sets exist on the IT and OT sides of the power system. They are driven by the two billion intelligent devices at the grid edge today, which are expected to grow to 20 billion by 2025; the 64 million smart meters installed over the past decade; and the cutting-edge synchrophasor monitor network of 2,500 sensors across North America delivering samples at a rate of 60 samples per second. Collectively, power system operators are engaging massive-scale data sets that offer significant opportunity to improve power system cyber situational awareness.

PNNL and others in the national lab, industry and academic communities are applying deep learning concepts to these data sets to extract relationships and trends that have meaning to issues such as cyber risk or control system anomalies, which can be indicators of cyber-attack. These results can deliver value in two ways:

1. They provide power system operators and/or planners with insights that inform better decision making in the dispatch of generation and secure operation of the power system.

2. Automated "machine to machine" exchanges enable the power system protection and control systems to recognize problems faster and respond safely. The "machine-to-machine" topic is one of the high priorities set by the Electricity Subsector Coordinating Council for public-private research and development (R&D) advancement.

Ultimately, this course of advanced R&D effort by PNNL and the broader community will help detect cyber and other risks faster and support the design of new systems that are inherently more resilient to cyber and other threats.

Advanced Science and Technology Research: To complement the improvements in situational awareness of IT and OT systems, PNNL is also applying advanced science and technology cyber resilience concepts in pursuit of new power system paradigms that are inherently resilient and adaptive. Elements of this research include:

- **Adaptive Networks:** The emerging modern grid is substantially more dependent upon communications networks, both in terms of capacity and performance as well as reliability. PNNL recently teamed with Schweitzer Engineering in Pullman, Washington to develop and deploy a product using a new concept called "software defined networks" to enable the reconfiguration of communication networks through software commands. Software defined networks provide an additional, adaptive defense layer. This new "software" layer of a computer network allows the network to change segmentation and to quarantine parts of the network dynamically. This means an adversary would need to break through an additional layer of technology, one that can change. This project resulted in a commercial product that achieved exceptional market presence in a very short time.

- **Data resilience:** Growth in e-commerce innovation and the consideration of new utility market constructs to better engage consumer interests in new services have resulted in new approaches to protecting data in open environments. One example is blockchain, the technology that Bitcoin uses to secure transactions. Blockchain is a method for recording transactions in a shared, encrypted ledger without the need for a central repository, which is significant because centralized data is a compelling target for cyber attackers. By spreading the data around in multiple places, it is much harder to attack, modify or manipulate. With regard to the grid, blockchain could be a part of grid modernization efforts, encourage distributed power generation and storage systems, and help secure emerging market constructs. PNNL is currently working with DOE and industry partners to determine the optimal use of such resilient data concepts as blockchain in emerging market constructs such as transactive energy.

- **Adaptive control systems:** A third technology innovation is the transition from fixed to adaptive control and protection systems which adjust in real-time based upon system conditions at that moment. Adaptive control systems can provide a more level cyber playing field by adjusting on the fly to confuse, obfuscate, and mislead adversaries as they work their way through a system, increasing the effort and knowledge needed to get through defenses, while also giving a better chance for detection and deployment of solutions to be effective. PNNL is developing advanced distributed and hybrid control theory and concepts that make the power system and key parts thereof, such as building control systems, more adaptive and resilient to cyber-attack. The Grid Modernization Laboratory Consortium also is conducting advanced control research that leverages fundamental mathematics and advance network theory to accommodate more distributed energy resources that can support power system resilience.

These are three examples of advanced technologies that will enable new paradigms of power system design to actively defend against cyber-attack and other risks facing the modern grid.

Cyber “Best Practices” and Valuation an Important Part of National Cyber Readiness

Science and technology efforts are critical to protect the electric grid and energy infrastructure from cyber-attack, but cannot alone achieve the end state goal. Grid operators must learn and implement basic “cyber hygiene” measures – practices and routines that can be undertaken regularly (or avoided) to keep utility systems in good shape. While large utilities are actively pursuing cybersecurity strategies to meet industry requirements, small and mid-sized utilities don’t have to meet those requirements and can view cyber defense as an expensive and complex undertaking. DOE is working with the American Public Power Association and the National Rural Electric Cooperative Association to help small and mid-sized utility managers improve their cybersecurity readiness.

Additionally, utilities at all levels – consumer-owned, investor-owned, municipalities – must have the capacity to understand the value of alternatives to improve their cybersecurity, system resilience and performance. State regulators need the same tools and data sets with which to evaluate cybersecurity and modernization plans and provide the regulatory incentives to achieve prudent efforts that delivers affordable resilience improvements to product offerings that enable modernization at scale. Finally, vendors must be able to define market opportunities to ensure rapid innovation in their product offerings. The Grid Modernization Laboratory Consortium portfolio includes research projects to develop a framework for valuation of the new grid technologies and concepts, including for cybersecurity, so that government and industry stakeholders can work together to assess the benefits and costs of security and resilience improvement strategies. This partnership between DOE, states, and industry is an important collaboration in charting a timely path to a more secure, resilient U.S. power system.

Conclusion

Industry and DOE have partnered to significantly advance the cyber situational awareness of the utility business and internet-facing computer networks over the past few years. The next step in the journey is to integrate these capabilities with enhanced situational awareness of control systems, providing both operators and automated protection systems the capacity to significantly enhance cyber awareness, security and resilience across utility IT and OT systems.

In parallel to "better defending" the current system, we must to continue to leverage the foundational science and technology tools of high performance computation, analytics, deep learning and control theory to develop more resilient system designs for networks, data and grid control systems. These will enable the power system to resist inevitable attacks, better defend against cyber and other hazards, and ultimately recover more quickly.

The DOE investments in fundamental science, applied technology and public-private field validation partnerships are foundational elements of an effective, integrated national cyber readiness strategy and capacity for the U.S. electric power system and its related infrastructures. I appreciate the opportunity to discuss this important issue with you today, and I am happy to answer your questions. Thank you.