Statement of Jason Fuller
Chief Energy Resilience Engineer, Electricity Sector
Pacific Northwest National Laboratory
Before the
United States House of Representatives
Committee on Science, Space, and Technology
Energy Subcommittee

March 23rd, 2023

Good afternoon. Thank you, Chairman Williams, Ranking Member Bowman, and Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the value of fundamental and applied research objectives as it relates to protecting the cyber and physical security of the U.S. electrical infrastructure.

My name is Jason Fuller. I have been a researcher at the Department of Energy's (DOE) Pacific Northwest National Laboratory (PNNL) for 14 years, focused on power systems analysis, modeling, and simulation. I am the Chief Energy Resilience Engineer and I lead Strategic Functions for PNNL's Electricity Infrastructure and Grid Sector. I also serve as the Infrastructure Modeling Lead for the Office of Electricity's (OE) North American Energy Resilience Model (NAERM).

Today I will address two main points:

1. The evolving nature of the U.S. electrical infrastructure and the increasingly complex threats it faces requires further investments in cutting edge research and development to maintain our Nation's competitive and security advantages, and

2. Basic and applied research is an integral part of innovating new methods to predict and monitor potential threats, whether man-made or natural, and protect our system from the impacts of those challenges.

The Changing Landscape

The U.S. power grid is rapidly changing from an earlier, simpler era with large generation stations and passive energy loads to a much more dynamic grid with growing distributed energy generation resources and much more active, connected, "smart" loads. Decreased costs and advancements in technology have led to consumer adoption of solar, energy storage, electric vehicles, and other grid edge technologies. This transition to more intermittent clean energy will accelerate the use of inverters and power electronics that will require new approaches to system protection and control. Many of these assets are owned by customers or third parties and therefore may not be within traditional direct control of electric utilities, introducing additional uncertainties. To support this new evolution of the power system, the control and communication systems will need to evolve and the systems protecting it will need to evolve, too. Advancements in methods for cybersecurity protection of mixed ownership control systems, and additional methods for securing the underlying communication networks, are needed.

The electric grid powers our daily lives and our Nation's economy, and our dependence on the electric power grid is only increasing. Deep electrification of building loads and transportation presents an opportunity for additional system flexibility and utility growth, but also leads to challenges in securing enough reliable energy to support the transition. And with an increasingly remote workforce, having consistent, reliable power at our homes is suddenly becoming a more critical part of the national economy. This changes the nature of how we think about reliability and resilience in the electricity sector, as well as sectors that rely on electricity, and potentially disrupts decades of thinking about how to prioritize preventative actions and restoration after a failure. This is leading many consumers to consider investments in backup generation, storage, or microgrids, to ensure uninterrupted service. This requires new innovations in operational technology, situational awareness, system architecture, and security to protect the operation of large numbers of third-party assets not previously part of power system operations.

Recent years have seen prolonged droughts and more extensive wildfires; increased intensity and frequency of rain, flooding, and hurricanes; and extended cold- and heat-wave events that can cause immense harm to the Nation's electrical infrastructure. Utilities use forecasts based on historical records to design the power system within certain reliability criteria but changing climate patterns disrupt traditional planning methods. New capabilities are needed to translate future extreme weather patterns into actionable decision-making by utilities and other stakeholders within their planning processes. New technologies are needed to respond to or prevent outages in extreme weather events, or other natural disasters, creating needed flexibility in our future power system.

Foreign actors are also aware of the criticality of the electrical system in powering our day-to-day lives and the importance to our overall society. It has long been considered a logical target for major cyber-physical intrusions, ranging from nuisances to complex, coordinated efforts, that could result in large-scale outages or targeted loss of critical loads. Like most complex systems, grid cyberattacks are an ever-evolving conflict with an asymmetric advantage, requiring the defenders to constantly create new tools to combat. To combat these efforts, this requires continued innovation to strengthen the trustworthiness of supply chain manufacturers and increase confidence that embedded systems perform their assigned tasks; to evaluate and assess the resilience of cybersecurity architectures in comparison with system vulnerabilities and risk; to create advanced tools to help gain a greater system understanding; and integrate human and machine intelligence and data-driven analytical platforms to enhance cyber adversary detection, insight discovery, and situational awareness through greater automation and response. And the Federal government has a continued role in developing the workforce of tomorrow to address these constantly shifting challenges.

The Importance of Research in Protecting the Nation's Electricity Infrastructure

Federal investment in basic research not only drives American innovation but also provides the necessary advancements for the next generation of technology to continue protecting against evolving threats. However, it often takes decades to realize the transition from early-stage investments to commercialized products. DOE's applied energy offices benefit from those early-stage investments and help transition advances in science to deployment in energy systems. Such Federal investment has been critical to advancing grid security and resilience technologies.

As an example, the advancements from the Office of Science's Advanced Scientific Computing Research (ASCR), and its predecessor organizations, led to innovations in parallel processing and supporting software libraries; solvers for differential equations and optimization; large-scale data analytics and machine learning; and multiple advances in processors. All of these have had significant impact on the electrical industry's ability to monitor, control, and protect the Nation's electrical system, often driven by additional investments from DOE's applied energy offices. Advanced visualization techniques coupled with computational advances and optimization tools have provided operators with unprecedented visibility into the real-time behavior of the system, increasing overall system security. Foundational research like this is now informing ongoing DOE programs like the Energy Threat Analysis Center (ETAC) where next generation cyber analytics are being deployed on real world data to help defend the Nation's critical energy infrastructure. Data analytic, machine learning, and artificial intelligence techniques are being used throughout the industry to discover abnormalities in system behaviors. The next generation of tools are just as important. Exascale computing, powered by the Leadership Computing Facility at Oak Ridge National Laboratory, offers the opportunity to solve power system challenges of unprecedented complexity, including optimizing the operation of tens of millions of controllable devices while also exploring a wide range of simultaneous threats. Quantum information sciences may provide the next generation of encryption protocols to protect control operations. New applied mathematical techniques in optimization and linear algebra, which electrical industry control centers heavily rely upon, will likely lead to tools that provide much faster and richer responses to system perturbations. Today's research is tomorrow's capabilities – the power industry has relied upon the fundamental advancements in computational technology and will continue to do so for the foreseeable future.

Further, partnerships between fundamental and applied energy research offices between agencies can often lead to innovative solutions for emerging power system challenges. For example, partnerships between the Division of Mathematical Sciences at the National Science Foundation (NSF) and the OE have led to improvements in security, reliability, and efficiency of the modern power grid. The program, named the Algorithms for Modern Power Systems (AMPS), is designed to enhance interdisciplinary research crossing power system engineering, mathematics, and statistics, and in part stemmed from Laboratory Directed Research and Development (LDRD) activities at PNNL. This unique partnership between NSF and OE has led to advancements in load and generation forecasting, microgrid operations, and risk prediction, among others, and presents an opportunity to give students a hands-on, real-world STEM education at DOE National Laboratories.

These efforts not only build new technology, but act as a national repository of skills and expertise for the country when it is needed most. For example, the DOE national labs have proudly supported Ukraine over the past year. PNNL has leveraged a long-standing relationship with Ukraine that dates to 2012, when we began work with Ukrenergo to improve grid resiliency and cyber security. PNNL teamed with Ukrenergo leadership to plan for their desynchronization from the Russian grid and synchronization with the European grid, ENTSO-E. PNNL and Idaho National Lab were providing grid cyber security assistance to Ukraine in support of full synchronization to ENTSO-E, and we ratcheted up those efforts following focused cyber-attacks that began in October. Joint appointees from Washington State University and PNNL were also able to leverage NSF and DOE research to utilize software developed to manage power system oscillations to determine that emergency synchronization with the European system would work, supporting Ukraine's power system in their time of need. DOE's National Laboratories supported real-time damage assessments of Ukraine's energy system through a combination of satellite imagery and tailored analytical tools to inform Ukrenergo's response strategy. These efforts are ongoing and have expanded to include a broader assessment of infrastructure damage. Without that repository of skills and long history of relationships to draw from, assistance would not have been possible.

PNNL's Electrical Infrastructure History

For more than three decades, PNNL has supported power system reliability, resilience and innovation for the nation, the Pacific Northwest, and Washington state. Over this period, cutting edge research has been an important part in supporting the continued security of the Nation's critical electrical system, including the following activities:

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 grid tool has demonstrated value by detecting impending system control and equipment faults for system operators, thus avoiding major outages.

2. Led public-private 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.

3. 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.

4. Run the Cyber Risk Information Sharing Program (CRISP) with NERC-EISAC (Electricity Information Sharing and Analysis Center) and DOE. CRISP is a public-private partnership

that delivers relevant and actionable cybersecurity information to participants from the U.S. electricity industry. Collaboration between government and private industry is essential to combat cyber threats to U.S. critical electric infrastructure. By leveraging the open-source cyber threat intelligence and government-informed reporting provided by PNNL, the E-ISAC provides CRISP participants with information related to advanced threat actors, custom automated analytics to identify anomalies, event and incident trending statistics and other information relevant for operators of critical electric infrastructure.

5. Leads the Cybersecurity Capability Maturity Model (C2M2) through a collaborative effort between public- and private-sector organizations, sponsored by DOE's Cybersecurity, Energy Security, and Emergency Response (CESER) program, the Electricity Subsector Coordinating Council (ESCC), and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). This allows for users of the model to assess their business practices supporting cybersecurity and learn where more investment would help meet their goals for cybersecurity. Cybersecurity insurance companies have used this to influence rates for insurance. PNNL has expanded on C2M2 to create assessment tools for electric utilities, building owners, the NIST Cybersecurity Framework, Facility Cybersecurity Framework, and Secure Design and Development Principles by partnering with the relevant stakeholders and offices.

6. Created an improved methodology and technology for electricity, oil, and gas owners and operators to continuously monitor legacy and smart energy delivery and critical control assets needed for reliable delivery of energy. Partnering with academia and vendors, SSASS-E (Safe, Secure Autonomous Scanning Solution for Energy) provides a continuous monitoring solution that is safe, secure, and effectively eliminates blind spots by identifying and analyzing transient mobile, virtual, cloud, IT, and control assets. Because of CESER's investments, industry now has greater insight and understanding (normative and outlier behavior) of their entire control system.

7. Deployed facilities, such as the Electricity Infrastructure Operations Center at PNNL, a working mockup of a utility control center funded by the OE, that enables human factors evaluation of visualization tools, advanced computational methods, and human responses in a realistic setting. This enables researchers and industry to advance the state-of-the-art in control room operations while reevaluating traditional approaches and enhancing reliability through advanced methods.

8. Developed ExaSGD, an Office of Science collaboration between PNNL, Lawrence Livermore National Laboratory, National Renewable Energy Laboratory, Argonne National Laboratory, and Oak Ridge National Laboratory, to develop the next generation of tools to address challenges associated with the addition of distributed and variable generation and optimize the grid's response to potential disruption events under different weather scenarios. This requires the simultaneous optimization of millions of realizations within a short turnaround to manage the integrity of the system and with greater

uncertainty. These tools are designed to utilize Oak Ridge's Frontier exascale supercomputer to meet those needs while also scaling to utility-accessible hardware.

9. Developed NAERM in a partnership with DOE and eight national labs, enabling advanced modeling and analysis of the Nation's electricity infrastructure and interdependent systems, such as natural gas and communication systems. NAERM offers energy system planners, operators, and Federal agency partners premier modeling tools to predict the consequences of natural and man-made threats and evaluate mitigation and response opportunities. It can quantitatively inform the strategic allocation of investments to respond to major electric system disruptions. It relies on many modeling tools and techniques developed under the Grid Modernization Laboratory Consortium (GMLC).

10. Expanded the Rapid Analytics for Disaster Response (RADR-Fire) image analytics and modeling suite to help mitigate damage to key energy infrastructure. This set of tools uses a combination of imagery processing, artificial intelligence, and cloud computing, to assess and predict wildfire damage, which can allow first responders and utilities to take measures to mitigate potential impacts and expedite infrastructure restoration. Coupled with Office of Science efforts to predict future wildfire behavior under drier and warmer conditions, decision-makers can be more informed when managing long-term investments.

11. Building the Grid Storage Launchpad (GSL), a critical facility to accelerate the development and deployment of grid-scale energy storage to enhance reliability, resilience and flexibility. The GSL, funded by the OE at PNNL, supports DOE's Energy Storage Grand Challenge and Long Duration Storage Shot and aims to secure domestic manufacturing supply chains and independently test and validate grid-scale storage technologies. The GSL facility will develop and promulgate rigorous grid performance standards and requirements that span the entire energy storage research and development cycle—from basic materials synthesis to advanced prototyping.

These examples illustrate the high return on federal investments when utilities, academia, and national labs collaborate across the country and combine fundamental advances and technology innovation with public-private validation and deployment.

Conclusion

In conclusion, the electric grid is a critical component of our Nation's economic success and daily life. The electric industry has greatly benefited from Federal research investments, both basic and applied, and will continue to benefit from those investments into the foreseeable future. As our system continues to further digitize and electrify, cyber and physical security of the electricity sector will remain a critical issue and research and development needs will continue to evolve along with it. Continued advancements will substantially enhance our ability to operate the Nation's power system in real time, enabling grid operators to better avoid outages and reduce the duration when they occur. These advanced tools and techniques will directly support enhanced situational awareness, providing analytic tools for faster response, better assessment and mitigation of risk, and planning tools for more efficient and resilient operations.

Thank you for the opportunity to provide the Committee with information on this topic. I would be happy to answer any questions that you may have.