Cyber Technology and Energy Infrastructure

Statement of Richard Raines, Ph.D.
Director of Electrical and Electronics Systems Research
Oak Ridge National Laboratory

Before the
Committee on Energy and Natural Resources
U.S. Senate
October 26, 2017

Thank you, Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee. I am Dr. Richard Raines, Director of the Electrical and Electronics Systems Research Division at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. It is an honor to participate in this hearing with this distinguished panel today.

INTRODUCTION

Oak Ridge National Laboratory is the largest Department of Energy (DOE) science and energy laboratory, conducting basic and applied research to deliver transformative solutions to compelling problems in energy and security. ORNL's diverse capabilities span a broad range of scientific and engineering disciplines, enabling the Laboratory to explore fundamental science challenges and to carry out the research needed to accelerate the delivery of solutions to the marketplace. ORNL supports DOE's national missions of:

- Scientific discovery—We assemble teams of experts from multiple disciplines, equip them with powerful instruments and research facilities, and address compelling national problems;

- Clean energy—We deliver technology solutions for energy sources such as nuclear fission/fusion, fossil energy, solar photovoltaics, geothermal, hydropower, and biofuels, as well as energy-efficient buildings, transportation, and manufacturing;

- Security—We develop and deploy "first-of-a-kind" science-based security technologies to make the United States, its critical infrastructure, and the world a safer place.

ORNL supports these missions through leadership in four major areas of science and technology:

- Computing—We accelerate scientific discovery and the technology development cycle through modeling and simulation on powerful supercomputers, including Titan, the nation's most powerful system for open scientific computing (fourth most powerful in the

world), advance data-intensive science, and sustain U.S. leadership in high-performance computing;

- Materials—We integrate basic and applied research to develop advanced materials for energy applications. The latest frontier in materials research is at the nanoscale—designing materials atom by atom —and we leverage ORNL assets such as Titan and the Center for Nanophase Materials Science for breakthrough materials research;

- Neutrons—We operate two of the world's leading neutron sources that enable scientists and engineers to gain new insights into materials and biological systems;

- Nuclear—We advance the scientific basis for 21st century nuclear fission and fusion technologies and systems, and we produce isotopes for research, industry, and medicine.

Today's briefing reflects my perspective as director of electrical and electronics systems research and as the lead for energy system cybersecurity at a national laboratory with an intense focus on solving compelling national problems in energy and security.

GRID VULNERABILITY: A GROWING THREAT

The nation's electrical grid is a vital resource upon which our economy and our citizens' daily lives depend. It is also a system that is highly vulnerable to cyber intrusions as more and more utility controls and "smart" technologies rely on public internet connections. These advanced technologies give operators better control and make the grid more efficient and resilient. But they come at a price: the potential exposure of devices and systems to very savvy computer specialists whose intent may be nefarious. As such, cybersecurity measures and capabilities must be constantly improved to address these rapidly emerging threats as we modernize grid infrastructure.

The electrical grid is an interconnected network of power, communication and control systems that requires vigilance in cybersecurity that is shared by all associated partners. All must operate with the recognition that vulnerabilities will be discovered and exploited by adversarial actors. Energy owners and operators have the primary responsibility to protect their systems from failure. The federal government is responsible for ensuring national and economic security, and the health and safety of American citizens and communities. It is in everyone's interest that we engage in a closely coordinated defense of our energy networks, to reduce the types of physical and cyberattacks that could trigger a large-scale and prolonged energy disruption with direct bearing on our strength as a nation.

Operational technologies, such as electric power grids, offer realizable targets for the midrange to sophisticated actor. The grid has emerged as a viable target for exploitation for many reasons, including simple control logic and operations, and globally produced sensors, but largely due to growing interconnectivity with the internet. Attackers exploit systems that lack current software configurations or unsuspecting operators who may not have been trained to avoid attacks such as

phishing. The intrusions can inflict damage on physical infrastructure by infiltrating the digital systems that control assets—damaging equipment and disrupting vital services even without a physical attack. As witnessed in the Ukraine in 2015 and again in 2016, the cyber threat is real and damaging.

In the Ukrainian cyberattacks, the adversary exploited the human component of the system's operations to gain access and escalate privileges for total control of the targeted system. Additionally, the attackers circumvented reporting mechanisms that were designed to alert system monitors of abnormal behavior. These actions resulted in power losses to more than 225,000 customers over a period of a few hours. While power was restored to consumers relatively quickly, the overall implications of this attack were not known for weeks. A key takeaway from these attacks was the reactive nature of the system operator responses. Forensic analysis revealed that little to no protective mechanisms were in place to preclude the attack from occurring—all efforts were restorative in nature.

Fast-forwarding to May of this year, the President recognized the growing cyber threat to U.S. critical assets and sought new assessments under an executive order[1] on strengthening the cybersecurity of federal networks and critical infrastructure.

Furthermore, in an August report[2] released by the President's National Infrastructure Advisory Council (NIAC), senior executives from industry and state and local governments stated that national leadership, in close collaboration with industry, is essential to support cybersecurity of high-risk assets. The report listed 11 recommended actions that the federal government and the private sector can take to defend critical private systems from aggressive cyberattacks including "…establishing separate, secure communications networks specifically designated for the most critical cyber networks…."

Our challenge in the United States is to implement cyber solutions to better protect energy sector communications and controls, while continuing to make the grid "smarter" and more resilient when problems do arise, including the challenges of severe weather events such as we recently saw with Hurricanes Harvey, Irma, and Maria.

It is a task made difficult by the grid's existing operational requirements and complex interconnectivity. The electric grid is a 24/7/365 operating system. The United States' strategic and societal interests rely on the grid's continuous, real-time, and reliable operation, which underpins the social fabric of this country. This operational tempo makes grid research, development, and the deployment of solutions a difficult challenge for industry to address alone.

This is where the DOE's national laboratories provide essential national research. The National Laboratory System is uniquely positioned to address cybersecurity challenges through technology breakthroughs in partnership with the private sector. At ORNL, expertise and capabilities in high-performance computing, data and graph analytics, discrete mathematics,

[1] http://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] http://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

power systems and engineering, embedded systems and wireless technologies, sensors and controls provide solutions and breakthroughs for detecting and deterring cyberattacks.

ORNL EXPERIENCE: TECHNOLOGICAL SOLUTIONS

ORNL brings capabilities and expertise to both 1) protect the electric grid from cyberattack, and 2) modernize grid infrastructure and increase its ability to respond quickly to disruption.

Our scientists and engineers are engaged in several areas of research designed to increase both grid cybersecurity and resilience, or the system's ability to quickly rebound from disruption. Modernizing grid infrastructure and making it more resilient is essential to grid security.

ORNL has developed numerous technologies for cybersecurity. These technologies range from hardware device monitors (such as BEHOLDER), to software that can detect dormant malicious code (HYPERION), to platforms that can discover and detect the presence of advanced persistent threats (ORCA).

Additional ORNL-developed cyber-physical tools and capabilities include:

- GridEye sensors located across the U.S. for real-time monitoring of the power grid;
- EAGLE-I, a visualization and analysis system designed to predict possible energy system outages as well as help first-responders rapidly locate outages when they occur;
- Oak Ridge Cyber Analytics (ORCA), a real-time cybersecurity platform for detecting advanced persistent threats and zero-day exploits;
- Situ**,** a real-time cyber situational awareness tool capable of determining anomalies in network-related traffic; and
- Timing Authentication Secured by Quantum Correlations (TASQC**),** a ground-based timing capability for secure communications.

As announced in September 2017 by DOE's Office of Electricity Delivery and Energy Reliability, ORNL is taking on several additional projects for grid resilience and cybersecurity.

As part of DOE's Grid Modernization Laboratory Consortium (GMLC), which leverages the capabilities and expertise of all 17 national laboratories, ORNL will be involved in two **resilient distribution systems** projects:

- Integration of responsive residential loads into distribution management systems. This project aims to provide electric utilities with software and hardware that make possible demand-side management of residential loads to improve grid resiliency.
- Increasing distribution system resiliency using flexible distributed energy resources and microgrid assets enabled by OpenFMB, or Open Field Message Bus. OpenFMB is a

framework that allows generation assets to communicate with each other for better system flexibility, rather than being controlled by a single system.

Both projects address ways to enhance electricity distribution systems, including microgrids – localized grids that can disconnect from the traditional grid and operate autonomously, a capability that helps to mitigate disturbances and strengthen grid resilience.

Under DOE's **cybersecurity for energy delivery systems** research area, ORNL will be involved in five projects:

- *DarkNet*. A project to get the electric grid off the public internet. The project will define requirements for a secure energy delivery control system network that is independent of the public internet and uses existing but currently unused optical fiber, known as "dark fiber." The NIAC report referenced above, for instance, lists the creation of a separate, secure communications network specifically designated for critical infrastructure as its number one recommendation. The DarkNet concept is discussed in more detail below.

- *Quantum physics-secured communications for the energy sector* (referencing our national security needs to outpace Chinese advances demonstrated in orbiting satellite systems http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance). Development of a quantum-rooted grid security framework in which information is carried in quantum states of light, so that any attempt to read that information is revealed in real-time, detectable changes to the quantum states.

- *Quantum key distribution for the energy sector*. Trusted node relays and networks. Research, design, and prototype of a quantum secure communication operational network, including trustworthy relays to extend distance and decrease cost for critical energy infrastructure.

- *Malware operational mitigation.* Working with energy sector partners to coordinate utility system malware detection and analysis and provide real-time validation of vulnerabilities to system operators.

- *Energy delivery systems with verifiable trustworthiness.* Providing a tool to verify the integrity of firmware used in energy delivery system devices, without taking the equipment offline.

These projects continue ORNL's long history of working with public and private partners to achieve the energy sector's vision of resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

In addressing the area of grid security, ORNL is mindful that the nation's privately-owned electricity assets present a unique challenge, and we are leveraging our long history of working closely with private sector partners to develop effective research.

ORNL is working with utility companies such as the Chattanooga Electric Power Board (EPB) and Southern Company to help design, assess and install microgrids. Companies are trying to

understand the value proposition of these technologies for improved grid resiliency. With ORNL's assistance, EPB is evaluating the idea of "dynamic microgrids" where sections of the distribution system—potentially with distributed energy resources—can be sectionalized into independent microgrids to determine if this will improve grid resiliency. ORNL's research with EPB is a prime example of how a close working relationship with industry can deepen our understanding of these challenges and produce workable solutions. The EPB system has been a successful "living laboratory" for advanced sensors and other technology developed by ORNL to make the grid more secure and resilient.

We are also working with Southern Company to test new microgrid technology that provides local control of resources like solar power and energy storage sited in a "connected neighborhood" and then seamlessly integrated into the larger power grid.

Most recently, ORNL has considered how its scientific expertise may be leveraged to help an area in which the local power grid is essentially being rebuilt from the ground up. Puerto Rico was devastated by Hurricane Maria last month. The island's critical infrastructure, including its power transmission and distribution grid serving more than 1.4 million customers, was nearly demolished by the powerful storm. As the relief and recovery effort continues, we are mindful that many of the solutions developed for grid resilience could be purposely built into a completely new, robust system for Puerto Rico.

Through distributed energy resources, for instance, the Puerto Rico Electric Power Authority could benefit from microgrids, with more power generation spread throughout its territory, sited locally in neighborhoods and communities and providing greater flexibility when the larger grid is disrupted.

Complementary opportunities exist to support the development of a more secure and resilient Puerto Rican infrastructure, which will ultimately lead to better quality of life for its residents and reliable electricity to support its businesses.

THE DARKNET CONCEPT

As part of DarkNet, ORNL is investigating ways to move electric grid controls and communications away from the public internet and onto secure networks. The goal of DarkNet is to develop and implement, in conjunction with private and public partners, a highly secure, resilient, and redundant communications, sensing, and technical assistance solution supporting all elements of the electricity enterprise and its supply chain. The vision is to shield the nation's electric grid from hostile cyber penetrations while also advancing the state-of-the-art in anticipatory threat mitigation. DarkNet will design and build an isolated, secure communications network to protect and transport the nation's most sensitive critical infrastructure data—beginning with the electric grid.

Under DarkNet, ORNL and its partners, will investigate ways to take advantage of underutilized fiber optic capacity already on utility systems across the country but not accessible to the

internet. This approach can be used to move grid command and control functions onto private, isolated networks using "dark" or unlit fiber.

ORNL scientists and engineers are evaluating the over-capacity of fiber deployed in the past two decades and determining whether it offers a platform for a new communications and control architecture with innovative cyber-physical security measures. With advanced sensor technologies that monitor the grid for any disturbances that indicate intrusion, ORNL will develop methods that automatically detect, isolate, and defend against these attacks—with the goal of a self-aware, self-healing network. Utilizing ORNL's unique high-performance computing platforms and energy testbeds, anticipatory threat modeling and analysis will aid the development of capabilities to rapidly identify emerging threats, gain awareness of the potential threat's capabilities, and dynamically posture resources (sensors and mitigation devices) to minimize, if not eliminate, the threat and disruptive consequences.

DarkNet's key differentiator from previous cybersecurity solutions lies in its holistic approach to 1) use existing resources (i.e., unlit fiber) for separation from an inherently unsecureable infrastructure (the internet); and 2) develop and rapidly deploy new and innovative foundational security capabilities.

Key DarkNet objectives include:

- Enhancing infrastructure (new and existing dark fiber) as a cost-effective protective measure, using advanced communications and cybersecurity technologies;
- Leveraging emerging communications security protocols that establish protected links across the grid;
- Working with industry to create living laboratories to test security functionality and resilience—partnering with utilities and suppliers for proof of concept;
- Implementing new technologies in toolkit form and operational security approaches to protect against cyber and insider threats;
- Enhancing grid state monitoring with advanced sensing, measurements, escalating alert and situational awareness; and
- Using the existing buried infrastructure (dark fiber) as a cost-effective protective measure, leveraging advanced communications (ultra-fast 5G-LTE networks, satellite communications, and private wireless networks) and cybersecurity technologies suitable for expanding smart grid requirements.

DarkNet will evolve from an implementation framework already under development to a series of integrated research, development, test, and evaluation projects that will have the potential to yield near- and far-term cybersecurity solutions.

In conclusion, if the DarkNet concept is funded and implemented, it will enable national continuity of operations, rapid restoration, and cost-effective protective measures to thwart damage from cyberattacks, operational and physical threats, and natural disasters. Security and

resilience enhancements are not about bolting on a costly, cumbersome exoskeleton. As a nation, we must infuse the grid's operational DNA with capabilities that make it immune to attack and degradation.

CLOSING REMARKS

Whether the threat is natural or manmade, intentional or not, a secure, resilient electrical grid with hardened defenses is essential to the security of our nation. The grid's critical systems must evolve to address a variety of challenges such as cyberattack, severe weather, a changing mix of power generation types, the growth of interconnected smart devices, and the aging of electricity infrastructure.

Sometimes called the world's largest machine, a reliable, secure electric grid is foundational to U.S. competitiveness, economic vitality, and our very way of life. ORNL and the other DOE national laboratories stand ready to work with industry and other institutions to develop and employ innovative technical solutions to protect the nation's power grid. Thank you again for the opportunity to provide this briefing. I welcome your questions on this important topic.

APPENDIX

Summary of ORNL and National Lab Cyber R&D Capabilities for Energy Sector Protection

The National Laboratory System is well-suited to exploring and developing technological solutions for protecting the energy grid. Partnerships with government, industry and academia are longstanding and mature. The national laboratories transition early stage research and development technologies to fielded and operational tools/platforms via partnerships with industry and Federal government partners.

Key ORNL Cyber-Physical Capabilities

- **Facilities**
  - **Distributed Energy Control and Communication (DECC)** laboratory for testing and evaluating emerging energy security tools and techniques
  - **Complete System-Level, Efficient & Interoperable Solution for Microgrid Integrated Control (CSEISMIC)** for testing and evaluation of microgrid control and security
  - **Real-Time Digital Simulator (RTDS)** for simulating electrical nodes on the power grid. ORNL capability to simulate 366 nodes
- **Tools**
  - **GridEye** sensors located across the U.S. for real-time monitoring of power grid
  - **Visualizing Energy Resources Dynamically on the Earth (VERDE)**, a visualization and analysis system designed to predict possible energy system outages as well as help first-responders rapidly locate the outages when they occur
  - **EAGLE-I**, a comprehensive, real-time energy monitoring dashboard developed by DOE/OE for integration with VERDE
  - **Oak Ridge Cyber Analytics (ORCA)**, a real-time cybersecurity platform for detecting advanced persistent threats and 0-day exploits
  - **Situ**, a real-time cyber situational awareness tool capable of determining anomalies in network related traffic
  - **Timing Authentication Secured by Quantum Correlations (TASQC),** a ground-based timing capability for secure communications
  - **Hyperion**, a cyber security technology designed to look inside an executable program and determine software's function or behavior without the use of the software's source code.
  - **BEHOLDER**, technology being developed by ORNL in partnership with General Electric Research to exploit fine-grained timing data collected from remote network and SCADA (supervisory control and data acquisition) devices to reveal the presence of software and network intrusions.

National Laboratory Partnerships for Cyber-Physical Security

- **Cybersecurity Risk Information Sharing Program (CRISP)**
  - Partnership between PNNL, INL, ANL, and ORNL funded by DOE
  - Provide cyber threat information to industry partners
- **Cyber Analytic Tools and Techniques (CATT)**
  - Partnership between PNNL, INL, ANL and ORNL funded by DOE/OE and DOE/IN
  - Provide automated & advanced cyber analytics capabilities for industry partners and IC
- **Cybersecurity R&D Gap Analysis**
  - Partnership between PNNL, ANL, LLNL, ORNL, and Battelle Memorial Institute
  - Two-year effort to determine cybersecurity R&D gaps and develop way-ahead strategy

National Electric Grid Cybersecurity R&D Needs

- **Anticipatory Threat Determination**: the ability to provide threat predictions to accurately predict emerging/advanced threats
- **Dynamic Resource Allocation:** the ability to dynamically sense a given network and adapt its resources to "harden" critical resources based on realized environment changes
- **Alternative Timing Capabilities:** the ability to use non-GPS timing systems to avoid spoofing of critical timing signals
- **Real-time Device and User Authentication:** the ability to ensure that devices/software have not been tampered with as well as granting user access based on multiple levels of authentication