Statement of Thomas Zacharia, Ph.D.
Deputy Director for Science and Technology, Oak Ridge National Laboratory

Before the
Subcommittee on Energy
Committee on Energy and Natural Resources
U.S. Senate
March 28, 2017

Chairman Gardner, Ranking Member Manchin, and Members of the Committee: Thank you for the opportunity to appear before you today. I am Dr. Thomas Zacharia, Deputy Director of Science and Technology at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. It is an honor to provide this briefing on cybersecurity threats to the US electric grid and technology advancements to minimize those threats.

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, 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 and its critical infrastructure, and the world more secure.

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 (third largest 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;
- 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 the deputy director for science and technology of a national laboratory with an intense focus on solving compelling national problems in energy and security. These problems are closely linked, in that energy security is a vital component of our national security.

Oak Ridge National Laboratory has a long and storied history in working with the electric utility industry to solve complex problems. This has included working with public utilities, large investor-owned companies, municipalities, as well as rural electric cooperatives.

ORNL researchers have developed highly secure Internet of Things (IoT) sensors and systems specifically designed to provide enhanced measurements for improving electric grid operations. Such devices have been installed at Chattanooga Electric Power Board (EPB) substations and are providing extended grid operation measurements to EPB's control center.

ORNL has been engaged with electric utilities and rural co-ops regarding the use of small unmanned aerial systems (UAS)—commonly called "drones"—through our UAS Research Center. A 168-page best practices guide for electric utility usage of drones for system inspections was released this month with more than 3,000 downloads.

Private industry has already developed innovative solutions to secure the grid, but the task is becoming increasingly difficult due to more and progressively sophisticated cyberattacks. New vulnerabilities, such as distributed power generation and the growing number of Internet-connected devices on the system, present additional challenges.

Supply chain vulnerability adds additional complexity to cyberdefense and requires more action. The vulnerabilities encompass technology systems and processes that are typically the responsibility of non-utility organizations like instrumentation, information technology, and control system providers.

SB 79 addresses an approach to deal with the vulnerability of critical components for the electric grid supply chain. The intent of the bill focuses on a critical need to evaluate technology platforms and standards. The next step should be to engage industry, national labs, and academia to develop a national cyber-informed engineering strategy to isolate and defend entities.

What makes the grid smart are the interconnections that enable communications between devices, which in turn make the system more agile, adaptive, and able to preempt disturbances. However, information technology devices embedded throughout the system also create more access points for potential disruption.

According to David Johnson, EPB chief technology officer and vice president for information technology, cybersecurity defense is a daily challenge as the utility fights back against denial of service attacks, physical system attacks, malicious intent attacks, and authentication attacks. "The challenge in today's technology environment is to secure our systems without inhibiting

productivity or service to our customers. The single largest threat to EPB cybersecurity is connection to the public Internet," Johnson said.

Reliance on the Internet for non-secured business connectivity, technical supports for products, and data exchange is the core electric grid attack vector at present. I believe that the experts from EPB are correct that a sustainable solution to electrical grid security is the elimination of the grid's direct connectivity to the Internet, as David Johnson noted.

With the growing sophistication of cyberintrusions, we need to go beyond today's practices. The nation's electric grid needs a new solution, and it needs it now.

With DOE and electric utilities, we have been exploring ways to get critical infrastructure off the public Internet. Some utilities are already moving in this direction by creating a separate architecture for their communications systems. But insulating the grid from increasingly complex attacks requires a multidisciplinary effort that perfectly aligns with the mission of the national laboratories.

GRID VULNERABILITY: A NATIONAL SECURITY THREAT

What's at Stake

The nation's electric grid is a vital resource upon which our economy and citizens' daily lives depend. But it is a system that is uniquely vulnerable to cyberattack at a time when more utility controls and "smart" technology are connected to the public Internet than ever.

The grid is an integral part of the life of every human being living in a developed society. On a personal level, electricity powers many creature comforts in the home, and many conveniences that ease everyday living. Electricity powers commercial and industrial enterprises—the engines of present-day economies. Even for those commercial and industrial processes using other fuels, electricity powers the control systems inherent in those processes. There is no aspect of modern civilization that is not impacted—directly or indirectly—by the electric grid.

There are close inter-dependencies between various critical infrastructures. The telecommunications grid, for instance, carries the signals used to control all aspects of the electric grid. The electric grid, in turn, powers the components of the telecommunications grid. While emergency operating procedures can mitigate the loss of services, neither grid can maintain sustained long-term operations without the other.

Technological Solutions

The national laboratory system is uniquely positioned to address cybersecurity challenges through technology breakthroughs in partnership with the private sector. At Oak Ridge National Laboratory, expertise and capabilities in high-performance computing, data and graph analytics, discrete mathematics, power systems and engineering, embedded systems and wireless technologies, sensors and controls are critical to provide solutions and breakthroughs to detect and deter cyberattacks. ORNL has a long history of discovery and innovations in power systems and critical infrastructure protection technology development and assessment. The lab possesses the capabilities to produce advanced solutions for industry and federal, state, and local agencies.

Specifically, the following technological advancements and solutions are needed to ensure a reliable, efficient, resilient, secure grid infrastructure across the country:

1. Eliminate direct connectivity to the Internet. Taking a page from global cloud firms that have established dedicated VPNs connecting their compute centers, the electric grid networks should be configured similarly, creating a closed and secure system with few, very well protected points of presence (POPs) to the external networks. Those POPs must have the best technologies to ensure they cannot be breached. Dark fiber across the United States may provide a cost-effective protective measure, exploiting advanced communications (5G-LTE, satcom and private wireless) and cybersecurity technologies suitable for the expanding smart grid requirements.
2. Implement advanced cyberdefensive measures beyond what is possible on the public Internet. This includes innovative novel communication security approaches being applied in other sectors and evaluated on the energy infrastructure.
3. Develop supply chain components and Internet of Things devices with security built in.
4. Provide wide-area situational awareness and decision support by enhancing grid state monitoring with advanced sensing and measurements. Build off existing situational awareness tools Cybersecurity Risk Information Sharing Program (CRISP), and Environment for Analysis of Geo-Located Energy Information (EAGLE-I) technologies.
5. Use living laboratories in partnership with utilities and national laboratories to test functionality and resilience of advanced cyber- and cyberphysical solutions to accelerate transition to practice.

Advancements Made

ORNL has developed numerous technologies used in the conduct of cybersecurity (see Appendix A). 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).

Other cyber-physical tools and capabilities include GridEye sensors located across the U.S. for real-time systems monitoring, and EAGLE-I, Environment for Analysis of Geo-Located Energy Information, which monitors the nation's energy sector in real time. This can be leveraged with the PNNL-led effort on the Cybersecurity Risk Information Sharing Program (CRISP), to provide cyber threat information to industry partners.

Another good example is ORNL working with a private firm to further develop quantum key distribution (QKD) technology as a solution to harden the grid. The technology, called AQCESS (for Accessible QKD for Cost Effective Secret Sharing), greatly increases the number of nodes that can be supported by a single QKD channel. The nodes are cost-effective and can be added at any time, thereby reducing the per-node cost, while enhancing the flexibility and accessibility of a QKD network.

ORNL's unique expertise in advanced manufacturing has supported its creation of low-cost, 3D-printed sensors that can identify voltage issues and power failures as soon as they occur, as well as fuse performance analysis with weather and climate indicators, making grid security, regular maintenance, and disaster response more efficient and cost-effective. These devices can be manufactured in the US with built-in security.

In addition, ORNL is researching unique methods and technologies to harden the grid and its supply chain against harm, whether intended or not. These include: "Fingerprinting" technologies to monitor device behavior at the chip level to identify the presence of malware or attempts at spoofing that could cause harm to critical infrastructure; systems to replace reliance on GPS systems for timing signals and synchronization; and researching the task of getting the grid "off the Internet" by turning to private networks leveraging underutilized fiber optic capabilities.

The Importance of Partnerships

However, without our public-private partnerships, these technologies will not be adopted by industry. ORNL's industry partnerships have been essential to the development, testing, and deployment of innovative technologies to modernize the grid and protect it from both physical- and cyberattack.

ORNL works with several utilities on grid modernization and security innovations, including the Chattanooga Electric Power Board (EPB), Dominion, Duke Energy, Southern Company, and Tennessee Valley Authority.

For instance, ORNL and DOE have enjoyed a productive working relationship with the Chattanooga EPB. These efforts support America's technological leadership, national security, and the goal to create a new, more reliable, and affordable electric utility service for the Internet Age. The EPB smart grid and advanced communications network also make a living laboratory to test new technology developed by ORNL and other labs.

DOE and ORNL are also leveraging the EPB automated smart grid and fiber optic network infrastructure to develop next generation of cybersecurity defense systems, including next-generation quantum cyber security software that has the potential to prevent undetected hacker intrusions into IT networks. The software will be tested in the coming year on EPB dark fiber and later as an integrated part of EPB normal electric system operations data traffic. We will have the ability to test and measure its effectiveness. If could be a game changer for the future of electric grid security.

EPB Chairman Joe Ferguson recently remarked on the value of the DOE EPB working relationship: *"Since we started our partnership with DOE over 3 years ago we have enjoyed real success, the kind of success that makes a difference to EPB business capabilities and to the quality of life enjoyed by the people of our community. I have no doubt that we have just begun to realize the benefits of our success. Together we will go on to even greater achievements in future for all of the people of our country."*

NATIONAL LABORATORY EXPERTISE AND CAPABILITIES

DOE's scientific and technical capabilities are rooted in its system of national laboratories—17 world-class institutions that constitute the most comprehensive research and development network of its kind (see Appendix B). The laboratories work as a network with industry, academia, and other federal agencies to focus on complex, mission-critical research and development activities.

The national laboratories:

- Work at the forefront of fundamental research, unveiling secrets of the basic building blocks of matter and are creating a new generation of materials (including biological and bio-inspired materials) to underpin advances in energy generation, storage, transmission, efficiency, and security.
- Lead in RD&D that supports the national security missions of DOE, and they partner with industry, academia, and other Federal agencies to provide innovative solutions in the broader areas of defense, homeland security, cybersecurity, and intelligence.

Through these activities—conducted at large scales and with significant, long-term investments of resources, including world-class scientific and technical expertise—DOE's national laboratory enterprise serves as an enduring science and technology powerhouse for the nation.

One example of the laboratories working together on major challenges is the Grid Modernization Laboratory Consortium (GMLC). This was established as a strategic partnership between DOE and the national laboratories to bring together leading experts, technologies, and resources to collaborate on the goal of modernizing the nation's grid. The benefits of the GMLC include more efficient use of resources; shared networks; improving learning and preservation of knowledge; enhanced lab coordination and collaboration; and regional perspective and relationships with local stakeholders and industry.

The United States is unique in the breadth and depth of scientific and engineering excellence possessed by its national laboratories and will continue to play a continued leading role in grid modernization, reliability, security and resilience.

CLOSING REMARKS

Sometimes called the world's largest machine, the electric grid is the cornerstone of our economic foundation, U.S. competitiveness, and our way of life. DOE's national laboratory system stands ready to work closely with industry and other institutions to plan and create innovative technical solutions to protect our grid. Thank you again for the opportunity to provide this briefing. I welcome your questions on this important topic.

APPENDIX A

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

The National Laboratory complex is well-suited to explore and develop technological solutions towards protecting the energy grid. Partnerships with government, industry and academia have been 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)** is 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** is a comprehensive, real-time energy monitoring dashboard developed by DOE/OE for integration with VERDE
  - **Oak Ridge Cyber Analytics (ORCA)** is a real-time cybersecurity platform for detecting advanced persistent threats and 0-day exploits
  - **Situ** is 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** is 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** in partnership with General Electric Research, ORNL is developing technology that exploits 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
  - Two year effort to determine cybersecurity R&D gaps and develop way-ahead strategy

National Electric Gird 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

APPENDIX B

Map of the DOE Laboratory System