SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

February 14, 2019

STATEMENT FOR THE RECORD FROM
DAVID EDWARD WHITEHEAD, CHIEF OPERATING OFFICER
SCHWEITZER ENGINEERING LABORATORIES, INC.
SUBMITTED TO THE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
U.S. SENATE
HEARING TO
"CONSIDER THE STATUS AND OUTLOOK FOR CYBERSECURITY
EFFORTS IN THE ENERGY INDUSTRY"

Chairman Murkowski, Ranking Member Manchin, and members of the Committee, thank you for the opportunity to share the views of Schweitzer Engineering Laboratories (SEL) on the important topic of securing our critical electric infrastructure from cyber threats.

SEL is an employee-owned U.S. manufacturer and provider of products, systems and services for the protection, monitoring, control, automation and metering of utility and industrial electric power systems worldwide. Our mission is to make electric power safer, more reliable and more economical. We are headquartered in Pullman, Washington, and employ 3,700 in the United States with a total of 5,200 employees around the world.

As is highlighted by today's hearing, cybersecurity is a critical component for secure and reliable operation of electric power systems. For 35 years, SEL has emphasized the importance of security in the products and solutions we create. When our first product was released in 1984, we had the foresight to incorporate multiple levels of password protection as well as physical alarms to signal unauthorized access attempts to equipment —something no one else in the industry was doing at the time. Today, whether it's regulatory compliance, securing power system assets or protecting operational technology networks, SEL offers security-focused solutions to help utilities protect electric networks and help vital industries protect their assets.

For most of its history, the bulk power system operated reliably and securely without communications. While the benefits of communications technologies have greatly enhanced the monitoring, automation and control capabilities of electric power systems, it is necessary to ensure communications systems are secure. I do not believe our security challenges are insurmountable.

Today, I would like to highlight three topics that I believe are critical to the cybersecurity challenges we face in the energy industry and our nation. First, I will review what we see as an essential role of government— "teaching the threat." Second, I will discuss

the difficult act of balancing regulation and innovation. Third, I will provide a few examples of how industry is actively addressing cybersecurity threats.

Point #1: *Teaching the threat.* We read in the news weekly, sometimes daily, about advanced, persistent threats from nation-states. Clearly, our adversaries are becoming more sophisticated in the way they target our critical infrastructure. We are constantly having to evolve our thinking and innovate against these threats. At SEL and other like-companies, we have some of the best engineers in the world doing just that. What we do not possess is access to the vast and sophisticated intelligence and information gathering that exists in our country. The U.S. government has the capabilities to identify, classify and communicate these threats. Sharing information with asset owners and equipment manufactures through a just-in-time approach is critical to keeping our systems and electrical infrastructure safe. It has been my experience that asset owners take cybersecurity seriously and will act if they understand the threat. At SEL, we take cybersecurity threats very seriously and we act immediately when we receive information. Many in our industry already have positive working relationships with various government agencies. Building out a more robust system of communication where government agencies move quickly and efficiently to share important information—to teach us about potential or actual threats—will only make our systems more secure.

Point #2: *Balancing regulation and innovation*. SEL is a company built on the foundation of innovation. At the entrance of our research and development building in Pullman, Washington, these words are boldly displayed: “The best way to predict the future is to invent it.” Our R&D researchers and inventors pass by this quote daily. Interestingly, our practice of building cybersecurity into everything we make was a concept learned by our founder early in his career while working for the Department of Defense.

Innovation and regulation do not have to be at odds with each other. Regulations, however, are often implemented as a reaction to an undesired event. Developing a regulation may be fine to address static situations, but cyber is a dynamically changing environment. As soon as a regulation is enacted to address a specific issue or event, bad actors are already looking for other avenues of exploitation.

Regulations have the capacity to limit how an institution may go about solving a problem. For example, if a new and innovative solution does not conform to regulations but is the best way to address a security element at a company, the company may choose not to employ the solution, or worse, be fined for noncompliance if they chose to use that solution. Further, regulations will never be able to anticipate new and innovative solutions. For example, NERC CIP-005-5 requires multifactor authentication for all Interactive Remote Access sessions. What happens when new and potentially more effective authentication methods are developed?

As you are aware, a great deal of time is being spent discussing, debating, demonstrating and proving compliance. I believe this time could be better spent on creating and deploying innovative solutions that will keep us in front of threats.

There are clear and obvious needs for standards and regulation, and we are always ready to work together to create solutions, but we should be encouraged to work together in finding ways to continue fostering critical innovation that outpaces our adversaries. We cannot allow bad actors, who are unconstrained by regulations, to outpace us.

Point #3. *Industry is actively addressing cybersecurity threats.* There is so much cutting-edge work being done in our industry to keep ahead of cyber threats. During the past 35 years since the development of our first product, SEL has continuously advanced our cyber security solutions. As systems became more integrated, we moved to a security-in-depth approach—building layers of security so that systems are not dependent on one security feature, but instead consist of many layers. And solutions range from simple to very sophisticated. I remind folks to never connect critical infrastructure to the internet; audit this—a simple solution. Software-Defined Networking is emerging as the solution for engineered and cyber-secured industrial networking.

SEL is partnering with universities, including Washington State University, University of Idaho, Montana Tech and Purdue, to develop new ways to secure industrial networks. We have participated in the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program. Under the CEDS program, SEL has partnered with utilities and national laboratories across the country to identify, design and test new solutions for protecting critical infrastructure from cyber-attacks.

The federal government is not the only entity paying attention to cybersecurity; industry is addressing cybersecurity too. Last week, I had the opportunity to attend DistribuTECH, an electric power industry conference. It was exciting to see cutting-edge cyber solutions being offered by both new startups and well-established suppliers. There are many brilliant minds working diligently to solve cybersecurity challenges.

As new threats emerge—and they will—industry and government must work together and learn from each other to effectively secure our critical infrastructure. And I know we can.

Thank you for the opportunity to testify, and I look forward to any questions you may have.