Testimony of

William H. Sanders

Donald Biggar Willett Professor of Engineering
Head, Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Before the
United States Senate
Committee on Energy and Natural Resources

March 1, 2018

Introduction

Good morning Chairwoman Murkowski, Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak today.

I am a Donald Biggar Willett Professor of Engineering and the Head of the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. I was the founding director of the Information Trust Institute at the University of Illinois and served as director of the Coordinated Science Laboratory at Illinois. I am a professor in the Department of Electrical and Computer Engineering and in the Department of Computer Science. I am a Fellow of the IEEE, the ACM, and the AAAS; a past chair of the IEEE Technical Committee on Fault-Tolerant Computing; and past vice-chair of the IFIP Working Group 10.4 on Dependable Computing.

I am an expert on secure and dependable computing with a focus on critical infrastructures. I have published more than 270 technical papers in those areas. I was the 2016 recipient of the IEEE Innovation in Societal Infrastructure Award for "assessment-driven design of trustworthy cyber infrastructures for electric grid systems." Since 2005, I have led or co-led major government-funded academic research centers (TCIP, TCIPG, and CREDC) that work to make the grid secure and resilient. I was also a member of the committee that wrote the National Academies of Sciences, Engineering, and Medicine consensus report entitled "Enhancing the Resilience of the Nation's Electricity System." In short, my experiences provide me with a unique perspective to offer the Committee insight and recommendations concerning the impairments to and approaches for providing cybersecurity and cyber resiliency in the nation's energy infrastructure.

In my remarks today, I will:

- Describe the concept of cyber resiliency and the importance of resiliency in the cyber systems that control the grid,

(Portions of this testimony were taken verbatim from the National Academies of Sciences, Engineering, and Medicine report "Enhancing the Resilience of the Nation's Electricity System, ISBN 978-0-309-46307-2 | DOI 10.17226/24836, available at http://nap.edu/24836 and the associated "Report in Brief")

- Describe the unique contribution universities (including Illinois) play in developing new, innovative technologies and approaches to preventing, detecting, and recovering from cybersecurity threats to the grid,
- Make specific recommendations of research to enhance the resiliency of the cyber portion of the power grid to attacks, and
- Argue that Congress should continue to fund and increase funding to DOE and other government agencies to advance this research.

Cyber Resiliency

"Resiliency" is a fundamental concept that differs from traditional metrics such as reliability or cybersecurity. In the context of electric power, resiliency is not just about being able to lessen the likelihood that outages will occur, but also about managing and coping with outage events when they do occur. The goal is to lessen outage impacts, regrouping quickly and efficiently once an event ends, and, in the process, learning to deal with other events better in the future.

Stephen E. Flynn (2008) has outlined a four-stage framing of the concept of resilience: (1) preparing to make the system as robust as possible in the face of possible future stresses or attacks; (2) relying on resources to manage and ameliorate the consequences of an event once it has occurred; (3) recovering as quickly as possible once the event is over; and (4) remaining alert to insights and lessons that can be drawn (through all stages of the process) so that if and when another event occurs, a better job can be done at all stages.

With resiliency, we attempt, to the greatest extent possible, to avoid a large-scale event (in this case, a long-term blackout), but understand and accept that it may not be totally possible to avoid an event, and thus work to respond as quickly as possible to the event once it occurs—preserving "critical" individual and societal services during the period of degraded operation—and, over time, strive for full recovery and enhanced robustness to further impairments that could result in additional large-scale events.

Because the power system is hierarchical, these same concepts apply at several different levels of the system, including across the high-voltage grid, the regional grids (some of which are operated by regional transmission organizations), local transmission and distribution systems (typically the domain of utilities), and the end-user level (on both the utility and customer sides of the meter), and across both the cyber and conventional physical portions of the power grid. It is also clear that the resiliency of the power grid is critically dependent on other interconnected infrastructures (e.g., oil and gas).

A relatively new concern, and the subject of my core expertise, is the resiliency of the cyber portion of the grid, and how it affects overall grid resiliency. The electric power system has become increasingly reliant on its cyber infrastructure to deliver electricity to the consumers. This infrastructure includes computers, communication networks, other control system electronics, smart meters, and other distribution-side cyber assets. A compromise of the power grid control system or other portions of the grid's cyber infrastructure can have serious consequences, ranging from a simple disruption of service with no damage to the physical components to permanent damage to hardware that can have long-lasting effects on the

performance of the system. Any consideration of improved power grid resiliency requires consideration of ways to improve the resiliency of the grid's cyber infrastructure.

Over the last decade, much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resiliency. The sources of guidance on protection as a mechanism to achieve grid cybersecurity are numerous. It is now, however, becoming apparent that protection alone is not sufficient and can never be made perfect. Cybercriminals are difficult to apprehend, and there are nearly 81,000 vulnerabilities in the NIST National Vulnerability Database (NVD). An experiment conducted by the National Rural Electric Cooperative Association and N-Dimension in April 2014 determined that a typical small utility is probed or attacked every 3 seconds around the clock. Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable, and there is evidence of increases in the rate of penetration in the past year.

Fortunately, the successful attacks to date have largely been concentrated on utility business systems, as opposed to monitoring and control systems (termed "operational technology" or "OT" systems), in part because the operational technology systems have fewer attack surfaces, fewer users with more limited privileges, greater use of encryption, and more use of analog technology. However, there is a substantial and growing risk of a successful breach of operational technology systems, and the potential impacts of such a breach could be significant. These risks are growing in part because, as the grid is modernized, there is greater reliance on grid components with significant cyber controls. In addition, further integration of operational technology systems with utility business systems, despite its potential for increased efficiency, also poses serious risks.

Given that protection cannot be made perfect, and the risk is growing, cyber resiliency is critically important. Cyber resiliency aims to protect through established cybersecurity techniques, but acknowledges that such protections can never be perfect, and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some solutions from classical cybersecurity can support cyber resiliency (e.g., intrusion detection and response), the majority of the cybersecurity work to date has focused on preventing the occurrence of successful attacks, rather than detecting and responding to partially successful attacks that occur.

In contrast, a cyber resiliency architecture should implement a strategy for mitigating cyberattacks and other impairments by monitoring the system and dynamically responding to perceived impairments to achieve resiliency goals. The resiliency goals for the cyber infrastructure require a clear understanding of the interaction between the cyber and conventional physical portions of the power grid, and how impairments on either side (cyber or physical) could impact the other. By their nature, such goals are inherently system-specific, but as a general principle they should balance the desires to minimize the amount of time a system is compromised and maximize the services provided by the system. Often, instead of taking the system offline once an attack has been detected, a cyber-resilient architecture attempts to heal the system while providing critical cyber and physical services. Based on the resiliency goals, cyber resiliency architectures typically employ sensors to monitor the state of the system on all levels of abstraction and detect abnormal behaviors. The data from multiple levels are then fused to create higher-level views of the system. Those views aid in detecting attacks and other cyber and

physical impairments, and in identifying failure to deliver critical services. A response engine, often with human input, recommends the best course of action. The goal, after perhaps multiple responses, is complete recovery, i.e., restoring the cyber system to a fully operational state.

TCIP/TCIPG and CREDC

These findings have grown out of collaborative academic-industry-government settings, including three major research activities that I have led or co-led over the last twelve years. In particular, I served as the Director and Principal Investigator (PI) of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center and currently serve as a co-PI of the Cyber-Resilient Energy Delivery Consortium (CREDC), which conducts research at the forefront of national efforts to make the U.S. power grid resilient.

The Trustworthy Cyber Infrastructure for the Power Grid projects (TCIP, 2005–2010; and TCIPG, 2009–2015), which were partnerships of four academic institutions, were conducted to meet the challenge of making the electricity grid resilient. The initial TCIP project (of which I was also Director and PI) was funded primarily by the National Science Foundation, with additional support by the Department of Energy's Office of Electricity Delivery and Energy Reliability, and by the Department of Homeland Security's Science and Technology Directorate, HSARPA, Cyber Security Division. The subsequent TCIPG project was funded by the Department of Energy's Office of Electricity Delivery and Energy Reliability with partial support from the Department of Homeland Security's Science and Technology Directorate, HSARPA, Cyber Security Division.

In those projects, we collaborated with national laboratories and the utility sector to protect the U.S. power grid by significantly improving the way the power grid infrastructure is designed, making it more secure, resilient, and safe. In both technology and impact, TCIP/TCIPG was a successful partnership of government, academia, and industry, creating multiple startup companies (including Network Perception, Inc., which I co-founded) and transitioning multiple technologies to industry (including First Energy, Schweitzer Engineering Laboratories, ABB, Honeywell, Ameren, Telecordia, GE, Entergy, EPRI, DTE Energy, and PJM, among others). The projects also had a significant positive impact on workforce education, delivering successful short courses, producing graduates, and providing the knowledge necessary to do interdisciplinary work of the same type at other universities.

CREDC (funded by the Department of Energy Office of Electricity Delivery and Energy Reliability with support from the Department of Homeland Security's Science and Technology Directorate, HSARPA, Cyber Security Division) is a partnership of 10 academic institutions and 2 national labs that performs research and development in support of the Energy Sector Control Systems Working Group's Roadmap of resilient Energy Delivery Systems (EDS) that focuses on the cybersecurity of EDS. In doing so, CREDC addresses the cybersecurity of power grids, as well as oil and gas refinery and pipeline operations. To do this, CREDC is developing projects with significant and measurable sector impact, involving industry partners (asset owners, equipment vendors, and technology providers) early and often, with activities that range from helping to identify critical sector needs, to performing pilot deployment and technology adoption. In fact, Robert M. Lee, who is also testifying here today, is a CREDC industrial advisory board member.

While progress is being made, further work is critically needed to define cyber resiliency architectures that protect against, detect, respond to, and recover from cyber attacks that occur.

National Academy Recommendation Regarding Cyber Resiliency of the Grid

Specific guidance about cyber resiliency research that is critically needed comes from a consensus study published in July 2017 by the National Academies of Sciences, Engineering, and Medicine entitled "Enhancing the Resilience of the Nation's Electricity System."

The study focused largely on reducing the nation's vulnerability to large-area, long-duration outages—those that span several service areas or even states and last three days or longer. It found that much can be done to make both large and small outages less likely, but they cannot be totally eliminated, no matter how much money or effort is invested. To increase the resilience of the grid, our report argues that the nation must not only work to prevent and minimize the size of outages but must also develop strategies to cope with outages when they happen, recover rapidly afterward, and incorporate lessons learned into future planning and response efforts.

As one of the co-authors of the report, I helped craft seven overarching recommendations. One of these recommendations is particularly relevant to the concept of cyber resilience:

Overarching Recommendation 5: *The Department of Energy, together with the Department of Homeland Security, academic research teams, the national labs, and the private sector, should carry out a program of research, development, and demonstration activities to develop and deploy capabilities for the*

- *continuous collection of diverse (cyber and physical) sensor data;*
- *fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);*
- *visualization techniques needed to allow operators and engineers to maintain situation awareness;*
- *analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;*
- *restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and*
- *creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.*

Those six capabilities—(1) continuous data collection, (2) fusion of sensor data, (3) visualization, (4) analytics, (5) restoration, and (6) post-event tools—are critical elements of an effective strategy for cyber resiliency. These capabilities can be achieved only if academia, industry, and government work closely together in a focused research and development program.

Summary

The cyber threat to grid resiliency is real, and the time to act is now. It is critical that the committee understands the following:

1) Grid resiliency is different from cybersecurity and requires a fundamentally new approach.
2) With grid resiliency, we attempt, to the greatest extent possible, to avoid long-term blackouts, but understand and admit that it may not be totally possible to avoid them, and thus we work to respond as quickly as possible to the event once it occurs (preserving "critical" services during the period of degraded operation) and, over time, strive for full recovery and enhanced robustness.
3) The grid can be resilient only if its cyber infrastructure is resilient, so research and development are critically needed that provide assured mechanisms to ensure cyber resiliency.
4) Six capabilities—(1) continuous data collection, (2) fusion of sensor data, (3) visualization, (4) analytics, (5) restoration, and (6) post-event tools—are critical to creating an effective strategy for cyber resiliency.
5) Those capabilities can be achieved only if academia, industry, and government work closely together in a focused research and development program.
6) Congress should continue to fund and increase funding to DOE and other government agencies to advance this research.

Thank you for the opportunity to be here with you today. I would be happy to answer any questions that you have.