U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON ENERGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

Cybersecurity for Power Systems

HEARING CHARTER

Wednesday, October 21, 2015
10:00 a.m. – 11:30 a.m.
2318 Rayburn House Office Building

PURPOSE

The Subcommittees on Energy and Research and Technology will hold a joint hearing titled *Cybersecurity for Power Systems* on Wednesday, October 21, 2015, starting at 10:00 a.m. in Room 2318 Rayburn House Office Building. The purpose of this hearing is to examine efforts by federal agencies, industry, and the Department of Energy national labs to mitigate cybersecurity threats to the U.S. power supply. Witnesses have been asked to outline operating techniques and technology that can be used to prevent system vulnerability to cyber-attacks in the electric sector. This hearing will explore solutions to mitigate cyber threats identified in a Committee hearing last September entitled *Examining Vulnerabilities of America's Power Supply*.[1]

WITNESSES

- **Mr. Brent Stacey,** Associate Lab Director for National & Homeland Science and Technology, Idaho National Lab
- **Mr. Bennett Gaines,** Senior Vice President, Corporate Services and Chief Information Officer, FirstEnergy Service Company
- **Ms. Annabelle Lee,** Senior Technical Executive in the Power Delivery and Utilization Sector, Electric Power Research Institute
- **Mr. Greg Wilshusen,** Director of Information Security Issues, Government Accountability Office

BACKGROUND

American critical energy infrastructure, including electrical power plants, transmission and distribution lines, oil and gas pipelines, and transformers and substations remain some of the most vulnerable critical infrastructure to cyber-attack. The Department of Homeland Security has designated the energy sector as one of 16 critical infrastructure sectors, largely due to the

[1] Information on the hearing available at: https://science.house.gov/legislation/hearings/examining-vulnerabilities-america-s-power-supply-0

"enabling function" energy contributes across all critical infrastructure sectors.[2] Maintaining the stability and security of the electric grid will require modernization of existing industrial control systems and increasing incorporation of two-way, internet connected systems to manage reliability as more distributed energy systems are introduced to the electric grid.[3]

As discussed during the Committee hearing last September, America's electric grid is being modernized through an increased use of "smart grid" technology and distributed energy sources. However, this modernization also increases the risk of cyber-attack.[4] While smart grid technology uses digital information and control technology to improve reliability, security, and efficiency of the electric grid, adding technology that increases the interconnectedness of industrial control and IT systems can increase its vulnerability to cyber-attack.[5]

System Vulnerabilities

One key area of vulnerability within the grid is the Supervisory Control and Data Acquisition (SCADA) system that has been in use since the 1970s. These legacy systems have historically consisted of remote terminal units often connected to mainframe computers via telephone lines or radio connections and were not connected to central IT networks. Over the years, electric grid modernization efforts have increasingly created more access points to these analog systems.[6] As these legacy systems were not designed with IT network vulnerabilities in mind, digital security features were not integrated into their industrial control systems.

The integration of distributed generation and digital operating systems in conventional power plants can also increase cybersecurity vulnerabilities for critical energy infrastructure. While distributed generation and micro-grids can increase grid resiliency in the event of a disruption, more access points for cyber-attacks are created as distributed energy sources and users (e.g., plug-in electric vehicles) are added to power grid.[7]

Another area of vulnerability for cyber-attack is the increasing integration of "smart grid" technology. In practice, the "smart grid" generally refers to a technology used to modernize utility electricity delivery systems using computer-based remote control and automation that incorporate two-way communication technology and computer processing that has been used for decades in other industries into functions on the electric grid.[8] While the vast majority of America's electric power grid today primarily delivers electricity in a one-way flow from

---

[2] Department of Homeland Security, *Critical Infrastructure Sectors*. Last updated August 26, 2015. Available at http://www.dhs.gov/critical-infrastructure-sectors

[3] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[4] Bartol, Nadia, *Statement before the Subcommittee on Oversight and Subcommittee on Energy, Committee on Science, Space, and Technology*. Examining Vulnerabilities of America's Power Supply, July 30, 2015. Available at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY21-WState-NBartol-20150910.pdf

[5] Department of Energy, Office of Electricity Delivery & Energy Reliability, *Smart Grid*. Available at: http://energy.gov/oe/services/technology-development/smart-grid

[6] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[7] Ibid.

[8] Ibid.

generator to outlet, the number of interconnected smart grid devices is only expected to grow, with industry experts estimating that there could be as many as 50 billion interconnected smart devices in the world by 2020.[9] This increased use of smart grid technology adding automatic two-way communication between distribution and consumption sites creates cybersecurity vulnerabilities to the system as a whole.[10]

In addition, the security and privacy measures built into smart electricity meters could put American consumers' personal information at risk, as these systems send data about energy use wirelessly to electric distribution companies and control the flow of power to customers.[11] Components of the smart grid are also controlled by software, which may make these devices and functions subject to manipulation over the network.

Ongoing Threats

While there has been no reported cyber-attack that has resulted in widespread loss of power, there have been many attempted attacks. An investigation completed by USA Today earlier this year found that the United States power grid "faces physical or online attacks approximately 'once every four days.'"[12] In addition, it appears that these cyber threats could be highly sophisticated. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[13] Increasing examples of cyber intrusions and malware (such as BlackEnergy, HAVEX, and Sandworm) on industrial control systems of critical infrastructure have also been reported. [14]

Federal Mitigation Efforts

Federal cybersecurity management, regulation, research, and development for energy systems is distributed between the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) the Department of Energy, the Department of Homeland Security, and the National Institute for Standards and Technology (NIST). The Energy Independence and Security Act of 2007 (EISA) established federal support for the modernization of America's electric grid and required actions on cybersecurity by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and DOE.[15]

---

[9] Bartol, Nadia, *Statement before the Subcommittee on Oversight and Subcommittee on Energy, Committee on Science, Space, and Technology*. Examining Vulnerabilities of America's Power Supply, July 30, 2015. Available at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY21-WState-NBartol-20150910.pdf

[10] National Institute of Standards and Technology, *Smart Grid: A Beginner's Guide*. Available at: http://www.nist.gov/smartgrid/beginnersguide.cfm

[11] Campbell, Richard J., *The Smart Grid and Cybersecurity – Regulatory Policy and Issues*. Congressional Research Service, June 15, 2011. Available at: http://www.crs.gov/pdfloader/R41886

[12] Ibid.

[13] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015. Available at: http://www.crs.gov/pdfloader/R43989

[14] Ibid.

[15] Wilshusen, Gregory. *Challenges in Securing the Modernized Electricity Grid*. Testimony

Today, NIST has developed *Guidelines for Smart Grid Cybersecurity*, a comprehensive, voluntary framework for industry to follow in developing effective cybersecurity strategies. NIST also led the development of the "Framework for Improving Critical Infrastructure Cybersecurity," outlining industry methodologies, procedures, and processes to synchronize approaches to address cyber risks.[16] FERC, the federal regulatory agency, continues to approve industry cybersecurity standards developed and proposed by the private corporation NERC. NERC also manages the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which is designed to establish situational awareness, incident management, coordination, and communication capabilities across America's power grid operators through timely information sharing.[17]

The Department of Energy has established initiatives to facilitate development of industry tools for voluntary risk assessment and smart grid technology, and the Department of Energy National labs provide risk assessment, modeling, and technology development expertise, including the Cyber Security Test Bed at Idaho National Lab that allows industry to test control systems under the conditions of a cyber-attack.[18] The Department of Homeland Security operates the National Cybersecurity and Communications Integration Center (NCCIC) to facilitate information sharing between public and private entities to reduce vulnerabilities and improve mitigation and recovery response, as well as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), designed to strengthen industrial control systems in electric systems.[19]

Due in part to the number of agencies involved in the process, federal and state cyber threat mitigation efforts are often burdened by different and unclear regulatory authorities, lack of monitoring to ensure industry standards are met, slow communication between agencies, and effective information sharing between industry and relevant federal entities. These challenges have been repeatedly identified by the Government Accountability Office (GAO).[20]

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. February 28, 2012. Available at http://gao.gov/assets/590/588913.pdf

[16] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* . February 12, 2014, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[17] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015. Available at: http://www.crs.gov/pdfloader/R43989

[18] Idaho National Laboratory. *INL Cyber Security Research: Defending the Network Against Hackers.* Department of Energy. Available at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-INL_Cyber_Security_Research.pdf

[19] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[20] Wilshusen, Gregory. *Challenges in Securing the Modernized Electricity Grid*. Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. February 28, 2012. Available at http://gao.gov/assets/590/588913.pdf

Additional References:

1. McMillian, Robert. “Cyber Risk Isn’t Always in the Computer: Vulnerable industrial systems that support data centers can open a back door to hackers” Wall Street Journal. Sept. 24, 2015. Available at http://www.wsj.com/articles/cyber-risk-isnt-always-in-the-computer-1443125108.

2. Reilly, Steve. “Bracing for a big power grid attack: 'One is too many'” USA Today. March 24, 2015. Available at http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/