Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Bill Shuster
Chairman

Christopher P. Bertram, Staff Director

Peter A. DeFazio
Ranking Member

Katherine W. Dedrick, Democratic Staff Director

April 8, 2016

SUMMARY OF SUBJECT MATTER

TO: Members, Subcommittee on Economic Development, Public Buildings, and Emergency Management

FROM: Staff, Subcommittee on Economic Development, Public Buildings, and Emergency Management

RE: Subcommittee Hearing on "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?"

PURPOSE

The Subcommittee on Economic Development, Public Buildings, and Emergency Management will meet on Thursday, April 14, 2016, at 10:00 a.m. in 2167 Rayburn House Office Building for a hearing titled "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?" The purpose of the hearing is twofold:

1. To explore the risks, vulnerabilities and consequences of a prolonged, widespread power outage and understand the primary federal roles, authorities and resources available to help communities, particularly at the local level, manage the aftermath of such a disaster; and
2. To assess the efforts and coordination among the participants—public, private and non-profit—in the electrical power sector, including planning, preparedness and mitigation efforts, response and recovery capabilities, information sharing, and standards setting.

The Subcommittee will receive testimony from the Federal Emergency Management Agency (FEMA), the Department of Energy (DOE), the Department of Homeland Security's National Protection and Programs Directorate, the Congressional Research Service (CRS), the North American Electric Reliability Corporation (NERC), and a representative from the electrical industry.

BACKGROUND

The Elements of the Electrical System

The electric grid is one of the Nation's most critical infrastructures. The bulk power system is a large, complex, and robust system of networked generation facilities, transmission and distribution lines, transformers and substations, and control and communication technologies which together, bring power to American homes and businesses (see Attachment A).

The Roles of Federal Entities

Federal Emergency Management Agency (FEMA)

FEMA coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror.

Department of Energy Office of Electricity Delivery and Energy Reliability

DOE serves as the sector specific lead agency for grid security. The Office of Electricity Delivery and Energy Reliability (OE) works to ensure that the Nation's energy delivery system is secure, resilient and reliable and develops new technologies to improve the infrastructure and the federal and state electricity policies and programs. OE also works to bolster the resiliency of the electric grid and assists with restoration when major energy supply interruptions occur.

The Fixing America's Surface Transportation Act, or the FAST Act (P.L. 114-94), amended the Federal Power Act (16 U.S.C. 824 *et seq.*) to: (i) require DOE to develop procedures to improve emergency preparedness for energy supply disruptions; (ii) authorize DOE to take measures to address Presidentially-declared grid security emergencies and protect the bulk power system or defend critical electric infrastructure; and (iii) require DOE to establish a strategic transformer reserve to store spare large power transformers and emergency mobile substations in strategically located facilities for use during emergencies.[1]

Department of Homeland Security (DHS)

DHS coordinates security information and preparedness for the Nation's critical infrastructure. The National Protection and Programs Directorate (NPPD) executes the Department's mission related to enhancing the resilience of the Nation's infrastructure against cyber and physical threats. NPPD collaborates with federal, state, local, tribal, territorial, international, and private-sector entities to maintain situational awareness of both physical and cyber events, share information about risks that may disrupt critical infrastructure, and build capabilities to reduce those risks. NPPD, through its cyber protection programs housed in the National Cybersecurity and Communications Integration Center (NCCIC), shares cyber threat and mitigation information with government, private sector, and academic partners drawing on its operators and analysts while ensuring continuity of national security and emergency preparedness communications.

[1] Conference Report 114-357 to accompany H.R. 22 FAST Act, December 1, 2015.

Federal Energy Regulatory Commission (FERC)

FERC oversees the development and enforcement of mandatory reliability standards for the bulk power system. With representatives of other federal and state agencies and the electric industry, FERC helps identify and address threats to energy infrastructure security. The Federal Power Act directs FERC to work with an independent Electric Reliability Organization (ERO) to develop reliability standards for the bulk power system. In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the ERO.

Other Entities

North American Electric Reliability Corporation (NERC)

Pursuant to the Energy Policy Act of 2005, NERC develops and establishes consensus industry standards pursuant to an open and inclusive stakeholder process with FERC oversight and approval. NERC also regularly conducts outreach to and training for industry partners through assessments, exercises, webinars, and guidelines. In 2011, NERC facilitated the first-ever play exercise and executive tabletop discussion, or GridEx, for the Electricity Sub-sector in North America. NERC now holds a biennial distributed play exercise and executive tabletop discussion to exercise readiness, review plans, and explore policy decisions. On March 31, 2016, NERC released the findings of GridExIII held in November 2015 which "showed continued improvement to coordination, communication and emergency response actions to how industry would respond to a cyber or physical attack from previous exercises."

Electricity Subsector Coordinating Council (ESCC)

Formed in 2013, the ESCC is the principal liaison between the electric sector and the federal government for coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Electric company CEOs and senior Administration officials from DOE, DHS, the White House, and the Federal Bureau of Investigation (FBI) meet regularly to focus primarily on three key areas: tools and technology, information flow, and incident response. The ESCC focuses on threat mitigation through preparation, prevention, response, and recovery.

Electricity Information Sharing and Analysis Center (E-ISAC)

The E-ISAC gathers information from electric industry participants about security-related events, disturbances, and off-normal occurrences within the Electricity Sub-sector and shares that information with key governmental entities. In turn, these governmental entities provide the E-ISAC with information regarding risks, threats, and warnings that the E-ISAC then disseminates throughout the Electricity Sub-sector.

For example, immediately after a 2013 sniper attack on the Pacific Gas and Electric's Metcalf substation, located in California, the E-ISAC alerted industry of the event and provided advice on steps to mitigate and protect against such attacks. In addition, the E-ISAC, DOE, FERC, DHS, and FBI conducted outreach to raise awareness of the event, inform industry of mitigation activities, and provide a forum for industry to meet with state, local, and federal authorities to discuss physical security concerns. This was an unprecedented public-private

partnership effort to address physical security concerns and involved U.S. and Canadian interests.

Threats to the Grid

Any of the grid elements can be damaged by natural events, such as severe storms or geomagnetic disturbances, as well as intentional, malicious events, such as cyber and physical security attacks. Incidents may disrupt the flow of power or reduce the reliability of the system. Several, if not all, of the other critical infrastructure sectors, are dependent on electric power. Simply put, a massive power outage could interfere with the everyday lives of millions of Americans.

Cyber Threats

The electric power industry has been making cybersecurity an increasing priority. The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks.[2] 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."[3]

The electric power industry is the only critical infrastructure industry with mandatory and enforceable cybersecurity standards. NERC as the designated ERO, worked with the electric power industry to develop Critical Infrastructure Protection (CIP) standards, which were approved by FERC in 2008, making them mandatory for bulk electric system owners and operators. Since 2008, the standards have been updated as the threat landscape evolves.

Physical Threats

Unlike cyber threats, which are constantly evolving, many threats to physical infrastructure have been known for years, if not decades, and are more readily understood. Electric utilities take these threats seriously and deploy measures to mitigate such threats.

Simple mitigation techniques like cameras and locks can help utilities deal with routine problems. The key to electric utility physical security, however, is the industries' ''defense-in-depth'' approach, which uses modeling to assess criticality and to build redundancies, resiliency and the ability to recover, should an extraordinary event occur. While systems are built to withstand attacks, successful attacks may still occur even with such planning.

The topic of physical security has become more prominent since the 2013 sniper attack on the Metcalf substation. After that event, the entire electric sector assessed its impacts and shared lessons learned. DOE and DHS, in coordination with the FBI, the E-ISAC and industry experts, also held a series of briefings for utility owners and operators and local law enforcement regarding security of electric substations.

---

[2] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Monitor (ICS-MM201212), October-December 2012, Original release date: January 02, 2013 | Last revised: February 19, 2014 available at https://ics-cert.us-cert.gov/monitors/ICS-MM201212.

[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 .

Consequences

Examples of consequences of events impacting the grid include:

- The 2003 blackout in Ohio, caused by a tree branch coupled with software issues and human error, was blamed for contributing directly to ten deaths with further indirect impact on the surrounding population. It took two days to return electricity to the entirety of the affected area.[4]
- After Superstorm Sandy in 2012, millions of people were left without power. Despite broad disaster relief efforts, it took thirteen days to restore power to at least 95 percent of customers in New York and eleven days to restore power to 95 percent of customers in New Jersey.[5]
- The Metcalf substation attack in 2013 caused over $15 million in damage, but did not lead to any loss of power or life.[6]

[4] Barron, James, "THE BLACKOUT OF 2003: The Overview; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS," N.Y. Times, available at http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html?pagewanted=all .

[5] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "Comparing the Impacts of Northeast Hurricanes on Energy Infrastructure, " April 2013, available at http://www.oe.netl.doe.gov/docs/Northeast%20Storm%20Comparison_FINAL_041513c.pdf .

[6] Smith, Rebecca, "Assault on California Power Station Raises Alarm on Potential for Terrorism," Wall Street Journal, February 5, 2014, available at http://www.wsj.com/articles/SB10001424052702304851104579359141941621778 .

WITNESS LIST

PANEL 1

The Honorable W. Craig Fugate
Administrator
Federal Emergency Management Agency

Ms. Patricia A. Hoffman
Assistant Secretary
Office of Electricity Delivery & Energy Reliability

Ms. Caitlin A. Durkovich
Assistant Secretary for Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Mr. Richard Campbell
Specialist in Energy Policy
Congressional Research Service

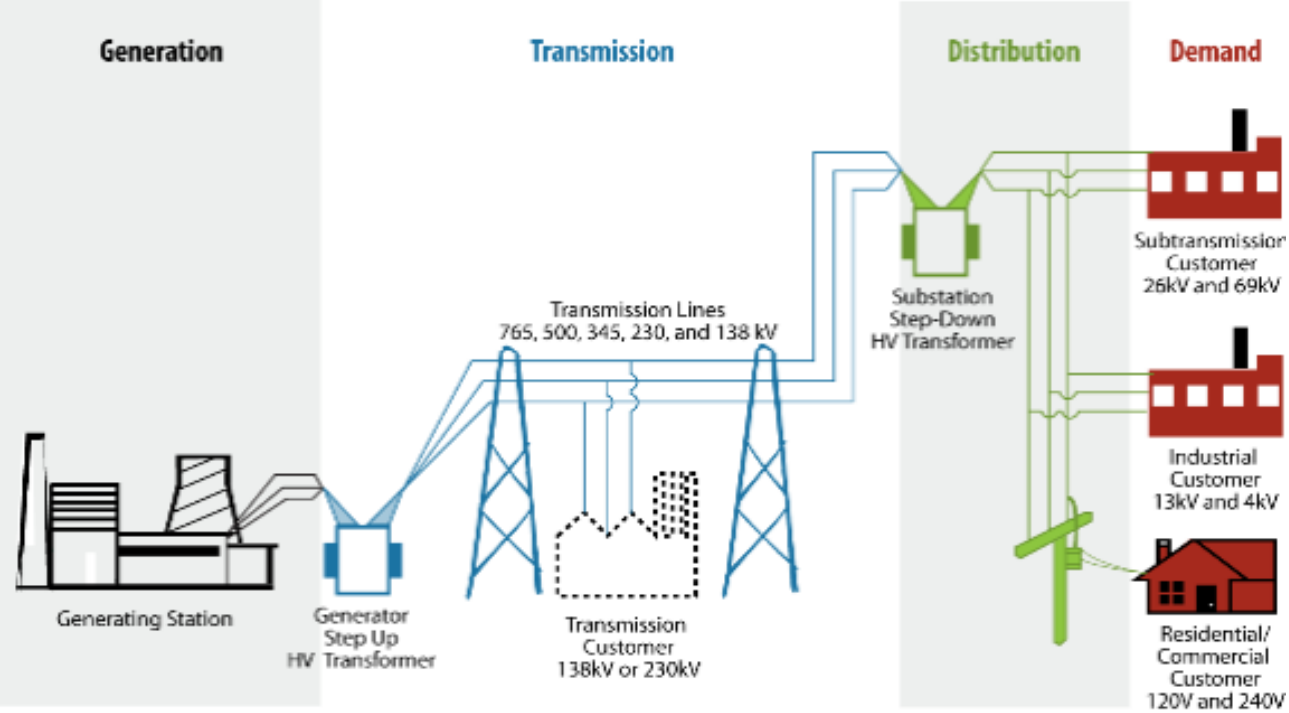
PANEL 2

Mr. Gerry W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation

Mr. William H. Spence
Chief Executive Officer
PPL Corporation

Ms. Bobbi J. Kilmer
President and CEO
Claverack Rural Electric Cooperative

Attachment A Electric Power System Elements



Source: Congressional Research Service, based on graphic found at https://reports.energy.gov/BlackoutFinal-Web.pdf .