Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM April 11, 2016

To: Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management
Attention: Pamela Williams

From: Richard Campbell, Specialist in Energy Policy, x 7-7905

Subject: **Testimony - Blackout! Are we Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?**

Good Morning Chairman, Ranking Member, and Members of the Subcommittee. My name is Richard Campbell. I am a Specialist in Energy Policy for the Congressional Research Service (CRS). On behalf of CRS, I would like to thank the Committee for inviting me to testify here today.

My testimony will provide background on the possible consequences of a failure of the electric grid, the roles and responsibilities of the respective parties, and some of the objective challenges in the recovery efforts. I should note that CRS does not advocate policy, or take a position on specific legislation.

Potential Failure of the Electric Grid

The electric power grid in the United States comprises all of the power plants generating electricity, together with the transmission and distribution lines and systems which bring power to end-use customers. The grid also connects the many publicly and privately owned electric utility and other wholesale power companies in different states and regions of the United States.[1] However, with changes in federal law,[2] regulatory changes, and modernization of the electric power infrastructure as drivers, the grid is changing from a largely patchwork system built to serve the needs of individual electric utility companies to essentially a national interconnected system, accommodating massive transfers of electrical energy among regions of the United States.

Electricity generation is vital to the commerce and daily functioning of United States. While the U.S. electric grid has operated historically with a high level of reliability, the various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events.

[1] As of 2013, there were 189 investor-owned electric utilities, 2,013 publicly-owned electric utilities, 887 consumer-owned rural electric cooperatives, and nine federal electric utilities. American Public Power Association, *U.S. Electric Utility Industry Statistics*, 2015, http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf.

[2] Key legislation includes the Public Utility Regulatory Policies Act of 1978 (P.L. 95-617, as amended), the Energy Policy Act of 1992 (P.L. 102-486), the Energy Policy Act of 2005 (P.L.109-58), and the Energy Independence and Security Act of 2007 (P.L. 110–140).

Electric power is generated and sent over transmission lines to substations which reduce the voltage levels for distribution to end-use customers. The cables carrying electric power to customers generally exist in an exterior or "above ground" environment largely exposed to the elements. As such, power outages can result from floods or seasonal storms which often combine the furies of wind, rain, snow, or ice. The more severe weather events can damage electric power transmission and distribution infrastructure as trees or overhanging branches fall on electricity lines. Most failures of the grid occur in local distribution systems rather than bulk power transmission systems, as the rights-of-way for transmission lines are wider, and are cleared to prevent damage from trees. The cost of weather-related power outages may range from $25 billion to $55 billion annually.[3]

Other impairment or failure of the grid can potentially result from attacks, terrorism, or even extremes of space weather. For example, a nuclear weapon exploded at a high altitude over the United States would cause an electromagnetic pulse which could destroy power transformers and other critical components. [4] Similarly, a severe solar storm could have damaging impacts on power transformers. Sunspots send plasma from coronal mass ejections into space, which could interact with the Earth's magnetic field causing ground induced currents powerful enough to overload transformers. The last major solar flare eruption in 1989 caused blackouts in the Canadian province of Quebec. Even greater solar storms occur in cycles of approximately 100 years, with major events being recorded in 1859 and 1921.[5]

Much of the infrastructure which serves the U.S. power grid is aging. As of 2009, the average age of power plants was over 30 years, with most of these facilities having a life expectancy of 40 years.[6] Electric transmission and distribution system components are similarly aging, with power transformers averaging over 40 years of age,[7] and 70% of transmission lines being 25 years old or older,[8] as of 2007.

As the grid is modernized, new intelligent technologies utilizing two-way communications and other digital capabilities, are being incorporated with Internet connectivity. The "Smart Grid" refers to this evolving electric power network.[9] While these advances may improve the efficiency and performance of the grid, they also increase its vulnerability to cyberattacks launched from the Internet. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyberattack has increased focus on the cybersecurity of the grid. Modernization of many industrial control systems (ICS), in particular, Supervisory Control and Data Acquisition (SCADA) systems used by electric utilities, have also resulted in connections to the Internet.[10] The increasing frequency of cyber intrusions on ICS is a concern to the electric power sector. Power production and flows on the grid are controlled remotely by a number of IC technologies. The National Security Agency reported that it has seen intrusions into IC

[3] "Power outages can impact electricity consumers primarily through property loss and business disruption. This can result in lost orders, and damage to perishable goods and inventories for businesses. Power outages can critically affect manufacturing operations mainly through downtime as workers are idled, and potentially damage equipment and production processes." CRS Report R42696, *Weather-Related Power Outages and Electric System Resiliency*, by Richard J. Campbell.

[4] See Congressional Distribution Memorandum, *Space Weather and EMP threats to the Grid*, 2015, by Richard Campbell.

[5] Ibid.

[6] Massachusetts Institute of Technology, Retrofitting of Coal-Fired Power Plants for CO2 Emissions Reductions, March 23, 2009, http://web.mit.edu/mitei/docs/reports/meeting-report.pdf.

[7] Thomas A. Prevost and David J. Woodcock, *Transformer Fleet Health and Risk Assessment*, Weidman Electrical Technology, IEEE PES Transformers Committee Tutorial, March 13, 2007, http://grouper.ieee.org/groups/transformers/info/S07/S07-TR_LifeExtension.pdf.

[8] K. Anderson, D. Furey, and K. Omar, *Frayed Wires: U.S. Transmission System Shows its Age*, Fitch Ratings, October 25, 2006.

[9] In recognition of the need to deploy new technologies, Congress indicated its support for grid modernization in the Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140). Specifically, Section 1301 of the act states: "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth ... which together characterize a Smart Grid."

[10] CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell. (Hereinafter, CIBS).

systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[11]

Although there has not been a publicly-reported cybersecurity event or physical attack resulting in a large scale power outage in the United States,[12] the potential for such attacks to cause a wide scale, long lasting outage cannot be dismissed. The first blackouts attributed to a cyberattack happened in the Ukraine in December 2015.[13] The power outages affected approximately 225,000 customers, and are said to have originated from remote cyber intrusions at three regional electric power distribution companies. The cyberattackers targeted industrial control and operating systems at multiple central and regional facilities. The cyberattack also targeted other critical infrastructure,[14] apparently in an attempt to impair recovery efforts.

A report[15] released by the National Research Council (NRC) in 2012 concluded that well-informed terrorists could black out a large region of the country for weeks or even months.

> An event of this magnitude and duration could lead to turmoil, widespread public fear and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold*.
>
> The largest power system disruptions experienced to date in the United States have caused high economic impacts. Considering that a systematically designed and executed terrorist attack could cause disruptions that were even more widespread and of longer duration, it is no stretch of the imagination to think that such attacks could entail costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product (GDP), which is currently about $12.5 trillion.[16]

The NRC report further commented on the potential effects of a combined cyber and physical attack on the grid.

> If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled.[17]

Similar conclusions were reached in a 2015 report from Cambridge University and Lloyds of London, which theorized that a targeted cyberattack could leave 15 states and 93 million people from New York City to Washington, D.C. without power. The scenario estimated the total impact to the U.S. economy at between $243 billion and $1 trillion, resulting from "direct damage to assets and infrastructure, decline in

---

[11] Peter Behr, *Cyberattackers have penetrated U.S. infrastructure systems -- NSA Chief*, Environment & Energy Daily, November 21, 2014, http://www.eenews.net/energywire/stories/1060009391.

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

[13] DHS - Industrial Control Systems Cyber Emergency Response team, *Cyber-Attack Against Ukrainian Critical Infrastructure*, Alert (IR-ALERT-H-16-056-01), February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[14] "In addition, three other organizations, some from other critical infrastructure sectors, were also intruded upon but did not experience operational impacts." Ibid.

[15] National Academy of Sciences, *Terrorism and the Electric Power Delivery System*, 2012, http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

[16] Ibid, page 1.

[17] Ibid, page 2.

sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain."[18]

The 2013 attack on the Metcalf substation in California further cast light on the physical vulnerabilities of the grid. After someone broke into a nearby underground vault to cut telephone cables, snipers opened fire on the substation, knocking out 17 large power transformers sending power to Silicon Valley. A blackout was averted by rerouting power around the substation, and local power plants had to produce more electricity. But it took the local utility 27 days to restore the substation. The Federal Energy Regulatory Commission's (FERC's) chairman at the time (Jon Wellinghoff) reportedly said that "if [the attack] were widely replicated across the country, it could take down the U.S. electric grid and black out much of the country."[19]

Recovery from a well-planned cyber and physical attack on the grid could be complicated by the cost and vulnerability of critical components. While a physical attack on transmission towers to bring down power lines could cause blackouts, the strategic destruction of a number of critical high-voltage transformers could cause long-lasting power outages. These transformers are very large, and difficult to move. A large scale attack may use up the limited inventory of spare units,[20] and it may take months or even years to build new units. The availability of other large components, such as high-voltage circuit breakers could also hamper recovery efforts.[21]

Industry and Government Coordination on Recovery Efforts

The electric utility industry generally prepares for power outages from weather-related events, and views the potential for a major cybersecurity attack or similar event as a low probability risk. As such, the industry seeks to balance grid security efforts and expenditures with the perceived risks. In the event of a large power outage, electric utilities often call upon other utilities via their mutual assistance agreements[22] (MAAs) to help restore services. MAAs can help to reduce the duration of weather-related outages by bringing in outside resources to aid the recovery effort.

If an event is severe enough to be a federally-declared disaster,[23] the Department of Homeland Security's (DHS's) Federal Emergency Management Agency (FEMA) is empowered to provide federal assistance.

---

[18] University of Cambridge Centre for Risk Studies and Lloyds of London, *Business Blackout*, The insurance implications of a cyber attack on the US Power Grid, 2015, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

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

[20] The electric power industry has several programs for participating companies to share spare transformer equipment. For example," [the Edison Electric Institute's Spare Transformer Equipment Program] requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a 'triggering event'—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state of emergency by the President...[and in] 2012, NERC initiated its Spare Equipment Database program intended to serve as a tool to 'facilitate timely communications between those needing long-lead time equipment damaged in a [high impact, low frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization.'" See CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

[21] NAS.

[22] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, May 2014, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.

[23] "[The] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 100-707, signed into law November 23, (continued...)

> FEMA's mission is to reduce the loss of life and property and protect communities nationwide from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA leads and supports the nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery and mitigation.[24]

FEMA can provide financial assistance to electric utilities to aid in disaster recovery efforts. In general, FEMA will determine a utility's eligibility, and "will cover at least 75 percent of the repair, restoration or replacement costs for infrastructure owned by eligible applicants."[25]

The electric power industry also works with the Departments of Energy and Homeland Security on a number of cyber and physical security initiatives.[26] The Electricity Sub-Sector Coordinating Council (ESCC) is the principal liaison between the federal government and the electric power sector. It represents the electricity sub-sector (as part of the Energy Critical Infrastructure sector)[27] under DHS's National Infrastructure Protection Plan (NIPP).[28] The ESCC draws its membership from all segments of the electric utility industry, and is led by three chief executive officers – one each from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association.[29] Among its activities, the ESCC coordinates industry and government efforts on grid security, guides infrastructure investments and R&D for critical infrastructure protection, seeks to improve threat information sharing and processes with public- and private-sector stakeholders, and coordinates cross sector activities with other critical infrastructure sectors.

The bulk electric power system has mandatory and enforceable standards for cybersecurity. The Energy Policy Act of 2005 (EPACT) (P.L. 109-58) gave the Federal Energy Regulatory Commission authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for critical infrastructure protection (CIP) which are updated considering the status of reliability and cybersecurity concerns for the grid. FERC recently added mandatory and enforceable physical security requirements to its critical infrastructure protection standards.[30]

The electric utility industry also conducts a biennial grid security and emergency response exercise (GridEx) in which electric power and other stakeholders respond to simulated cyber and physical attacks.

(...continued)

1988; amended the Disaster Relief Act of 1974, Public Law 93-288. It created the system in place today by which a presidential disaster declaration of an emergency triggers financial and physical assistance through the Federal Emergency Management Agency (FEMA). The Act gives FEMA the responsibility for coordinating government-wide relief efforts." See http://www.fema.gov/about-agency.

[24] Federal Emergency Management Agency, *FEMA*, FEMA B-653, July 2008, http://www.fema.gov/pdf/about/brochure.pdf.

[25] Edison Electric Institute, *Federal Disaster Assistance and Utilities*, 2014, http://www.eei.org/issuesandpolicy/RES/14Tab5.pdf.

[26] See CIBS, page 16.

[27] The Energy Critical Infrastructure sector includes the electricity, petroleum, and natural gas subsectors. Department of Homeland Security, *Critical Infrastructure Sectors*, 2015, https://www.dhs.gov/critical-infrastructure-sectors.

[28] Department of Homeland Security, *National Infrastructure Protection Plan*, October 27, 2015, https://www.dhs.gov/national-infrastructure-protection-plan.

[29] Edison Electric Institute, *Electric Subsector Coordinating Council*, March 2015, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/ESCC%20Brochure.pdf.

[30] However, these rules largely do not apply to distribution system utilities which are subject to mostly state regulation. FERC Order No. 773 establishes a "bright-line" threshold essentially considering all transmission facilities and related facilities operating at 100 kilovolts or above to be part of the bulk electric power system. As such, these facilities are subject to the applicable NERC reliability standards.

The most recent exercise, GridEx III took place on November 18-19, 2015, and involved 364 organizations from across North America.[31]

In the event of a wide-scale power outage caused by a major attack or a disaster, electric utility efforts to restore power would likely have to be augmented by state and federal resources. Given the potential for damage to the nation's economy from a major attack on the grid, some might suggest a greater focus on recovery is needed and should become as much a part of a grid security strategy as the efforts to secure the system. NERC has essentially agreed, saying in its GridEx III report that severe emergency situations may require greater coordination with states and the federal government to identify physical risks to electricity facilities, and to identify cyber risks in addressing malware on control systems before recovery efforts could begin.[32]

Congress included provisions to give the U.S. Department of Energy (DOE) new authority to order electric utilities and NERC to implement emergency security actions in the "Fixing America's Surface Transportation Act" (FAST; P.L. 114-94).[33] DOE is designated as the lead sector specific agency for cybersecurity for the Energy sector.[34] Section 61004 of FAST also requires DOE (in consultation with FERC, NERC, and electrical infrastructure operators) to develop a plan for storing spare large power transformers and emergency mobile substations which can be quickly deployed to replace damaged large power transformers and substations which serve grid-critical functions.[35]

Areas for Further Congressional Consideration

In any discussion of extended power outages, two prominent themes emerge—preparation and recovery. If utilities are aware of an impending storm or weather-related event which may cause outages, they are expected to make preparations for restoration of services in as timely a manner as possible. Recovery from any such event will depend on the severity of the storm and the resulting damage. Recovery can be hastened, and the amount of damage to electric power infrastructure can be minimized, if good maintenance, restoration, organization, and communications strategies are followed on an ongoing basis.

However, a coordinated, major cyber and physical attack on the electric grid would severely test the ability of the nation to recover, especially as plans for such a recovery are currently in progress. The electric utility industry generally bases its response to the potential for such events based on the perceived

[31] "The electricity industry participants included chief executives from investor and publicly owned utilities, cooperatives, and independent system operators from the U.S. and Canada. The U.S. federal and state governments were represented by senior officials from various departments and agencies. In addition, approximately 70 individuals associated with the participants attended the tabletop as observers to provide feedback." Observers included the White House; National Security Council; Department of Energy; Department of Homeland Security, including Federal Emergency Management Agency; Department of Defense, including U.S. Cyber Command, U.S. Northern Command, North American Aerospace Defense Command; National Security Agency; Federal Bureau of Investigation; and the National Guard. North American Electric Reliability Corporation, *Grid Security Exercise - GridEx III*, March 2016, http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf. (Hereinafter, GridExIII).

[32] Ibid. Page 15.

[33] Section 61003 of FAST creates a new section 215A of the Federal Power Act, that following a written determination by the President, authorizes DOE to order utilities, the North American Electric Reliability Corporation (NERC), and Regional Entities to implement emergency security measures for up to 15 days at a time.

[34] The energy sector is one of 16 critical infrastructure sectors identified in Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience. Sector specific agencies are designated with specialized expertise in those critical infrastructure sectors that are tasked with various roles and responsibilities for their respective sectors, as specified in PPD-21 (i.e., development of sector-specific plans, coordination with the Department of Homeland Security, and incident management responsibilities).

[35] Paul Parfomak, *Electric Grid Physical Security: Recent Legislation*, CRS Insight IN10425, 2016.

risks. The industry relies on the federal government to share relevant, real-time intelligence on risks from terrorism or cybersecurity threats, communicating the quality of threat information in a timely manner so it can respond appropriately. Improvements in threat/risk assessment would aid this process.

A focus on recovery would have to consider the mutual dependence and implications to other critical infrastructure (especially communications systems)[36] of an electric grid failure, and how quickly such impacts could proliferate if not planned for in advance. Congress may consider how the grid of the future will address cyber and physical security concerns, as more distributed generation is incorporated. The U.S. electric grid is evolving. Incorporating elements to increase system resiliency as it develops will aid in reducing the vulnerability of the system.

NERC itself concluded in its report on GridEx III that, after a major grid disruption, restarting generation and energizing transmission and distribution systems would be a first priority. Restoring service to communications systems, oil and gas, water supply/treatment and hospital customers would be a secondary priority. Electric power systems may be operating at reduced levels of service and reliability for an extended period at such a time. Congress may consider how planning for subsequent restoration of services would proceed to ensure that all civilian communities are kept informed, and treated as equitably as possible in disaster recovery efforts.

[36] "[PPD-21] identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." The White House, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, Presidential Policy Directive / PPD-21, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.