Electric Grid Cybersecurity

(name redacted)
Specialist in Energy Policy

September 4, 2018

Congressional Research Service
7-....
www.crs.gov
R45312

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Electricity generation is vital to the commerce and daily functioning of the United States. The U.S. electric power grid comprises all of the power plants generating electricity, together with the transmission and distribution lines and systems that bring power to end-use customers. The U.S. electric grid has operated historically with a high level of reliability; however, the various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events.

The bulk power system faces new and evolving cybersecurity threats. Cyber threats can come from direct attacks aimed at electric grid or other critical infrastructure that could impact the operations or security of the grid. Arguably, the greatest cyber threats to the grid have been intrusions focused on manipulating industrial control system (ICS) networks. Cyber intrusions on the electric grid have resulted in malware on ICS networks with the capability of causing damage or taking over certain aspects of system control or functionality. Recent concerns have extended to Internet of Things (IoT) devices connected to networks. IoT devices have been increasingly targeted by botnet malware (whereby the hacker takes over the operation of a large number of infected devices) to launch denial-of-service or other cyber attacks. If such IoT cyber attacks were able to access electric utility ICS networks, they could potentially impair these systems or cause electric power networks to operate based on manipulated conditions or false information.

Congress gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the bulk power system under the Energy Policy Act of 2005 (P.L. 109-58; EPACT05). FERC can approve or remand back reliability standards proposed by the Electric Reliability Organization (ERO), which bulk-power system owners and operators must follow to help ensure the reliable operation of the grid. The North American Electric Reliability Corporation serves currently as the ERO, and proposes mandatory and enforceable reliability standards for Critical Infrastructure Protection (which include physical and cybersecurity).

There have been increasing reports about foreign hackers targeting the U.S. electric power system and other critical infrastructure. While these intrusions have not been reported as having resulted in significant disruptions, concerns have increased over the potential of the intrusions for potentially damaging cyber attacks. In 2017, the President issued Executive Order (EO) 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" because the risks of cyber threats to critical infrastructure are perceived as a national security imperative. EO 13800 called for an assessment of a prolonged electric power outage resulting from a cyber attack, and an evaluation of the "readiness and gaps in the United States' ability to manage and mitigate consequences of a cyber incident against the electricity subsector." The cyber supply chain and public-private cybersecurity information sharing were listed among a number of major cybersecurity concerns.

Electricity is a subsector of the energy critical infrastructure (CI) sector. Given that the grid relies on several of the other CI sectors (for example, water and fuel transportation), the question of whether these other sectors should also have similar mandatory standards focused on support of the electric power sector may be an issue for Congress to consider.

The electric power system in the United States is evolving, but not consistently across sectors and regions of the country. While some may say such inconsistencies may add a level of complexity that may make a nationwide cyber event more unlikely, the consistent development of a modern electric power system would likely add to the prospects of U.S. economic health and competitiveness. Policy options designed to ensure that the developing electric power system is as secure as possible, will likely be a major consideration for Congress.

Contents

Tables

Appendixes

Contacts

Introduction

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

While natural and operational failures can be mitigated somewhat by planning and prudent investments, cybersecurity is a growing concern for both electric utilities and other critical infrastructure entities. Adoption of digital technologies has improved the efficiency and speed of operations and processes, and allowed for an almost instantaneous exchange of information between connected devices. Often, these digital devices are also connected to the internet to increase the ability to share information with a multitude of users and devices. While the benefits of internet-connected digital technologies are many, so too are the risks of a cybersecurity breach from exposure to a globally internet-connected environment.

The electric grid relies on a number of electronic devices, switches, and circuit breakers to regulate and report on the flow of electricity at different parts of the system. Together, these pieces of mechanical and automated equipment constitute the grid's industrial control system (ICS) network, managing power plant controls, transformer yard and power bus functions, transmission, and distribution substations. The grid's ICS networks essentially operate in a "control loop" in which sensors continually check key components, with variable responses against control variables to ensure that the system is functioning as designed. ICS networks control industrial processes in a number of energy and manufacturing operations. One particular type of ICS network common in the electric power industry is a supervisory control and data acquisition (SCADA) system which gathers information from remote stations across a utility system to control geographically dispersed assets.

In 2015, a cyber attack on distribution utility substations in Ukraine shut off power to over 225,000 utility customers for several hours, and was the first time that a cyber attack was publicly acknowledged to have caused a grid power outage.[1] A second cyber attack in Ukraine in 2016 was reported on an electricity control center in the city of Kiev, shutting down substations which controlled 200 megawatts of capacity. The potential for a similar attack on the U.S. grid was seen as a possibility.[2]

Some recent reports about foreign hackers targeting the U.S. electric power system and other critical infrastructure are summarized below. While these intrusions have not been reported as having resulted in significant disruptions, concerns have increased over the potential for these intrusions to result in damaging cyber attacks in the future.[3] The intrusions, which have been

[1] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 18, 2016, https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[2] John Condliffe, *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*, MIT Technology Review, December 22, 2016, https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

[3] Robert Walton, *U.S. Sounds Alarm over Increased Cyber Threat to Energy, Other Sectors*, UtilityDive, October 24, 2017, https://www.utilitydive.com/news/us-sounds-alarm-over-increased-cyber-threat-to-energy-other-sectors/507987/.

directed at the ICS networks of energy, manufacturing, communications and nuclear entities, include the following:

- Cyber intrusions on the SCADA systems of the Bowman Dam in Rye, New York resulted in federal indictments against a group of hackers linked to Iran's Islamic Revolutionary Guard Corps.[4]
- Cyber intrusions in October 2017 were reported to have targeted electric company ICS networks in a reconnaissance and information gathering campaign attributed to North Korea.[5]
- In March 2018, the United States Computer Emergency Readiness Team (US-CERT) issued an alert concerning cyber intrusions at critical energy and manufacturing infrastructure companies. The Department of Homeland Security and the Federal Bureau of Investigation concluded that Russian government hackers conducted a multi-stage intrusion campaign to access files on ICS networks. The malware conducted network reconnaissance, collecting information on ICS and SCADA systems before being found.[6]

Further attacks on U.S. critical energy infrastructure are expected, as nation states view disruption of the U.S. economy as a potential target.[7]

This report discusses the current state of electric grid cybersecurity, and the interconnected dependency of critical infrastructure with regard to electric sector reliability. Current efforts to ensure the reliability of the grid are highlighted, and potential grid vulnerabilities are explored with a focus on the electric power sector's mutual dependency on other critical infrastructure. Technologies and actions to address perceived future threats are described, and possible risks to approaches moored in technology-based cybersecurity defense systems. Finally, since the possibility does exist for a major cyber and/or physical security attack to result in significant damage or impairment, the potential need to build resilience into the grid to enable a quicker recovery is discussed.

Electric Grid Reliability

Congress gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the bulk-power system under the Energy Policy Act of 2005 (P.L. 109-58; EPACT05). Reliability standards were added as section 215 of the Federal Power Act (FPA) in an effort to help ensure the reliable operation of the bulk power system so that "instability,

[4] U.S. Department of Justice, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities," press release, March 24, 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

[5] Chris Bing, *Hackers Linked to North Korea Targeted U.S. ICS Companies, Breached Energy Firm*, Cyberscoop, October 10, 2017, https://www.cyberscoop.com/north-korea-ics-hacking-dhs-ics-cert/.

[6] U.S. Computer Emergency Readiness Team, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Alert (TA18-074A), March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

[7] Director of National Intelligence Daniel Coats warned that the U.S. should brace for "localized and temporary disruptions of critical infrastructure," observing that the proliferation of digital devices and newly "emboldened and better equipped" adversaries may resort to damaging cyber operations in geopolitical crises that fall short of war. The assessment singled out Russia, China, Iran, and North Korea as posing the biggest cyberthreats to the United States. Daniel R. Coats, *Worldwide Threat Assessment*, Statement for the Record, February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf.

uncontrolled separation, or cascading failures" will not occur as a result of a sudden disturbance.[8] Section 215 of the FPA also defines FERC's jurisdiction in terms of "users, owners and operators" of the bulk power system.[9]

FERC can approve or remand back reliability standards proposed by the Electric Reliability Organization (ERO), which bulk-power system owners and operators must follow to help ensure the reliable operation of the grid. 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. Reliability standards address programs ranging from vegetation clearances in electric transmission line rights-of-way to policies and procedures for critical infrastructure protection focused on the cyber- and physical security of power plants and supporting facilities. The standards are both mandatory and enforceable in that violators of reliability rules may be subject to a civil fine of up to $1 million per violation for each day that it continues. While the bulk electric power system has mandatory and enforceable standards for both cyber and physical security for critical infrastructure protection, these are developed on a consensus basis before being submitted to FERC, which determines whether to accept or remand the standard back to NERC for revision.

Under the Federal Power Act, FERC's authority is largely limited to wholesale power sales and the transmission of electricity in interstate commerce, while states have authority over retail sales by electric distribution systems. FERC acknowledges that EPACT05 excluded local distribution systems from its reliability mandate under Section 215 of the Federal Power Act, as not being part of the bulk power system. That criterion excluded facilities in Alaska and Hawaii, and virtually the entire grid in cities with large distribution systems like New York City. In 2012, FERC approved NERC's criteria for the definition of the bulk electric system.[10] These criteria and definitions apply to all NERC regions and are a bright-line threshold including all Transmission Elements operated at 100 kilovolts (kV) or higher, and real power[11] and reactive power[12] resources connected at 100 kV or higher.[13]

---

[8] Reliability, according to the U.S. Department of Energy, is the ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components. See https://www.energy.gov/sites/prod/files/2017/01/f34/Chapter%20IV%20Ensuring%20Electricity%20System%20Reliability%2C%20Security%2C%20and%20Resilience.pdf.

[9] 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.

[10] See 139 FERC 61,247.

[11] Real (or active) power is the "component of electric power that performs work, typically measured in kilowatts (kW) or megawatts (MW)." See http://www.eia.gov/tools/glossary/index.cfm.

[12] Reactive power is the "portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is a derived value equal to the vector difference between the apparent power and the real power. It is usually expressed as kilovolt-amperes reactive (KVAR) or megavoltampere reactive (MVAR)." See http://www.eia.gov/tools/glossary/index.cfm.

[13] The discussion of bulk electric system "Transmission Elements" begins with a general definition. These are "[a]ny electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components." North American Electric Reliability Corporation, *Bulk Electric System Definition Reference Document*, Version 2, April 2014, p. 5, https://www.nerc.com/pa/RAPA/BES%20DL/bes_phase2_reference_document_20140325_final_clean.pdf.

Some Recent Developments in Grid Cyber Policy

The increase in the number of cyber attacks aimed at U.S. critical energy infrastructure has led to heightened attention from the federal government.[14] While a cyber attack on the U.S. grid similar to the cyber attacks in Ukraine was not expected to result in the same type of consequences (given the older electricity systems in place in Ukraine), the potential for financial market and economic disruption may be a legitimate concern.

Presidential Executive Order 13800

In 2017, President Trump issued Executive Order (E.O.) 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" because the risks of cyber threats to critical infrastructure are perceived as a national security imperative.[15] E.O. 13800 called for an assessment of a prolonged electric power outage resulting from a cyber attack, and an evaluation of the "readiness and gaps in the United States' ability to manage and mitigate consequences of a cyber incident against the electric subsector." The cyber supply chain and public-private cybersecurity information sharing were listed among a number of major cybersecurity potential vulnerabilities.

Department of Energy Establishes New Cybersecurity Office

The Fixing America's Surface Transportation Act (FAST Act; P.L. 114-94) gives the Department of Energy (DOE) new authority to order electric utilities and NERC to implement emergency security actions.[16] DOE is designated as the lead sector specific agency for the Energy sector, with responsibilities for both physical and cyber security.[17]

DOE has established a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "bolster DOE's efforts in cybersecurity and energy security."[18] CESER is to focus on more coordinated preparedness and response to natural and man-made threats to energy infrastructure security.

Following E.O. 13800, DOE established a five-year strategy for reducing cyber risks in the U.S. energy sector which is intended to serve as the basis for CESER activities. Under the strategy,

[14] Rebecca Kern, *Utilities Prepare for Increased Cyberattacks on the Electric Grid*, Bloomberg Environment and Enviroment Report, August 7, 2018, https://www.bna.com/utilities-prepare-increased-n73014481471/.

[15] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Federal Register* 22391.

[16] 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.

[17] The energy sector is one of 16 critical infrastructure sectors identified in Presidential Policy Directive-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).

[18] DOE, *Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response*, February 14, 2018, https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency.

CESER will carry out the DOE's Office of Electricity's cybersecurity responsibilities in supporting the physical and cybersecurity needs of energy owners and operators.[19]

Three main goals have been established under the strategy:

- **Strengthen Energy Sector Cybersecurity Preparedness—**focuses efforts through Cybersecurity Risk Information Sharing Program (CRISP) activities;[20]
- **Coordinate Cyber Incident Response and Recovery—**establishes a coordinated national cyber incident response capability for the energy sector to augment cyber mutual assistance. DOE's national laboratories are to develop an integrated set of specialized cyber resources and capabilities that can be deployed to help energy companies identify and respond to a cyber attack; and
- **Accelerate Game-Changing Research, Development, and Demonstration (RD&D) of Resilient Energy Delivery Systems**—keys on research, development and demonstration of new cybersecurity tools and technologies for automated defense of future energy delivery systems.

Revised Voluntary Cybersecurity Framework

While the bulk electric system has mandatory and enforceable rules for cyber and physical security, other energy sectors do not. In April 2018, the National Institute of Standards and Technology (NIST) released its revised voluntary Cybersecurity Framework. The framework is a risk-based approach to cybersecurity that is generally applicable to industries using a range of IT technologies, including Internet of Things (IoT) devices. The Framework focuses on "using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."[21]

Cyber and Physical Security of the Grid

The energy sector is one of 16 infrastructure sectors designated as critical infrastructure by Presidential Policy Directive-21 (PPD-21).[22] The stated goal of PPD-21 is to advance "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." The energy sector under the policy directive includes electricity, oil, and natural gas. The reliance of virtually all industries on electric power is recognized by the U.S. Department of Homeland Security (DHS), which has the primary responsibility for implementing PPD-21.[23]

---

[19] DOE, *Multiyear Plan for Energy Sector Cybersecurity*, March 2018, https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

[20] CRISP provides energy sector owners and operators with a capability to voluntarily share cyber threat data in near-real-time, analyze this data using U.S. intelligence, and receive machine-to-machine threat alerts and mitigation measures.

[21] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[22] See Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[23] "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." DHS, *Critical Infrastructure Sectors*, 2018, https://www.dhs.gov/critical-infrastructure-sectors.

A report released by the National Research Council (NRC) in 2012 recognized the vulnerability of the electric power delivery system to either cyber and/or physical attacks. The NRC report concluded that well-informed terrorists could black out a large region of the country for weeks or even months.[24]

> 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.[25]

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.[26]

Similar conclusions were reached in a 2015 report from the University of Cambridge and Lloyds of London, which stated that a targeted cyber attack 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 sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain."[27]

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 were called upon to produce more electricity. It took the local utility 27 days to restore the substation. The Federal Energy Regulatory Commission's (FERC's) chairman at the time 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."[28] Largely as a result of the grid

[24] 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.

[25] Ibid, p. 1.

[26] Ibid, p. 2.

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

[28] 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.

vulnerabilities highlighted by this incident, FERC directed NERC to develop a physical security standard (which culminated in CIP-014).[29]

Since the 2015 cyber attack in Ukraine, some have expressed increased concerns over the cybersecurity of interconnected U.S. electric power systems. The 2015 Ukraine cyber attack and blackouts demonstrated that an electric grid could be infiltrated, controlled, and rendered inoperable through Internet-connected systems by an outside, unauthorized entity.

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 potentially cause long-lasting power outages. These transformers are large, and difficult to move. A large-scale attack may use up the limited inventory of spare units,[30] and it may take months or years to build new units (due mainly to the size and often unique specifications of high-voltage transformers). The availability of other large components, such as high-voltage circuit breakers could also hamper recovery efforts.[31] The security of the supply chain for grid devices and components is discussed later in this report.

Critical Infrastructure Protection Standards

NERC has a set of mandatory and enforceable standards for electricity reliability to protect the critical infrastructure of the bulk electric system (BES). NERC periodically updates the applicable version of the critical infrastructure protection cybersecurity (CIP) standards, which leads to a new compliance phase for the owners and operators of the BES.

The current iteration of NERC's standards is CIP Version 6, which contains several updates to Version 5 requirements, largely reflecting increased security for BES assets and training for utility personnel.[32] **Table 1** in the Appendix of this report lists the current standards in effect and several standards pending regulatory approval from FERC.

NERC's CIP Version 5 moved utility companies towards active planning for system security needs rather than solely compliance with the standards. It established criteria mandating that BES owner/operators focus on improving the security of critical assets.[33] BES assets, were categorized as low or high impact, and were to be protected according to the level of requirements for that impact category. CIP Version 5 also required encryption of grid command and control signals; "role based" instead of "risk-based" classifications requiring multiple levels of compliance considering facilities with low, medium or high-level potential impacts on the BES; monitoring

[29] See the Appendix, **Table A-1**, "NERC Critical Infrastructure Protection Standards."

[30] 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 (name redacted) .

[31] 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.

[32] NERC, *CIP Standards*, 2017, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[33] NERC CIP Version 5 went into effect in July 2015.

and control of remote access Internet connections (with inclusion of serial connections); multiple-factor authentication (rather than a one-step password for access), incident response recovery plans; physical security of BES cyber assets to prevent unauthorized physical entry and access; and cataloging of all software and all security patches on BES devices.

Grid Security Exercises

Every two years, the North American Electric Reliability Corporation (NERC) organizes a two-day grid security exercise (called GridEx) to test the electricity sector's ability to respond to grid security emergencies caused by cyber and physical attacks. The goals of GridEx include the determination of ways to best secure the grid and improve future response by improving communications among companies, state and federal agencies, identifying lessons learned, and engaging senior company leadership. The 2017 GridEx drill was the fourth iteration of the exercise, and had over 6,500 participants from the United States, Canada, and Mexico.[34]

NERC released its public report of the results of GridEx IV drill, listing lessons learned and recommendations to enhance grid security.

> Recommendations in the report included increasing coordination between utilities and federal, state and local governments, enhancing information sharing capabilities for the Electricity Subsector Coordinating Council [ESCC] and Energy Government Coordinating Council, developing ESCC processes for emergency orders and continuing to promote the Cyber Mutual Assistance Program.[35]

A focus on recovery from a potential large-scale physical or cyber attack appears to be an increasing part of the exercises. The Cyber Mutual Assistance (CMA) program is intended to provide a pool of utility cybersecurity experts who can share their expertise with other utilities in the event of a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency. NERC recommended that more utilities should participate in the CMA program. Additionally, NERC proposed that the ESCC and the Electricity Information Sharing and Analysis Center (E-ISAC) also increase their participation in the CMA program to encourage the efficient sharing of relevant information.[36]

Cyber Threats to the Grid

The bulk power system faces new and evolving cybersecurity threats on a daily basis. Cyber risks can come from direct attacks aimed at the electric grid or other critical infrastructure which could impact the operations or security of the grid. Arguably, the greatest cyber threats to the grid have been attacks focused on manipulating industrial control systems which are increasingly connected to the Internet to manage the production and regional flows of electricity.[37]

---

[34] DOE, *GridEx IV: Government and Industry Exercise Together to Improve the Response to Grid Security Emergencies*, November 21, 2017, https://www.energy.gov/articles/gridex-iv-government-and-industry-exercise-together-improve-response-grid-security.

[35] NERC, *Grid Security Exercise GridEx IV—Lessons Learned*, public report, March 2018, https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf.

[36] Ibid, p. 16.

[37] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, August 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

Industrial Control System Vulnerabilities

ICS-CERT issues an annual report on ICS network vulnerabilities based on reports of cyber intrusions.[38] Private companies also issue similar reports drawn from ICS-CERT alerts and their own sources. As one example, in 2017, the security firm Dragos (which specializes in industrial-control systems) looked at 163 new security vulnerabilities it found in industrial control devices. It stated that the devices with the vulnerabilities it found were typically "insecure-by-design," since they were located deep within ICS networks.[39] It found that 61% of these vulnerabilities would likely cause a "severe operational impact," if exploited in a cyber attack. Dragos said that about 15% of these vulnerabilities could be "leveraged to gain initial access into a control network," meaning that a hacker would likely have to first have gained access to a network in order to exploit the vulnerability.[40]

Some Recent Malware Threats

Cyber intrusions on the electric grid have resulted in the deposits of malware on grid ICS networks with the capability of causing damage or taking over certain aspects of system control or functionality.

Triton

The Mandiant consulting company reported that it responded to a cyber intrusion at a critical infrastructure organization where malware was deployed to manipulate an industrial safety system.[41]

> The targeted systems provided emergency shutdown capability for industrial processes. We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shut down operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack.[42]

Since the reported attack was focused on hacking SIS controllers, FireEye (a private security firm) stated its opinion that the intrusion was intended to be a high-impact attack with physical consequences, and that this was not the type of attack expected from a cyber-crime group aimed at financial extortion.[43]

The Triconex equipment referred to by FireEye is manufactured by Schneider Electric, which reported that cyber attacks on its Triconex equipment were targeted.

---

[38] ICS-CERT, *Year in Review 2016*, 2017, https://ics-cert.us-cert.gov/Year-Review-2016.

[39] DRAGOS, *Industrial Control Vulnerabilities: 2017 in Review*, 2018, https://dragos.com/media/2017-Review-Industrial-Control-Vulnerabilities.pdf.

[40] Ibid.

[41] FireEye, *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*, December 14, 2017, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[42] Ibid.

[43] "A SIS is an autonomous control system that independently monitors the status of the process under control. If the process exceeds the parameters that define a hazardous state, the SIS attempts to bring the process back into a safe state or automatically performs a safe shutdown of the process." Ibid.

> The attack on the Schneider customer in part exploited a previously unknown, or zero day, vulnerability in Schneider's Triconex Tricon safety system firmware. And the hackers deployed a *remote access trojan* [i.e., a malware program that includes a back door for administrative control over the target computer] in the second stage of their exploitation, a first for malware that targets industrial control systems.[44]

Crash Override/Industroyer

The malware deployed to attack a transmission system control center in the 2016 cyber attack in Ukraine was named "Industroyer" or "Crash Override" by cybersecurity companies ESET and Dragos.[45] The malware accesses the same protocols used by electric grid systems to communicate with each other.

> The platform fundamentally abuses the functionality of a targeted ICS system's legitimate control system to achieve its intended effect. While the known capabilities do not appear to be U.S.-focused, it is important to recognize that the general [tactics, techniques, and procedures] used in CrashOverride could be leveraged with modified technical implementations to affect U.S.-based critical infrastructure. With further modification, CrashOverride or similar malware could have implications beyond electric power so all critical infrastructure organizations should be evaluating their systems to susceptibilities.[46]

This was reported to be the second known malware specifically designed to disrupt physical systems. The first malware recognized as targeting SCADA systems was the STUXNET computer worm, which was reported in 2010 to have destroyed centrifuges for uranium enrichment in Iran. The virus subsequently proliferated, with STUXNET subsequently being reported in 2012 to have spread to other company networks. However, no damage was reported to these other networks, due to the malware being designed to attack specific equipment.[47]

BlackEnergy 2 and 3

In 2015, cyber attackers are reported to have used the BlackEnergy 2 malware to cause the grid failure in Ukraine.[48] BlackEnergy 2 and 3 are versions of the BlackEnergy malware.

> The malware uses a modular functionality on [small office/home office] routers to collect intelligence, exploit [local area network] devices, and block actor-configurable network traffic. The malware can render a device inoperable, and has destructive functionality across routers, network-attached storage devices, and central processing unit (CPU) architectures running embedded Linux.[49]

---

[44] Lily Hay Newman, "Menacing Malware Shows the Dangers of Industrial System Sabotage," *WIRED*, January 18, 2018, https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/.

[45] Andy Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," *WIRED*, June 12, 2017, https://www.wired.com/story/crash-override-malware/.

[46] U.S. Computer Emergency Readiness Team, *CrashOverride Malware*, Alert (TA17-163A), June 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-163A. https://www.us-cert.gov/ncas/alerts/TA17-163A.

[47] David Kushner, *The Real Story of Stuxnet*, IEEE, February 26, p. 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[48] "Recent open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system." ICS-CERT, *Ongoing Sophisticated Malware Campaign Compromising ICS*, Alert (ICS-ALERT-14-281-01E), November 10, 2014, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[49] US-CERT, *Cyber Actors Target Home and Office Routers and Networked Devices Worldwide*, Alert (TA18-145A),

BlackEnergy is a special potential vulnerability for critical infrastructure companies because the software is being used in an Advanced Persistent Threat (APT) form ostensibly to gather information.[50] It can be used to monitor and interact with industrial control systems such as heating, ventilation, and air conditioning systems.[51]

Potential Cyber Threat to Grid from the Internet of Things

Cyber threats to the grid can also emerge from attacks directed via Internet of Things (IoT) devices connected to networks.[52] IoT devices have been increasingly targeted by botnet malware (whereby the hacker takes over the operation of a large number of infected devices) to launch denial-of-service or other cyber attacks.[53] If such IoT cyber attacks were able to access electric utility operational or industrial control systems, they could potentially impair these systems or cause electric power networks to operate based on manipulated conditions or false information.[54] For example, a potential IoT-based attack on residential or commercial thermostats could result in false power demand readings, causing a utility to ramp up power production unnecessarily. However, some IoT threats can possibly be mitigated by deliberate IoT device design, set-up, and maintenance practices.[55]

Supply Chain Risks

The electric utility industry increasingly depends on Operational Technology (OT) and Information Technology (IT) systems for the safe and efficient production and delivery of electricity. OT and IT systems rely on hardware devices and software systems, procured from a variety of manufacturers and vendors, often from international sources. The security of the

May 25, 2018, https://www.us-cert.gov/ncas/alerts/TA18-145A.

[50] "An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry." See https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

[51] Aravind Swaminathan and Stephen Hsieh, *Blackenergy Malware Highlights Special Confidentiality Considerations in Critical Infrastructure Breach Investigations*, DLA Piper, November 17, 2015, https://www.technologyslegaledge.com/2014/11/blackenergy-malware-highlights-special-confidentiality-considerations-in-critical-infrastructure-breach-investigations/.

[52] IoT devices "include smart TVs, smart speakers, toys, wearables and smart appliances. Smart meters, commercial security systems and smart city technologies—such as those used to monitor traffic and weather conditions—are examples of industrial and enterprise IoT devices. Other technologies, including smart air conditioning, smart thermostats, smart lighting and smart security, span home, enterprise and industrial uses." TechTarget, *Iot Devices (Internet of Things Devices)*, 2018, https://internetofthingsagenda.techtarget.com/definition/IoT-device.

[53] A denial-of-service attack is an attempt to make a machine or network resource unavailable to those attempting to reach it. Quora, *What are Different Types of Cyberattacks?*, 2018, https://www.quora.com/What-are-different-types-of-cyber-attacks.

[54] "The Mirai botnet took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites." Jack Wallen, *Five Nightmarish Attacks that Show the Risks of IoT Security*, June 1, 2017, https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/.

[55] "From looking at these attacks, it should be clear that the onus for preventing takedown by IoT is on both the user and the device developer. Going forward, every IoT device should ship with an updated kernel/firmware and include the ability to regularly update as new vulnerabilities are found. At the same time, anyone who deploys an IoT device needs to take the time to change the default user/password combination (if available) and constantly be on the lookout for suspect network activity. Finally, developers should seriously consider making default password change a requirement upon initial deployment of the device." Ibid.

design, manufacture, and patch management practices of these devices and systems is a potential vulnerability due to their global nature, and the general lack of consistent oversight of standards and practices to prevent impaired or compromised functionality.[56]

> Managing cyber supply chain risks require ensuring the integrity, security, quality and resilience of the supply chain and its products and services. Cyber supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cyber supply chain.[57]

The components of smart grid devices present another potential vulnerability.[58] Most of the smart meter, sensor, and other equipment makers are international companies who obtain their components from multinational sources. Taiwan, Singapore, China, and South Korea are among the largest overseas manufacturers of semiconductors and microprocessors for smart devices. The reliable operation of semiconductor and microprocessor-based devices is based on the low-level firmware controlling the device's basic functions.[59] Firmware, in the form of fixed machine-language code, is found in almost all the electronic devices making up smarter grid products such as programmable controllers and programmable logic arrays. If access were gained to such devices (especially during the manufacturing process), a section of code could be covertly inserted in the device and activated in such a way as to impair its functioning in a reliable manner. Since testing all such devices is likely impractical, some might suggest random or statistically based testing of the firmware in smarter grid devices. But the impairment would not need to be placed in all such devices coming off an assembly line. If a large enough sample was impaired, the effect might be enough to cast doubt on the reliability of a whole class of such devices.

Older, legacy systems may also be affected by potential supply chain vulnerabilities. Legacy systems are a challenging vulnerability because upgrades and repairs of equipment may not include the installation of up-to-date, security-focused patches.

In 2016, FERC issued Order No. 829 directing NERC to develop a Critical Infrastructure Protection reliability standard that would require affected entities to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.[60] According to FERC, the new or modified reliability standard should address:

- Software integrity and authenticity;
- Vendor remote access;
- Information system planning; and,
- Vendor risk management and procurement controls.

FERC states that there is no requirement for any specific controls, nor does FERC require any "one-size-fits-all" requirement. According to FERC, the new or modified reliability standard

[56] For further information, see CRS In Focus IF10920, *Cyber Supply Chain Risk Management: An Introduction*, by (name redacted)

[57] National Institute of Standards and Technology, *Cyber Supply Chain Risk Management*, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

[58] CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by (name redacted) .

[59] Firmware is software that is embedded in a hardware device that allows reading and executing the software, but does not allow modification, e.g., writing or deleting data by an end user. See http://www.its.bldrdoc.gov/fs-1037/dir-015/_2236.htm.

[60] 156 FERC ¶61,050.

should instead require responsible entities to develop a plan to meet the four objectives while providing flexibility to responsible entities as to how to meet those objectives.[61]

In September 2017, NERC submitted a petition for approval of the new Reliability Standard CIP-013-1, addressing supply chain risk management, and proposed revisions to two existing reliability standards (i.e., CIP-005-6 and CIP-010-3).[62] The proposed set of new and revised standards would address cybersecurity risks in the supply chain by:

- Establishing and implementing organizationally defined processes that integrate a cybersecurity risk management framework (proposed CIP-013-1);
- Implementing methods to identify active vendor remote access sessions and disable active vendor remote access when necessary (proposed modification to CIP-005-5); and,
- Verifying the identity of software publishers, and the integrity of all software and patches intended for use on BES Cyber Systems (proposed modification to CIP-010-2).

Other Grid Cybersecurity Issues

There are gaps in cybersecurity for electric power and energy systems. Some gaps are related to regulatory jurisdiction, while other gaps may relate to cost and relative complexity to address the issue. But considering the potential impact of a major grid cybersecurity event, the gaps may require further attention.

Operation Technology (OT) Systems

OT systems are often used by electric utilities to monitor and control power production processes. While these technologies have been considered air-gapped (i.e., separate from IT systems), modernization of ICS networks has led to OT and IT systems becoming increasingly interconnected.[63] And while a lot of attention has been focused on IT system cybersecurity, this is not always the case for OT networks.

> OT systems are often directly connected to the Internet, in some cases so that third-party vendors can remotely connect to the system to perform diagnostics and maintenance. In many of these instances, the OT systems are not protected by a firewall and are outdated, so they lack modern security features that would typically be used to protect an internet-facing connection (e.g. multi-factor authentication, strong passwords, logging and monitoring).[64]

[61] FERC, *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, July 21, 2016, https://ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

[62] NERC, *Reliability Standards for the Bulk Electric Systems of North America*, July 3, 2018, https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

[63] "OT also often includes control room applications, such as supervisory control and data acquisition (SCADA) systems that monitor the network, reaching out to devices as complex as substation gateways, or as simple as sensors." Jeff Meyers, *How the Convergence of IT and OT Enables Smart Grid Development*, Schneider Electric, 2013, http://www2.schneider-electric.com/documents/support/white-papers/electric-utilities/How-the-Convergence-of-IT-and-OT-Enables-Smart-Grid-Development.pdf.

[64] Price Waterhouse Coopers, *Cyber Savvy: Securing Operational Technology Assets*, December 2015, https://www.pwc.com.au/pdf/cyber-savvy-securing-operational-technology-assets.pdf.

Economic challenges, resource constraints, business requirements and the pace of technological change are factors which are reported as making it nearly impractical to completely segregate OT networks from IT networks.[65]

Human Factor in Cybersecurity

Many cybersecurity breaches are caused by individuals falling prey to phishing or similar attacks which are used to gain credentials to access utility systems.[66] The human factor is thus considered by many to be the weakest link in cybersecurity. This was the case in Ukraine, as hackers sent out malware-carrying emails. After links in the emails were opened by legitimate users, hackers acquired the credentials needed to access control and operations systems to cause blackouts at regional distribution utilities.[67] Development and deployment of better tools to secure the human interface could potentially reduce cybersecurity threats via email systems, in particular. In the meantime, targeted phishing attacks are reported to be increasing.

> [In September 2017,] Dragos picked up a new adversary, code-named "Covellite." ... Covellite has been targeting electric utilities in the U.S., Europe, and parts of East Asia with spear-phishing attacks that employ code and infrastructure eerily similar to that used by the so-called Lazarus Group, the most destructive and outright criminal of the state-sponsored hacking gangs.[68]

Multi-factor authentication is one security method focused on the human factor, as it requires two or more credentials (i.e., a password, a biometric factor, and/or a security token) to verify an individual's identity prior to gaining access to a network.[69] Therefore, a combination of something you know (i.e. a password), something you have (i.e., a token), or something you are (i.e., a biometric) establishes you as a legitimate user.

Electric Power Cybersecurity Gaps

FERC has authority over wholesale power sales and the transmission of electricity in interstate commerce, while states have authority over retail sales by electric distribution systems. FERC acknowledged that the Energy Policy Act of 2005 excluded local distribution systems from its reliability mandate under Section 215 of the Federal Power Act, as not being part of the bulk power system. FERC's revised 2012 definition brought some of these larger distribution system components under BES regulation, without bringing the distribution utilities under FERC's

---

[65] Ibid.

[66] According to the US-CERT, "Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords, that can further expose them to future compromises. Additionally, these fraudulent websites may contain malicious code." at https://www.us-cert.gov/report-phishing.

[67] Mathew J. Schwartz, *More Phishing Attacks Target Ukraine Energy Sector*, Information Security Media Group, January 22, 2016, http://www.bankinfosecurity.com/phishing-attacks-again-target-ukraine-energy-sector-a-8822/op-1.

[68] Daily Beast, *North Korean Hackers May Be Developing Malware That Could Shut Down the U.S. Power Grid*, March 1, 2018, https://www.thedailybeast.com/north-korean-hackers-may-be-developing-malware-that-could-shut-down-the-us-power-grid?ref=scroll.

[69] TechTarget Network, *Multifactor Authentication*, 2018, https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.

broader jurisdiction. However, most distribution systems are not required to comply with NERC CIP cybersecurity standards.

Mutual Dependency of Critical Infrastructure

Electricity production depends in large part upon other critical infrastructure sectors for fuel, fuel delivery, and support systems. PPD-21 also establishes Energy and Communications systems as "uniquely critical" infrastructure.[70] 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.

However, while the bulk electric system has mandatory and enforceable physical and cybersecurity rules, other critical infrastructure needed for the electric power sector to function does not. It is unlikely that an adversary capable of causing extreme impairment to the electric power system would overlook other, less protected critical infrastructure.

> Cybersecurity risks against the power and pipeline sectors are similar, as both use similar control systems, and there appears to be a broad consensus that cyber threats to this infrastructure are on the rise. Furthermore, with ever-greater physical interdependency between electricity generators and the natural gas pipelines that supply their fuel, many in Congress recognize that grid and pipeline cybersecurity are intertwined.[71]

Artificial Intelligence for Cybersecurity

With the introduction of digital Smart grid technologies to enhance and modernize grid operations, the speed and processing power of microprocessor-based ICS networks enhances the efficiency and control of power production and flows across electricity transmission and distribution systems. While the benefits to the electric power system and its users are many, there are potential risks as many IT and OT systems are connected to the Internet to improve data collection and information sharing. However, this exposure to the Internet leads to increased cybersecurity risks.

Artificial Intelligence

Artificial Intelligence (AI) is one of the technologies being deployed to mitigate cybersecurity risks. AI is a combination of computational technologies, machines, and software which have the capability to learn from inputs and be self-directed. AI allows computer systems to simulate human learning and problem solving.[72]

> Artificial intelligence algorithms are designed to make decisions, often using real-time data. They are unlike passive machines that are capable only of mechanical or predetermined responses. Using sensors, digital data, or remote inputs, they combine information from a variety of different sources, analyze the material instantly, and act on the insights derived from those data. With massive improvements in storage systems,

[70] See Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[71] CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by (name redacted), (name redacted), and (name redacted) .

[72] For more information on AI, see CRS In Focus IF10608, *Overview of Artificial Intelligence*, by (name redacted).

> processing speeds, and analytic techniques, they are capable of tremendous sophistication in analysis and decision making.[73]

The speed of processing of AI systems are currently seen as providing protection for ICS and other networks that human operators may not be able to match, especially as cyber attackers are employing increasingly sophisticated methodologies.[74]

One form of AI is Machine learning—algorithms based on statistical techniques—which give computer systems the ability to learn from a set of situations, and make decisions based upon alternative scenarios in reaction to those situations rather than from programmer instructions. The algorithms also adapt in response to new data and experiences to improve efficacy over time.[75] Under these circumstances, AI can potentially respond to a cyber attack scenario far more quickly than a human decision maker.

Data Analytics

Electric utilities are collecting massive amounts of data from ICS networks and customer-information systems. Generally, this accumulation is referred to as "Big data."

> Big data refers to the growth in the volume of structured and unstructured data, the speed at which it is created and collected, and the scope of how many data points are covered. Big data often comes from multiple sources and arrives in multiple formats.[76]

Using Data Analytic techniques, Big data can be turned into useful information.[77] High performance computing can take advantage of fast processing to examine data sets collected from Smart Grid systems into operational information, providing insights into customer behavior. It can also be used to recognize (or potentially predict) patterns or trends in data of new physical or cybersecurity threats to the grid.

Risks with AI and Machine Learning

The processing speed of Smart grid devices, coupled with the use of AI systems, also presents a cybersecurity potential vulnerability. AI systems learn from experience, and some observers say that these systems may be of limited use in cybersecurity defenses. Machine learning decisions made are based on the data the machine learning is trained and tested on. Machine learning is also subject to bias inherent in the data used to train the machines, as the coding reflects the preconceptions of the coding's programmers.

> AI systems are typically only as good as the data on which they are trained. They crystallize any biases or falsehoods found in their training data [Barocas, S., and A. D. Selbst, "Big Data's Disparate Impact," *California Law Review*, vol. 104, 2016.] The application of AI

[73] Darrell M. West and John R. Allen, *How Artificial Intelligence Is Transforming the World*, Brookings Institution, April 24, 2018, https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

[74] Salvador Llopis Sanchez, *Artificial Intelligence (AI) Enabled Cyber Defence*, European Defence Matters, 2018, https://www.eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-(ai)-enabled-cyber-defence.

[75] DOE, *An Executive's Guide to AI*, https://www.energy.gov/sites/prod/files/2018/05/f51/An-executives-guide-to-AI.pdf.

[76] Definition of Big Data at https://www.investopedia.com/terms/b/big-data.asp.

[77] "Data analytics is the process of examining data sets in order to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software. Data analytics technologies and techniques are widely used in commercial industries to enable organizations to make more-informed business decisions and by scientists and researchers to verify or disprove scientific models, theories and hypotheses." See http://searchdatamanagement.techtarget.com/definition/data-analytics.

> to surveillance or cybersecurity for national security opens a new attack vector based on this data diet vulnerability. Adversaries may learn how to systematically feed disinformation to AI surveillance systems, essentially creating an unwitting automated double agent.[78]

Thus, the bias of the programming can restrict how the machine learning addresses a situation. However, AI is a tool that can be used for offensive as well as defensive cybersecurity applications.

> The next generation of situation-aware malware will use AI to behave like a human attacker: performing reconnaissance, identifying targets, choosing methods of attack, and intelligently evading detection. Just as organizations can use artificial intelligence to enhance their security posture, cybercriminals may begin to use it to build smarter malware.[79]

Adversaries may discover how to use AI to stage future attacks on the grid, designed to disguise the intrusion and then overwhelm defenses.

> One factor restricting intelligence in malware is the need for small malware payloads to prevent detection… But it is conceivable that future developments in swarm or distributed AI may result in strategic botnets with small malware payloads but devastating effects.[80]

Improving Grid Cybersecurity

The Aurora simulation in 2007 was the first known event which proved that power plants could be vulnerable to a cyber attack.

> An AURORA attack results when a circuit breaker or breakers are opened and closed, resulting in an out-of-phase condition that can damage alternating current (AC) equipment connected to the grid. A demonstration of this for the Department of Homeland Security, conducted at the Idaho National Laboratory (INL) in 2007, was broadcast by CNN. [81]

AURORA demonstrated how a cyber attack could be used to destroy power generation equipment.[82]

Three years later, the Stuxnet attack against the industrial control system of an Iranian nuclear fuel enrichment plant provided the next warning. [83] Electric utilities were now aware that they must be prepared to address cyberthreats from a number of potential sources.

---

[78] Osonde A. Osoba and William Welser IV, *The Risks of Artificial Intelligence to Security and the Future of Work*, RAND Corporation, PE-237-RC (2017), 2017, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf.

[79] Derek Manky, *Artificial Intelligence: Cybersecurity Friend or Foe?*, InformationWeek, May 11, 2017, https://www.darkreading.com/threat-intelligence/artificial-intelligence-cybersecurity-friend-or-foe-/a/d-id/1328838.

[80] Osonde A. Osoba and William Welser IV, *The Risks of Artificial Intelligence to Security and the Future of Work*, RAND Corporation, PE-237-RC (2017), 2017, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf.

[81] Michael Swearingen, Steven Brunasso, and Joe Weiss, et al., *What You Need to Know (and Don't) About the AURORA Vulnerability*, Power Magazine, September 1, 2013, http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1.

[82] Jeanne Meserve, *Sources: Staged Cyberattack reveals Vulnerability in Power Grid*, CNN, September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

[83] David Kushner, *The Real Story of Stuxnet*, IEEE Spectrum, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Cybersecurity threats can arise from a number of sources, including deliberate cyber attacks by professional hackers, and acts of malice from discontented current or former employees.[84] They can also result from professional attackers, industrial spies, and organized crime groups,[85] and other groups with hacking capabilities such as hacktivists.[86] However, some observers would say that while terrorists[87] e.g., in seeking to damage the U.S. economy) may be able to buy the technical capacity for a cyber attack on the grid from hacktivists, they would be more likely to seek an attack causing direct physical destruction.

Increasing Cyber Monitoring and Incident Reporting

NERC aims to increase monitoring of the bulk electric system, and has proposed a plan for the E-ISAC to be staffed 24 hours daily. NERC states in its proposed 2019 budget that:

> 24x7 onsite capabilities could provide significant benefits to members, including (1) timely analysis and information sharing regarding developing physical or cyber security incidents that are discovered or occur outside of normal hours, and (2) the continued development of actionable intelligence during the overnight and weekend hours to enhance industry's preparation for, and response to, any potential physical or cyber security threat or incident.[88]

[84] "National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures. The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures. Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks." Industrial Control Systems Cyber Emergency Response Team, *Cyber Threat Source Descriptions*, 2016, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#hack. (Hereinafter, ICST).

[85] "International corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent. Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat." ICST.

[86] "Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause." ICST.

[87] "Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks. Their goal is to spread terror throughout the U.S. civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the U.S. and attacks to weaken the U.S. economy to detract from the Global War on Terror." ICST.

[88] NERC, *2019 Business Plan and Budget*, Draft 1, May 18, 2018, https://www.nerc.com/gov/bot/FINANCE/19BusPlanBud/2019%20NERC%20Business%20Plan%20and%20Budget.pdf.

FERC Increasing Reporting of Cyber Incidents

FERC also seeks increased reporting of cyber incidents. Currently, under critical infrastructure protection reliability standard CIP-008-5 for (Cyber Security – Incident Reporting and Response Planning), incidents must be reported only if they have compromised or disrupted one or more reliability tasks. FERC has directed NERC to expand the CIP-008 standard to require reporting of any attempts to break into a company's networks, rather than only reporting incidents that compromise a company's critical operations:

> Responsible entities must report cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS);
>
> Cyber security incident reports should be standardized to improve the quality of reporting and allow for ease of comparison across reports, analysis, and trending;
>
> Cyber security incident reports would be sent to those organizations best equipped to assess threats and communicate them to industry. Specifically, reports will continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC); the reports would also be sent to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). NERC would file an annual, public and anonymized summary of the reports with the Commission.[89]

Mandatory DOE Reporting of Grid Incidents and Disturbances

DOE, for its part, has established its own mandatory reporting requirements for U.S. electric utilities experiencing emergency incidents and disturbances.[90]

> Form OE-417 alerts the Department of Energy to electrical emergency incidents and disruptions. The ability of the DOE to quickly respond to energy emergencies that may impact the nation's infrastructure and help alleviate or prevent further disruptions depends on the industry's prompt response. As such, the timely filing of this form is of paramount importance.[91]

Electric power incidents and outages have various criteria for reporting depending on the level of urgency of the situation. An *Emergency Alert* must be filed within one hour of an incident, and includes physical attacks causing major interruptions or impacts to critical infrastructure facilities or to operations, cyber incidents causing interruptions of electrical system operations, and incidences of uncontrolled loss of 300 Megawatts or more of firm system loads (i.e., power provided to customers that is continuously available on demand and which is subject to interruption only under extreme circumstances) for 15 minutes or more from a single incident.[92]

Normal reports (due within six hours of company incidents), and *System* reports (for wider system issues, due by the later of 24 hours after the recognition of the incident or by the end of the next business day) have lesser criteria for notification of DOE.[93]

---

[89] FERC, *FERC Requires Expanded Cyber Security Incident Reporting*, July 19, 2018, https://www.ferc.gov/media/news-releases/2018/2018-3/07-19-18-E-1.asp#.W1X8jFNG2go.

[90] DOE, *Electric Emergency Incident and Disturbance Report*, Form OE-417, 2018, https://www.oe.netl.doe.gov/docs/OE417_Form_Instructions_05312021.pdf.

[91] Ibid.

[92] Ibid. Any incidence of one or more of the criteria occurring can necessitate an Emergency Alert report.

[93] Ibid. pp. 2-3.

DOE states that in addition to national security response, the information collected by Form OE-417 is to be used for reporting on electric power emergency incidents and disturbances in monthly Energy Information Administration (EIA) reports, and that it may use the data to develop legislative recommendations and reports to Congress, and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Enhancing the Threat/Risk Assessment

Many cybersecurity actions are reactive to the last threat discovered. While intrusion detection is considered a priority, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks to address their motivations (e.g., to extort money or to cause damage). Others might differ, saying that the focus should be on the attack and the system vulnerability exploited. Some utilities are undertaking security improvements in modernization programs, while other improvements would potentially have to be undertaken as special projects because of limitations for cost recovery under traditional cost-of-service ratemaking regulations under state government jurisdiction.[94] In such instances, the improvements may have to be justified as "used or useful" in providing electricity service to customers in utility rate cases.

Very often, the relative level of sophistication of the threat is related to the origin of the threat. Since many cyberthreats appear to originate from foreign entities (including some with nation state affinities), intelligence on the existence and nature of the threat, as well as the capability of dealing with the threat, often relies on the federal government's national security apparatus. Therefore, the information communicated from the government is generally more useful when it is both timely and relevant as to the severity of a threat, and communicate whether a need exists for immediate action. The electricity industry then provides the expertise necessary for understanding the relative risk to the grid of the potential threat, and the appropriate avenues for communicating the threat information.

The National Cybersecurity and Communications Integration Center (NCCIC) under the Department of Homeland Security's National Protection and Programs Directorate largely has the role of informing the electricity industry of cyber and physical threats to the grid.[95] The NCCIC is focused on cyber situational awareness, incident response, and management, and coordinates with the Electricity Information Sharing and Analysis Center (E-ISAC), operated by the North American Electric Reliability Corporation.

> The E-ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the Electricity Subsector, across interdependent sectors, and with government partners.[96]

The E-ISAC runs the voluntary NERC Cybersecurity Risk Information Sharing Program, which aims to facilitate a nearly real-time sharing of government enhanced threat information, enhance

[94] Many utilities operate under traditional regulatory regimes where the cost of providing electric power to end-use customers is subject to approval by state authorized public utility commissions (or similar state organizations).

[95] "The NCCIC works closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems, and actively engages with private sector companies and institutions, state, local, tribal, and territorial governments, and international counterparts. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with." DHS, "About the National Cybersecurity and Communications Integration Center," November 4, 2014, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

[96] E-ISAC, *Electricity Information Sharing and Analysis Center*, 2016, https://www.esisac.com/.

situational awareness, and better protect critical infrastructure.[97] CRISP deploys passive sensors called Information-Sharing Devices (ISDs) on participant company networks. The ISDs send encrypted data to an analysis center operated by the Pacific Northwest National Laboratory,[98] which analyzes the data, sending alerts with mitigation measures to CRISP participants through a secure network.[99] As of the end of 2015, 75% of U.S electricity customers were covered by companies which had deployed CRISP.[100] The Electricity Subsector Coordinating Council (ESCC), an entity led by industry chief executive officers and is the principal liaison between the federal government and the electric power sector, has called for the E-ISAC to be the "central source of information sharing between the Electricity Subsector and the government."[101]

Building Resiliency into the Grid

There has been speculation that a major cyber attack may be inevitable, given the many diverse actors in the cyber threat space with both political and apolitical motivations. Given such scenarios, some resources are focused on actions and technologies which can aid recovery from a cyber attack. Several potential courses to improve resiliency and which may quicken recovery efforts from a potential attack on the grid are discussed below.

Building the Smart Grid

New technologies are being considered for their potential to enhance electric power transmission and distribution system resiliency. For example, a 2013 report from the Electric Power Research Institute (EPRI) reviews innovative technologies for their ability to make the distribution system more resilient to weather-related power outages or terrorist attacks.[102] These innovations range from use of plug-in electric vehicles and solar photovoltaic systems as back-up power supplies for residences, to community energy storage projects using batteries.

Smart Grid technologies have also been proposed for reliability and resiliency. Sensors and automated controls can use real-time data to reconfigure a utility network to isolate problems.[103] One such system is called Dynamic Circuit Reconfiguration.[104]

---

[97] Marcus Sachs, *NERC Comments on Reliability*, FERC, FERC Reliability Technical Conference, June 1, 2016, http://www.ferc.gov/CalendarFiles/20160601082816-Sachs,%20NERC.pdf. (Hereinafter, FERCN).

[98] The Pacific Northwest National Laboratory has a national security function through its connection with DOE. See Pacific Northwest National Laboratory, *National Security*, July 2016, http://www.pnnl.gov/nationalsecurity/.

[99] American Public Power Association, *NERC Plans Major New Initiative on Cybersecurity Information Sharing*, September 4, 2014, http://publicpower.com/2014/nerc-plans-major-new-initiative-cybersecurity-information-sharing/.

[100] Testimony of William Spence, Chief Executive Officer, PPL Corporation. U.S. Congress, House Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings and Emergency Management, *Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?*, 114th Cong., 1st sess., April 14, 2016.

[101] FERCN, p. 3.

[102] Electric Power Research Institute, *Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies*, January 11, 2013, http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026889. (Hereinafter, EPRI.)

[103] See CRS Report R45156, *The Smart Grid: Status and Outlook*, by (name redacted) .

[104] "Many utilities have successfully deployed Distribution Automation with Optimal Network Reconfiguration. These systems involve the deployment of automated distribution switches/sectionalizers/reclosers, sensors, communications, control systems, and data analytics to automatically reconfigure circuit connections in order to maximize service restoration." EPRI, p. 7.

> Once deployed, these systems serve two roles. First, they limit the number of customers affected by faults.... Second, once the fault is isolated ... the systems enable restoration of service to unaffected sections from adjacent [circuit connections].[105]

EPRI emphasizes that such practices "must be tailored to events of different magnitudes and to different types of disruption (wind, flood, tsunami, earthquake, and terrorist or cyber attacks, etc.)."[106]

While Smart Grid solutions would utilize fast acting sensors and tools to gather and analyze information, the controls for the system would likely have to be located in a combination of central and distributed locations to aid a resilient cybersecurity strategy. However, distributed data centers powered by energy supplies independent of the grid may be needed to ensure that recovery from a cyber attack is not hampered by the loss of information and data needed to recover operations and business systems.

Distributed Energy Resources

Distributed resources[107] and microgrids[108] are also being considered both in terms of making the current grid more resilient and as an increased element of the future grid. The state of New York (among others) has been working with investor-owned electric utilities on a plan to deploy distributed resources at scale as part of its plan to modernize its energy systems.[109] The ability of microgrids to operate independently of the grid has potential in a cyber attack or other emergency,[110] and power can be generated by fossil fuel, combined heat and power plants, or renewable energy systems. Microgrids are also being investigated by the DOE as an element of a modern energy future for the grid.[111] Distributed generation[112] is growing and could potentially be a source for black start[113] power in the event of a grid failure, but these smaller power plants

[105] Ibid.

[106] EPRI, p.8.

[107] Distributed resources include energy efficiency, demand response, solar PV, wind power, energy storage, combined heat and power (cogeneration), and other technologies.

[108] A microgrid may be defined as "any collection of interconnected loads and distributed energy resources (i.e., distributed generation) within clearly defined electrical boundaries that can be controlled as a single entity and that can operate in both grid-connected or island mode (i.e., non-grid connected)." Gail Reitenbach, "Interest Growing in Commercial and Community Microgrids," *Power Magazine*, June 26, 2014, http://www.powermag.com/interest-growing-in-commercial-and-community-microgrids/.

[109] New York State Department of Public Service, *Reforming the Energy Vision*, January 28, 2016, http://www3.dps.ny.gov/W/PSCWeb.nsf/All/CC4F2EFA3A23551585257DEA007DCFE2.

[110] However, microgrids must have adequately protected operational control systems which will enable quick disconnection and independent operation (from the grid) if a fault or grid failure is detected.

[111] DOE, *Energy Department Announces Funding to Improve the Resiliency of the Electric Grid*, 2014, http://energy.gov/articles/energy-department-announces-funding-improve-resiliency-electric-grid.

[112] Distributed Generation (DG) is the term used to describe electric power generated at or near the point of consumption (i.e., the customer or load). DG thus differs from base load power plants (mostly coal and nuclear power units) which were designed for economies of scale, and located usually at some distance from where the electricity is consumed. DG includes traditional backup power sources (such as the large gas- or diesel-powered generators used by institutions and companies), combined heat and power facilities (used for industrial, district, and community power generation), and renewable electricity power systems used by some businesses and residences.

[113] "A black start unit is one that can start its own power without support from the grid in the event of a major system collapse or a system-wide blackout. In the U.S., every region within the North American Electric Reliability Corp. (NERC) has its own black start plan and procedures. Each region also designates certain plants as black start units." Lindsay Morris, "Black Start: Preparedness for Any Situation," *POWER Engineering*, July 1, 2011, https://www.power-eng.com/articles/print/volume-115/issue-7/features/black-start-preparedness-for-any-situation.html.

would have to be protected against cybersecurity attacks if they were to help in a black start situation.

Building a Strategic Reserve of Critical Components

Large, high voltage electric power transformers (LPTs) have received special attention as a critical component of the bulk electric system which could be targeted in physical and cyber attacks. Reserves of LPTs are few since these are high cost items, and LPTs are not commonly manufactured in the United States. LPTs require a fairly long lead time to manufacture, and may be designed to meet a customer's specifications. The investor-owned electric utilities have had a transformer sharing program in place since 2006 with those utilities that wanted to participate.[114] Nonetheless, Section 61004 of the FAST Act required DOE to submit a plan to Congress evaluating the feasibility of establishing a Strategic Transformer Reserve for the storage, in strategically located facilities, of spare large power transformers and emergency mobile substations to temporarily replace critically damaged LPTs and substations.

In March 2017, DOE submitted a report to Congress on the strategic reserve, highlighting the issues of time to build, cost, and potential federal ownership of a strategic reserve, as well as issues of where to place and maintain a strategic reserve. DOE found that given FERC's approval of CIP-014 reliability standards, supporting enhanced industry programs for spare transformer sharing might be a better way to achieve a strategic reserve. DOE also stated that it is encouraging manufacturers to design transformers to meet high resilience standards for electromagnetic pulse (EMP) and geomagnetic disturbances (GMD), as well as physical and cybersecurity.[115]

However, given industry's general reticence to allocate funding for potentially high impact, but low frequency events (such as EMP attack, GMD, severe weather, or seismic events as mentioned in the FAST Act), it is unclear whether an enhanced industry approach alone would meet the concerns of many in Congress with regard to a strategic reserve.

Other Issues for Congress

The electric power industry does not have the intelligence gathering capabilities to deal with the many cyber and physical threats to the grid, many of which appear to originate internationally. Instead, the U.S. government analyzes all-source intelligence to understand threats to the energy grid and shares that information with the electricity industry, which has the capability and expertise to understand the risks posed to the grid. How that information could be better disseminated and on a timelier basis has been raised as an issue by the electric power industry.

The bulk electric system is subject to mandatory and enforceable critical infrastructure protection rules for cyber and physical security under the FERC's reliability mandate. However, the energy sector is one of 16 critical infrastructure sectors identified by the Department of Homeland Security. Given that the grid relies on several of the other sectors (for example, for water and fuel transportation), the question of whether these other sectors should also have similar, mandatory

[114] The Edison Electric Institute's Spare Transformer Equipment Program (STEP) program is a pool of LPTs in various voltage classes and sizes (Megavolt-amperes or MVA) located at member utilities throughout North America. Edison Electric Institute, *Spare Transformers*, 2018, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

[115] For example, new performance measures may be established to improve resilience. DOE, *Strategic Transformer Reserve*, March 2017, https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

standards focused on support of the electric power sector may be an issue for Congress to consider.

The electric power system in the United States is evolving, but not consistently across sectors and regions of the country. While some may say such inconsistencies may add a level of complexity that may make a nationwide cyber event more unlikely, the consistent development of a modern electric power system would likely add to the prospects of U.S. economic health and competitiveness. Policy options designed to ensure that the developing electric power system is as secure as possible will likely be a major consideration for Congress.

Recent Legislation

115th Congress

The Grid Cybersecurity Research and Development Act (H.R. 4120), introduced in October 2017, would require the DOE to develop an initiative to mitigate the consequences on the electric grid of cyber attacks by increasing grid cybersecurity. DOE would also be required to work with other agencies and the private sector to develop guidance for cybersecurity research and development to improve electric sector cybersecurity. NIST would be required to develop voluntary training standards, and maintain a public database of cybersecurity training programs. The ESCC would be required to develop a coordinated interagency strategic plan to advance grid cybersecurity capabilities.

The Pipeline and Liquefied Natural Gas Facility Cybersecurity Preparedness Act (H.R. 5175), introduced in March 2018, would require the Secretary of Energy to carry out a program in consultation with other federal agencies, states, and the energy sector to ensure security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas facilities. The DOE would also be required to coordinate response and recovery to physical and cyber incidents impacting the energy sector, and demonstrate advanced cybersecurity and technologies projects for physical and cybersecurity.

The Cyber Sense Act of 2018 (H.R. 5239), introduced in March 2018, would establish a voluntary DOE program for testing product cybersecurity and technologies intended for use in the bulk-power system, including products related to ICS. It would also authorize the DOE to provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to help mitigate cybersecurity vulnerabilities.

The Enhancing Grid Security through Public-Private Partnerships Act (H.R. 5240), introduced in March 2018, would promote and advance physical and cybersecurity of electric utilities. The bill would require the Secretary of Energy to carry out a program (in concert the Energy Reliability Organization, industry stakeholders, and other federal agencies) to, among other activities, develop voluntary implementation of maturity models, self-assessments, and auditing methods to assess the physical and cybersecurity of electric utilities; provide training for electric utilities to address and mitigate supply chain risks; increase opportunities for sharing best practices; assist with cybersecurity training for electric utilities; and advance the cybersecurity of third-party vendors that work in partnerships with electric utilities.

The Promoting Cybersecurity for Rural Electric Utilities Act (S. 2991), introduced in June 2018, would amend the Rural Electrification Act of 1936 (7 U.S.C. 931 et seq.) to provide that cybersecurity and grid security improvements are eligible for electric loans and guarantees under that act.

Appendix. Bulk Electric System Critical Infrastructure Protection Standards

Table A-1. NERC Critical Infrastructure Protection Standards

Bulk Electric System

Standard	Type[a]	Name	Description
Current Standards			
CIP-002-5.1a	C	BES Cyber System Categorization	To identify and categorize Bulk Electric System (BES) Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.[b] Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003-6	C	Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-004-6	C	Personnel and Training	To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
CIP-005-5	C	Electronic Security Perimeter(s)	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-006-6	C	Physical Security of BES Cyber Systems	To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-007-6	C	System Security Management	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-008-5	C	Incident Reporting and Response Planning	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
CIP-009-6	C	Recovery Plans for BES Cyber Systems	To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
CIP-010-2	C	Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Standard	Type[a]	Name	Description
CIP-011-2	C	Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-014-2	P	Physical Security	To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.
Filed and Pending FERC Approval			
CIP-005-6	C	Electronic Security Perimeter(s)	Modified to address certain directives in FERC Order No. 829.
CIP-010-3	C	Configuration Change Management and Vulnerability Assessments	Modified to address certain directives in FERC Order No. 829.
CIP-013-1	C	Supply Chain Risk Management	**New standard per FERC Order No. 829.**[c] To mitigate cyber security risks to the reliable operation of the Bulk Electric System by implementing security controls for supply chain risk management of BES Cyber Systems.

Source: CRS, See North American Electric Reliability Corporation, CIP Standards at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Notes:

a. Type indicates C—Cybersecurity or P—Physical Security Standard.

b. One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls. BES Cyber System is defined as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary), http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers to the bulk electric system.

c. Revised Critical Infrastructure Protection Reliability Standards, Order No. 829, 156 FERC ¶ 61,050, at P 43 (2016).

Author Contact Information

(name redacted)
Specialist in Energy Policy
[redacted]@crs.loc.gov, 7-....