Congressional Research Service
Informing the legislative debate since 1914

# Cybersecurity Issues for the Bulk Power System

**Richard J. Campbell**
Specialist in Energy Policy

April 16, 2015

**Congressional Research Service**
7-5700
www.crs.gov
R43989

**CRS REPORT**
Prepared for Members and
Committees of Congress

c11173008

# Summary

In the United States, it is generally taken for granted that the electricity needed to power the U.S. economy is available on demand and will always be available to power our machines and devices. However, in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system. In particular, the cybersecurity of the electricity grid has been a focus of recent efforts to protect the integrity of the electric power system.

The increasing frequency of cyber intrusions on industrial control (IC) systems of critical infrastructure continues to be a concern to the electric power sector. Power production and flows on the nation's electricity grid are controlled remotely by a number of IC technologies. The National Security Agency (NSA) reported that it has seen intrusions into IC systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."

As the grid is modernized and the Smart Grid is deployed, new intelligent technologies utilizing two-way communications and other digital advantages are being optimized by Internet connectivity. Modernization of many IC systems (in particular, the Supervisory Control and Data Acquisition [SCADA] system) also has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they also will increase its vulnerability to potential cyberattacks. *Black Energy*, *Havex*, and *Sandworm* are all recent examples of malware targeting SCADA systems. New devices (like smart meters) and increasing points of access (such as renewable electricity facilities) introduce new additional areas through which a potential cyberattack may be launched at the grid.

Many cybersecurity actions are reactive to the last threat discovered. While intrusion detection is a priority, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks. Cybersecurity strategies may shift from figuring out whether a system has been compromised to an understanding of who authored the malicious software and why. Although malware intrusions may not have resulted in a significant disruption of grid operations so far, they still have been possible even with mandatory standards in place. The North American Electric Reliability Corporation's (NERC's) current set of standards, Critical Infrastructure Protection (CIP) Version 5, is moving toward active consideration of bulk electric system security needs rather than just compliance with minimum standards.

Electric utilities emphasize the need for timely information sharing and advocate for liability protection from potential damages resulting from a major cyber event. Some observers argue that it is the responsibility of electric utilities to embrace security as part of their strategic business planning and operations. The National Electric Sector Cybersecurity Organization has identified six failure scenario domains intended to assist utility cybersecurity efforts. These scenarios also illustrate the continuing vulnerability of the grid to potential cyber and physical attacks, or a combination of both.

This report highlights several areas for congressional consideration to improve grid cybersecurity. One issue is whether electric utilities have the resources to make the financial investment and recruit staff to reduce vulnerabilities. Another issue is that NERC CIP standards do not apply to all points of grid connection to the distribution system, and these connections still may represent cyber vulnerabilities. The adequacy of current standards where they do apply is also an issue.

# Contents



## Figures



## Tables

# Contacts

# Introduction

In the United States, it is generally taken for granted that the electricity needed to power the U.S. economy is available on demand and will always be available to power our machines and devices. However, in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system. In particular, the cybersecurity[1] of the electricity grid has been a focus of recent efforts to protect the integrity of the electric power system.[2]

Power flows on the nation's electricity grid are remotely controlled by a combination of older, legacy systems and newer control technologies. Many of these legacy technologies are analog in design and were not originally connected to the Internet[3] (although many are equipped with radio or other communications capabilities). But as the grid is modernized, the new "intelligent" technologies replacing them use advanced two-way communications and other digital advantages that likely will be optimized by Internet connectivity. While these advances will improve the efficiency and performance of the grid, they also potentially increase the vulnerability of the grid to cyberattacks.

Cybersecurity is today, and will continue to be, a major issue and focus area for the electric power sector. The energy sector (i.e., electricity, natural gas, and petroleum) is one of 16 critical infrastructure sectors designated by the Department of Homeland Security.[4] Incidents of reported cyber intrusions and attacks aimed at undermining the U.S. grid appear to be increasing.[5] While parts of the electric power subsector have mandatory and enforceable cyber and physical security standards,[6] some have argued that minimum, consensus-based standards are not enough to secure the system.[7] Further, the electric grid is not isolated from attacks on other critical infrastructure

[1] Cybersecurity may be defined as the secure (i.e., protected from outside intrusion, corruption or other unauthorized access) operation of networks, computers, hardware, and software systems for business and industrial control processes.

[2] The Energy Independence and Security Act (EISA) of 2007 (P.L. 110-140) outlined requirements for "a reliable and secure electricity infrastructure" with regard to electric system modernization and Smart Grid development. EISA directed the National Institute of Standards and Technology (NIST) to develop a framework for protocols and standards for the Smart Grid to achieve "interoperability" of devices and systems.

[3] Analog systems can represent cybersecurity vulnerabilities, especially if these are modem-connected and the modem is unsecured. U.S. Department of Homeland Security, National Cyber Security Division, *Recommended Practice for Securing Control System Modems*, January 2008, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/SecuringModems.pdf.

[4] See http://www.dhs.gov/critical-infrastructure-sectors.

[5] According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), there were 140 cyber incidents reported in 2011, 197 in 2012, and 257 cyber incidents reported in 2013. Of the incidents reported in 2013, 56% were directed at energy critical infrastructure, with most directed against electricity infrastructure. This can be compared with 2012, in which 41% of incidents involved energy (again, mostly electricity) facilities. See https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf.

[6] The Federal Energy Regulatory Commission (FERC) adopted the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) Version 5 standards for cybersecurity in April 2014 and subsequently adopted NERC CIP-014 for reliability standards addressing risks due to physical security threats and vulnerabilities in May 2014. See CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

[7] As will be discussed later in this report, a new set of cybersecurity standards have been revised to emphasize security over compliance and go into effect later this year.

sectors on which it depends (i.e., the natural gas subsector, water, and transportation), and mandatory and enforceable cybersecurity standards apply to only a few of the 16 critical infrastructure sectors.[8]

This report will discuss the current state of electric sector cybersecurity, surveying existing regulations and proposed efforts to improve cybersecurity in the wake of recently reported threats and potential vulnerabilities. The report will focus on the bulk power system[9] under authority of the Federal Energy Regulatory Commission (FERC), which Congress directed to establish mandatory and enforceable reliability standards.[10] Many cybersecurity standards and actions are in response to cyber events. As such, basic compliance with standards by electric utility companies may not be enough to achieve effective cybersecurity protections. Areas for possible further congressional consideration or action will be highlighted in this report.

# Grid Components and Potential Vulnerabilities

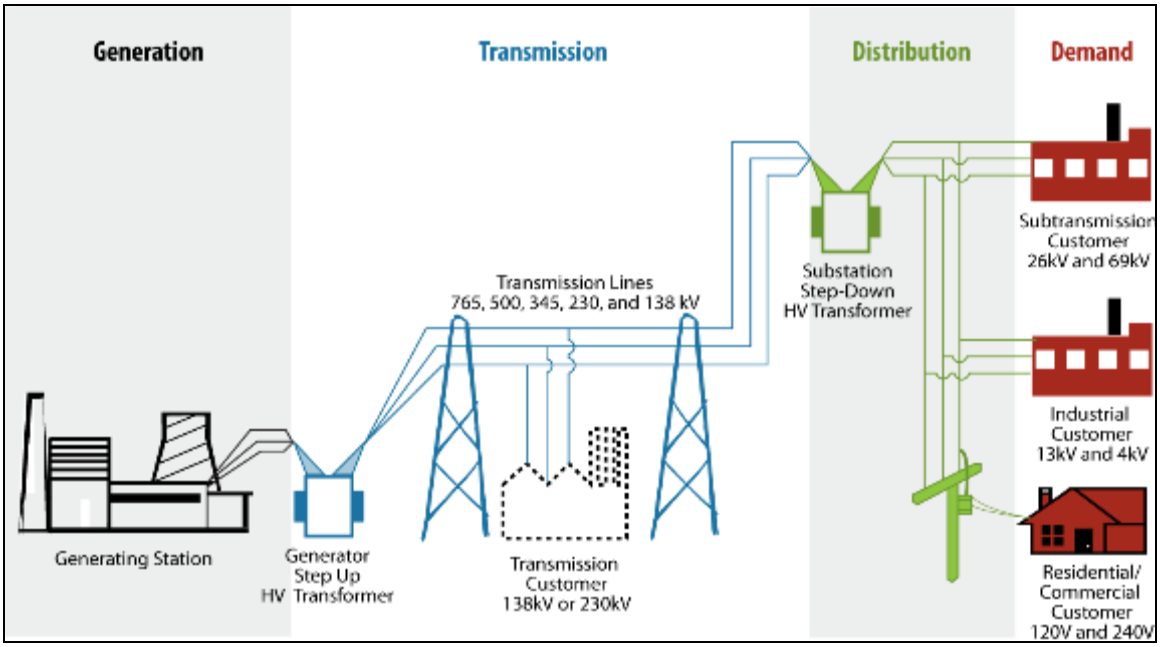
The electric utility business encompasses the process of generating electricity and sending power to the ultimate user. The electrical grid is the name given to the machinery and power lines that enable power to be sent from the power plant to the ultimate user of electricity. As seen in **Figure 1**, this generally requires an infrastructure made up of generating stations (where the power is produced), step-up transformers and transmission lines (whereby transformers increase the voltage so that the electricity can be sent over very long distances), and step-down transformers and distribution lines (whereby the voltage can be lowered allowing the electricity to be sent to businesses and homes to power machinery and devices). Depending on the regulatory regime in place, these system elements may be controlled by companies under state jurisdiction or entities under federal jurisdiction (such as regional transmission organizations or federal power marketing administrations).

[8] "Other critical infrastructure entities, such as depository institutions in the banking and finance sector; the bulk power system in the electricity subsector of the energy sector; the health care and public health sector; and the nuclear reactors, materials, and waste sector, are required to meet mandatory cybersecurity standards established by federal regulation." U.S. Government Accountability Office, *Cybersecurity - National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, p. 47, http://www.gao.gov/assets/660/652170.pdf.

[9] The bulk power system includes electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kilovolts or higher. The bulk power system generally does not include distribution system facilities, which are regulated by state or local authorities. See http://www.nerc.com/files/Glossary_2009April20.pdf.

[10] FERC received primary responsibility for the reliability of the bulk power system from the Energy Policy Act of 2005 (P.L. 109-58).

**Figure 1. Electric Power System Elements**




**Source:** Congressional Research Service, based on graphic found at https://reports.energy.gov/BlackoutFinal-Web.pdf (p. 5).

**Notes:** kV = kilovolts (or 1,000 volts).

Controlling and monitoring the various parts of the grid are industrial control (IC) systems, some of which are connected to the Internet. Other IC systems are not Internet-connected, and still rely on local area networks (LANs) or similar systems for control and reporting. The following paragraphs discuss these IC systems and potential vulnerabilities to intrusion and cyberattack.

## Electric Utility Industrial Control Systems

The 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 IC systems, managing power plant controls, transformer yard and power bus[11] functions, transmission system, and distribution substations.

The IC system essentially operates in a "control loop" in which sensors continually check key components, with variable responses against control variables in order to ensure that the system is functioning as designed. If responses show a disturbance resulting in operation of the system outside normal operating parameters, then the system adjusts actuators to bring the system back to process norms, or sends alerts to human-machine interfaces[12] (HMIs) to reconfigure the system

[11] The bus bar is the point at which electrical power from the power plant is connected to transmission system.

[12] "The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software." See Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, NIST Special Publication 800-82, June 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf. (Hereinafter NISTICS).

or adjust operations in the control algorithms. Diagnostics and maintenance utilities are built into the system to "prevent, identify and recover from abnormal operation or failures."[13]

## Supervisory Control and Data Acquisition Systems

One IC system used to control remote operations of the power grid is the Supervisory Control and Data Acquisition (SCADA) system.

> SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation ... A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.[14]

SCADA systems have been in use at least since the 1970s, and were adopted at a time when the focus of system design was on function and reliability. An example of a basic SCADA network is shown in **Figure 2**. Historically, these systems consisted of remote terminal units[15] which were often connected to a mainframe computer via telephone lines or radio connections. They were not typically connected to centralized networks. Utilities typically operated separate control systems created just to operate power plants and related infrastructure.[16]

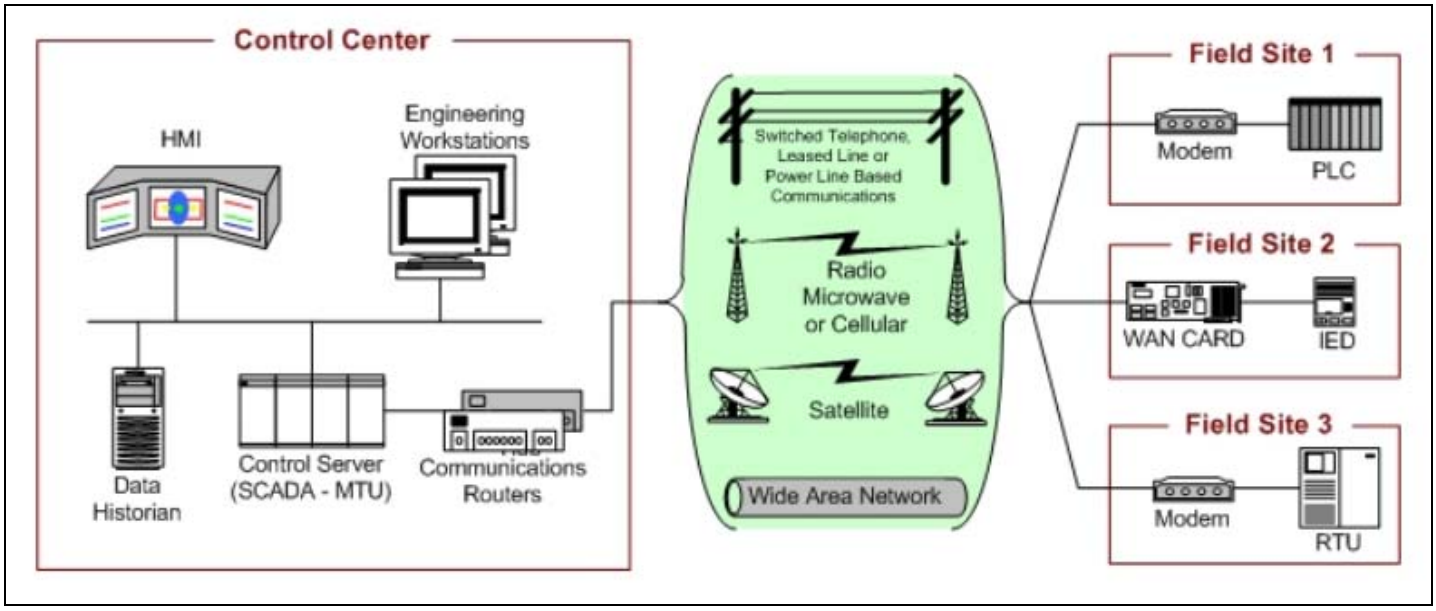
[13] Ibid.

[14] Ibid.

[15] "RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable." NISTICS.

[16] Stew Magnuson, "Power Companies Struggle to Maintain Defenses Against Cyberattack," *National Defense Magazine*, March 2014, http://www.nationaldefensemagazine.org/archive/2014/March/Pages/PowerCompaniesStruggletoMaintainDefensesAgainstCyberattacks.aspx.

**Figure 2. SCADA System General Layout**




**Source:** See *Guide to Industrial Control Systems Security* at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

**Notes**: WAN = Wide Area Network; MTU = Master Terminal Unit (server for SCADA system); IED = Intelligent Electronic Device; RTU = Remote Terminal Unit.

Over time, modification of SCADA systems has resulted in connection of many of these older, legacy systems to the Internet. However, many of these legacy SCADA systems were not designed with security features, allowing other potential pathways for a cyberattack.[17] As a result, these systems may be vulnerable to intrusion through data reporting pathways, or attacks (for example) using a thumb drive to download malware like the Stuxnet worm.[18] However, some of these earlier designs and configurations may not be as vulnerable to an Internet-launched cyberattack. The security issue, for old and new systems, then becomes both how they are connected to the utility's other systems, and what levels of security exist to detect and deter potential intrusions.

## Distributed Control Systems

Distributed control systems (DCSs) are used in power plant settings where process control requires feedback to maintain process conditions automatically about a desired set point. DCSs generally use several Programmable Logic Controllers (PLCs) to establish process tolerances. PLCs are typically microprocessor- or computer-based devices that are used extensively to

[17] "[These] vulnerabilities ... had been overlooked because taking advantage of them requires an attacker to have access to closed, local networks. Now, a cyberterrorist with a little knowledge and the right laptop can gain that access and cause chaos in a regional power system merely by linking up with the control panel at a secluded electric vehicle charging station." See Evan Halper, "Security holes in power grid have federal officials scrambling," *Los Angeles Times*, April 7, 2014, http://touch.latimes.com/#section/-1/article/p2p-79841438/. (Hereinafter CyberLT).

[18] "A computer worm differs from a virus in that the latter requires user action to set in motion of set of potential harmful activities whereas a worm is self-executable and will burrow its way through an operating system until it reaches its intended target." For more on Stuxnet, see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

control industrial equipment or processes. Communications over DCS or PLC networks need to be more reliable and function at higher speeds "compared to the long-distance communication systems used by SCADA systems" because of the process control functions of DCSs.[19]

## Modernization and the Smart Grid

The electric grid of the United States has been called an "engineering marvel," but it is a system which in many places is becoming an "aging marvel."

> America relies on an aging electrical grid and pipeline distribution systems, some of which originated in the 1880s. Investment in power transmission has increased since 2005, but ongoing permitting issues, weather events, and limited maintenance have contributed to an increasing number of failures and power interruptions. While demand for electricity has remained level, the availability of energy in the form of electricity, natural gas, and oil will become a greater challenge after 2020 as the population increases. Although about 17,000 miles of additional high-voltage transmission lines and significant oil and gas pipelines are planned over the next five years, permitting and siting issues threaten their completion.[20]

In recognition of the need to deploy new technologies, Congress indicated its support for grid modernization in the Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140). Specifically, Section 1301 of the act states:

> It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth ... which together characterize a Smart Grid...

The "Smart Grid" refers to the evolving electric power network as new information technology (IT) systems and communications capabilities are incorporated. EISA Section 1301 further states that aspects characterizing a Smart Grid include

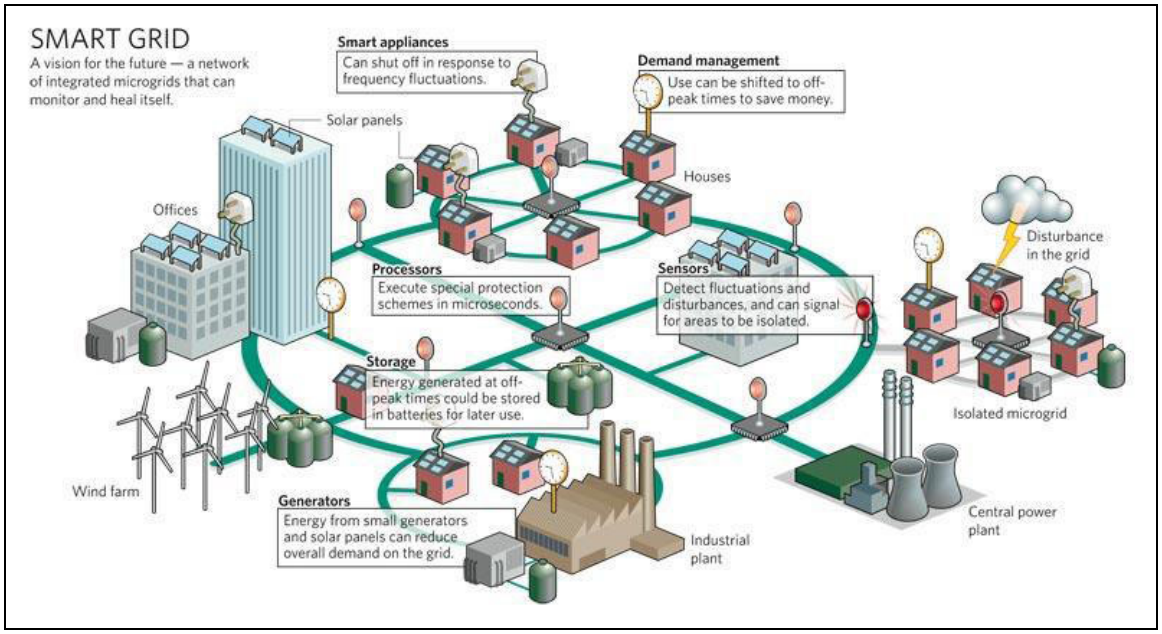
- Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
- Dynamic optimization of grid operations and resources, with full cybersecurity.
- Deployment of ''smart'' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

**Figure 3** provides a conceptual illustration of what a Smart Grid network may look like. The many disparate elements and user systems also emphasize the need for secure communications pathways required for Smart Grid operation.

[19] NISTICS.

[20] American Society of Civil Engineers, *Report Card for America's Infrastructure 2013*, p. 2013, http://www.infrastructurereportcard.org/energy/.

**Figure 3. Concept of a Smart Grid Network**




**Source:** Consumer Energy Report. See http://www.consumerenergyreport.com/wp-content/uploads/2010/04/smartgrid.jpg.

Smart Grid networks are also potentially better able to integrate the intermittent energy from renewable electricity technologies (i.e., renewable electricity systems such as distributed solar photovoltaic [PV] and wind), distributed generation, demand response, and consumer energy efficiency programs.[21]

While the potential of the Smart Grid to revolutionize the ways power is generated and used is great, so too are the potential cybersecurity risks.[22] Additional Smart Grid components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyberattack. Smart Grid components are built around microprocessor and other hardware devices whose basic functions are controlled by software programming. These devices and functions may be subject to manipulation over a network.[23] The information processing and communications attributes which make the Smart Grid attractive are the very same attributes which can increase the vulnerability of the electric power system and its critical infrastructure to a possible cyberattack. This risk is potentially increased for systems connected to the Internet.

[21] Department of Energy, *Enhancing the Smart Grid: Integrating Clean Distributed and Renewable Generation*, 2009, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/RDSI_fact_sheet-090209.pdf.

[22] CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[23] IEEE Smart Grid, *IEEE Smart Grid Cyber Security Round Up*, 2015.

## Other Potential Vulnerabilities

The grid has other potential vulnerabilities and avenues that a cyberattacker might seek to exploit. Independent researchers are reported to have found hacking into grid computer networks to be "startlingly easy," and they have alerted authorities to their findings.[24] While new security systems and controls are added to address known weaknesses, new vulnerabilities may emerge as new devices and avenues of access are added.

### *Distributed Generation*

Renewable electricity generation is increasing and is highly distributed to capture the best renewable resources available to maximize the amount of power generated. However, these facilities can represent potential backdoors for cyberattackers to access the grid. Renewable electricity companies in Europe reportedly were targeted by cyberattackers at a clean power website from which malware was passed to visitors, thus giving the attackers access to the power grid:

> The communication networks and software that link green energy sources to the grid as well as the electronic meters that send real time power usage to consumers and utilities are providing new back-door entry paths for computer hackers to raise havoc with the grid.[25]

### *Smart Meters*

Smart meters are an example of new systems added to the grid. While such systems are designed with security in mind (i.e., following international standards using best practices such as encryption of sensitive data, system protection from viruses and malware, access control and tamper alerts on meters, and two-party authorization), systems analysts acknowledge that such connected systems can have new vulnerabilities.[26] Smart meters were singled out as a vulnerability by a report as potentially being susceptible to fraud from "manipulated meter readings, misuse of private customer data and a threat of power outages through a large cyberattack."[27] One particular weakness was said to be the built-in encryption of data sent from smart meters to utilities. The meters are designed to last approximately 20 years, but it was speculated that the device's built-in cryptology system may not be secure for that long a period.[28] However, another source says that smart meter encryption and authentication "should be readily and proactively updatable" and combined with intrusion detection to better protect networks.[29]

---

[24] CyberLT.

[25] Louise Downing and James Polson, "Hackers Find Open Back Door to Power Grid With Renewables," *Bloomberg Business*, July 2, 2014, http://www.bloomberg.com/news/articles/2014-07-01/renewable-energy-s-expansion-exposing-grids-to-hacking.

[26] Christoph Steitz and Harro Ten Wolde, "Smart Meters Pose New Risks for Energy Industry," *Insurance Journal*, July 18, 2014, http://www.insurancejournal.com/news/international/2014/07/18/335214.htm.

[27] Ibid.

[28] Ibid.

[29] Paul Newton, "Security, security, security: the mantra for smart meter data," *UtilityWeek*, May 26, 2010, http://www.utilityweek.co.uk/news/Security-security-security-the-mantra-for-smart-meter-data/765952.

### *Supply Chains*

Supply chains are another potential vulnerability that affects old legacy systems as well as new Smart Grid hardware and software applications. Legacy systems are a particular concern because upgrades and repairs of equipment may not include installation of security upgrades. New procurement guidance for energy delivery systems focus on life cycle considerations by providing "baseline cybersecurity procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process."[30] Security of the supply chain for newer Smart Grid systems is a significant procurement concern because many components are obtained from many sources and vendors internationally. These sources may be considered targets of opportunity to compromise or counterfeit Smart Grid components. [31]

> Supply chain best practices in security and resilience need to be benchmarked and shared with the power sector. These practices need to be explored and explained in dialogues between IT and supply chain professionals, and between utilities and their suppliers.[32]

# The Grid Is Experiencing Cyber Intrusions

The increasing frequency of cyber intrusions on industrial control systems of critical infrastructure is a trend of concern to the electric utility industry. The National Security Agency reported that it has seen intrusions into IC systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[33] These intrusions, while they have not manifested in cyberattacks capable of inhibiting or disrupting electric system operations, still have reportedly occurred with CIP mandatory standards in place. Some have asserted that consensus-based standards are not strong enough, or are not developed quickly enough, to address cybersecurity needs, while others believe the cost of meeting the standards goes beyond the perceived risks.[34]

The following paragraphs describe several recently reported incidents of cyber intrusions and examples of malware[35] found on IC systems that are commonly used to control energy flows on the electric grid.

---

[30] Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014, http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

[31] Debra van Opstal, *Supply Chain Solutions for Smart Grid Security: Best Practices*, U.S. Resilience Project, 2012, https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SupplyChain-Solutions-for-Smart-Grid-Security.pdf.

[32] Ibid.

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

[34] Peter Behr, "As Smart Grid Expands, So Does Vulnerability to Cyber Attacks," *New York Times*, November 19, 2009, http://www.nytimes.com/cwire/2009/11/19/19climatewire-as-smart-grid-expands-so-does-vulnerability-25941.html?pagewanted=all.

[35] Malware is a computer program intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system.

### *BlackEnergy*

In October 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced that several industrial control systems had been infected by a variant of a Trojan horse[36] malware program called BlackEnergy.[37] Originally designed for "nuisance spam[38] attacks," the software for BlackEnergy was first reported in 2007 and is designed to target critical energy infrastructure.[39]

BlackEnergy is a special concern for critical infrastructure companies because the software is being used in an Advanced Persistent Threat (APT)[40] form ostensibly to gather information.

> BlackEnergy specifically targets human machine interface ("HMI") software, which enables users to monitor and interact with industrial control systems such as heating, ventilation, and air conditioning systems through a dashboard or other type of graphical interface. HMI software is typically running 24/7, can be remotely accessed, and is rarely updated, thus making it a favorite target for opportunistic hackers.[41]

While no attempts to "damage, modify, or otherwise disrupt the victim systems' control processes were found," the ICS-CERT alert indicates that this APT variant of BlackEnergy is a special concern because it is a modular malware capable moving through network files onto removable storage media.

> [T]ypical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.[42]

Hackers are reported to have used the BlackEnergy Trojan horse to deliver plug-in modules used for several purposes, including keylogging, audio recording, and grabbing screenshots. Researchers looking at the BlackEnergy malware are reported to have identified a plug-in that can destroy hard disks, and believe that the attackers will activate the module once they are discovered in order to hide their presence.[43]

---

[36] "The most dangerous malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a 'denial-of-service' (DDOS) attack." A denial-of-service attack is an attempt to make a machine or network resource unavailable to those attempting to reach it. See http://www.malwaretruth.com/the-list-of-malware-types/.

[37] See ICS-CERT alert at https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B. (Hereinafter ICSBlack).

[38] "Spam is unsolicited email, normally with an advertising content sent out as a mass mailing." See http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/.

[39] ICSBlack.

[40] "Advanced Persistent Threats (APTs) are a cybercrime category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached." See https://www.damballa.com/advanced-persistent-threats-a-brief-description/.

[41] Stephen Hsieh and Aravind Swaminathan, "BlackEnergy Malware Highlights Special Confidentiality Considerations in Critical Infrastructure Breach Investigations," *JD Supra*, November 18, 2014, http://www.jdsupra.com/legalnews/blackenergy-malware-highlights-special-c-97560/. (Hereinafter JDS).

[42] ICSBlack.

[43] JDS.

### *HAVEX*

The HAVEX malware is not new, but it has been modified several times since its first reported deployment. It has targeted the energy sector since "at least August 2012."[44] Originally, HAVEX was distributed via spam email or spear-phishing attacks.[45] This new version of HAVEX appears to have been designed as a Trojan horse specifically to infiltrate and modify "legitimate" software from ICS and SCADA suppliers, adding an instruction to run code (i.e., the "*mbcheck.dll*" file) containing the HAVEX malware.[46]

In the instance discovered, HAVEX malware was used as a remote access tool (RAT) to extract data from Outlook address books and ICS-related software files used for remote access from the infected computer to other industrial servers.[47] The cyberattack leaves the company's system in what appears to be a normal operating condition, but the attacker now has a backdoor to access and possibly control the company's ICS or SCADA operations.

The HAVEX malware possibly entered the control systems of targeted companies using one or multiple levels of attack:

1. Email Campaign: Executives and senior employees were targeted with malicious PDF attachments in February-June 2013.
2. Watering Hole Attack: Websites likely to be visited by people working in the energy sector were infected such that they redirected the site visitor to another compromised legitimate website hosting an exploit kit. The exploit kit then installs the RAT. This method of distribution began in June 2013.
3. Software Downloaded from ICS-Related Vendors: At least three ICS vendors' software downloads were hacked so that they included the RAT malware. [48]

HAVEX is also called "Backdoor.Oldrea" (or the "Energetic Bear RAT"), as it contains the malware known as "Kragany" or "Trojan.Kragany." HAVEX is a product of the Dragonfly group (aka Energetic Bear), which appears to be a "state-sponsored"[49] undertaking focused on espionage with sabotage as a "definite secondary capability."[50] The malware allows attackers to

[44] Crowdstrike, *Global Threat Report*, 2013, http://www.crowdstrike.com/new-crowdstrike-report-offers-unprecedented-insight-on-worlds-most-sophisticated-cyberattackers-3/.

[45] "Unlike regular phishing, which sends large numbers of emails to large numbers of people, spear-phishing refers to sending a phishing email to a particular person or relatively small group. Attackers may also heavily customize their spear-phishing emails, using public information gleaned from the Web, to make the emails seem more authentic." See http://www.darkreading.com/attacks-and-breaches/spear-phishing-attacks-on-the-rise/d/d-id/1098188.

[46] Daavid Hentunen and Antti Tikkanen, "Havex Hunts For ICS/SCADA Systems," *F-Secure*, June 23, 2014, https://www.f-secure.com/weblog/archives/00002718.html.

[47] Ibid

[48] Heather MacKenzie, "Dragonfly Malware Targets ICS Systems," *Tofino Security*, August 8, 2014, https://www.tofinosecurity.com/blog/dragonfly-malware-targets-ics-systems. (Hereinafter Dragonfly).

[49] "It is believed that the Dragonfly group is based in Eastern Europe, and that it is possibly being directed by Russia with state sponsorship involved." Ibid.

[50] Symantec, *"Emerging Threat: Dragonfly / Energetic Bear – APT Group*," July 30, 2014, http://fortunascorner.com/2014/07/01/massive-cyberattack-dragonfly-compromised-1k-power-plants-worldwide/.

upload and download files from the infected computer and run executable files. It was also reported to be capable of collecting passwords, taking screenshots and cataloguing documents.[51]

### *Sandworm*

Sandworm is a type of Trojan horse, and it was originally focused on a vulnerability in the Windows operating system (reported as patched by Microsoft in October 2014).[52] It was used to deliver malware through Powerpoint files on thumb drives using automatically run files, but that vector of attack has been largely closed.[53] The primary mode of Sandworm attack was spear-phishing, using grammatically well-written emails with topics of interest to the target. The malware contained an attachment that exploited the vulnerability to deliver variants of the BlackEnergy Trojan.[54]

The focus of the Sandworm attack discovered was SCADA systems, as the malware targeted specific software used for these systems.

> On October 14th, a report was publicly released regarding the Sandworm team. After beginning an investigation into the affiliated malware samples and domains, we quickly came to realization that this group is very likely targeting SCADA-centric victims who are using GE Intelligent Platform's CIMPLICITY HMI solution suite ... CIMPLICITY is an application suite that is used in conjunction with SCADA systems. A key component of any SCADA system is the HMI. The HMI (which stands for Human-Machine interface) can be viewed as an operator console that is used to monitor and control devices in an industrial environment.[55]

Sandworm can potentially have greater impacts on an enterprise, as the malware could be transferred to other corporate business systems.

> These devices can be responsible for automation control as well as safety operations... It is important to note that we are currently seeing CIMPLICITY being used as an attack vector; however, we have found no indication that this malware is manipulating any actual SCADA systems or data. Since HMIs are located in both the corporate and control networks, this attack could be used to target either network segment, or used to cross from the corporate to the control network.[56]

[51] Dragonfly.

[52] The attack relies on a vulnerability in Windows known as CVE-2014-4114, patched in Bulletin MS14-060.

[53] "[T]he attack used by Sandworm a so-called zero-day exploit, because the vulnerability was first exploited before a patch was available." Paul Ducklin, "The 'Sandworm' malware - what you need to know," *Sophos*, October 15, 2014, https://nakedsecurity.sophos.com/2014/10/15/the-sandworm-malware-what-you-need-to-know/.

[54] Adam Greenberg, "'Sandworm Team' exploits zero-day bug in espionage campaign," *SCMagazine*, October 14, 2015, http://www.scmagazine.com/sandworm-team-exploits-zero-day-bug-in-espionage-campaign/article/377238/.

[55] Kyle Wilhoit and Jim Gogolinski, "Sandworm to Blacken: The SCADA Connection," *TrendLabs Security Intelligence Blog*, October 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.

[56] Ibid.

# Mandatory Bulk Power Cybersecurity Standards

The bulk electric power system[57] has mandatory and enforceable standards for cybersecurity. The Energy Policy Act of 2005 (EPACT) (P.L. 109-58) gave the Federal Energy Regulatory Commission authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for critical infrastructure protection (CIP) which are updated considering the status of reliability and cybersecurity concerns for the grid.

FERC views grid security as a high priority, and separately established the Office of Energy Infrastructure Security (OEIS) to deal with cyber and physical security. OEIS has a mission to provide expertise to the Commission to "identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyberattacks and such physical threats as electromagnetic pulses."[58] However, FERC still asserts that it does not have the authority to act quickly in the event of a major cyber event.[59]

## Defining the Extent of FERC's Authority over Cybersecurity

NERC originally determined which electric industry facilities would be subject to mandatory reliability standards based on its definition of the term "bulk electric system" (BES). However, the regional bodies making up NERC had discretion in determining which facilities would be subject to these reliability standards under NERC's guidelines for the definition.

FERC has authority over wholesale power sales and the transmission of electricity in interstate commerce, and it is responsible for the reliability of the bulk electric system.[60] States regulate electric distribution systems.[61] FERC was concerned that certain facilities needed to ensure bulk

[57] 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.

[58] See http://www.ferc.gov/about/offices/oeis.asp.

[59] "However, as has been stated by FERC staff and members of the Commission in the past, the tools FERC currently has available to it are inadequate in the face of a fast moving or imminent [cyber]attack, and to the degree FERC does have authority it is limited to the bulk power system and not the myriad of other systems that interact with it. The FERC-NERC standard setting process does have the ability, over time, to create a security ecosystem that makes it much harder for cyber attacks to be successful. But that process is too slow and too open to deal with threats in real time." Federal Energy Regulatory Commission, *Written Testimony of Commissioner Tony Clark*, *Federal Energy Regulatory Commission, Before the Committee on Energy and Commerce Subcommittee on Energy and Power United States House of Representatives Hearing on FERC Perspective: Questions Concerning EPA's Proposed Clean Power Plan and other Grid Reliability Challenges Reliability Challenges*, July 29, 2014, http://www.ferc.gov/CalendarFiles/20140729091839-Clark-07-29-2014.pdf.

[60] See "What FERC Does" at http://www.ferc.gov/about/ferc-does.asp.

[61] "[T]he NERC-CIP framework has important limitations. First, NERC-CIP primarily covers only generation and transmission assets that qualify as 'critical assets' or 'critical cyber-assets.' With grid modernization, this identification is becoming increasingly problematic as many assets, such as advanced meters, do not fall under NERC-CIP but can have a major impact on grid reliability, safety and customer privacy. Estimates range from 80 percent to over 90 percent of grid assets are outside NERC-CIP's scope today. Second, NERC-CIP is primarily a compliance-based policy.

Compliance is an important component of addressing cybersecurity, but it is not enough to ensure that the rapidly (continued...)

power system reliability were not being considered under NERC's definition of the bulk electric system. FERC acknowledged that EPACT 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.[62] However, while that definition excluded facilities in Alaska and Hawaii, it also excluded virtually the entire grid in cities with large distribution systems like New York City.

In 2010, FERC directed NERC to develop uniform criteria for determining which facilities were necessary for the operation of the "interconnected transmission network," with the intention of including all such systems under NERC's CIP regulations. FERC approved NERC's revised criteria and new definition of the BES in 2012.[63] 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[64] and reactive power[65] resources connected at 100 kV or higher. This definition does not include facilities used in the local distribution of electric energy.

The revised definition of the BES allowed the potential inclusion of some facilities typically considered as distribution level, if they were seen as necessary for the operation of the interconnected transmission network. However, there are still many areas of potential access to the BES from the distribution system (which are not necessarily important to the operation of the transmission system), and thus beyond NERC's CIP regulations and FERC's reliability mandate. Because there are no mandatory standards of protection for distribution facilities below the bright-line threshold, these potentially "less protected" seams of the BES may provide a backdoor to cyber intrusions to the grid.[66]

## Toward a Focus on Security and Not Just Compliance

The current iteration of NERC's standards is CIP Version 5,[67] which appears to be moving utility companies toward an active consideration of system security needs rather than just compliance with the standards. It is largely the result of concerns that some owner/operators were not

(...continued)

evolving risks are adequately considered and acted upon effectively." Elizaveta Malashenko, Chris Villarrea, and J. David Erickson, *Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission*, California Public Utilities Commission, Grid Planning and Reliability Policy Paper, September 19, 2012, http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf.

[62] See FERC Order No. 693, FERC Stats. & Regs. 31,242 at page 77.

[63] See 139 FERC 61,247.

[64] 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.

[65] 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 megavolt-ampere reactive (MVAR)." See http://www.eia.gov/tools/glossary/index.cfm.

[66] "U.S: New Cybersecurity Organization to Defend Power Grid, March 5," *Israel Homeland Security*, March 5, 2014, http://i-hls.com/2014/03/u-s-new-cybersecurity-organization-defend-power-grid/?utm_source=rss&utm_medium=rss&utm_campaign=u-s-new-cybersecurity-organization-defend-power-grid.

[67] NERC CIP Version 5 goes into effect in July 2015. See http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx.

designating their bulk electric power facilities as "critical cyber assets," leaving potential "holes" in bulk electric power system cybersecurity.[68]

> The most notable change is the tiered impact rating system, which classifies bulk electric system (BES) Cyber Systems into High, Medium, and Low categories. This approach results in all cyber assets that could impact BES Facilities being in scope for the CIP standards ... Version 5's tiered classification brings all BES generating facilities into scope for at least some requirements. Cyber assets meeting certain criteria will be grouped into systems and assigned a High, Medium, or Low impact rating based upon the characteristics of the facility they support. For example, BES Cyber Systems at plants larger than 1,500 MW may receive a Medium impact rating, while most black-start units will be Low impact. All such systems, referred to officially as BES Cyber Systems, will be assigned at least a Low impact rating and will be required to comply with at least a portion of the requirements.[69]

CIP Version 5 therefore establishes new criteria and requirements for bulk electric system (BES) Cyber Systems,[70] mandating compliance but requiring owner/operators of bulk electric systems to focus on improving the security of critical assets. BES assets, once categorized as low or high impact, must be protected according to the level of requirements for that impact category. Among other factors, CIP Version 5 now requires 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 impacts on the BES; monitoring and control of remote access Internet connections (with inclusion of serial connections); multiple-factor authentication (rather than a simple 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. [71, 72]

Among the concerns raised with the implementation of CIP Version 5 is the potentially high cost.[73] With the new BES designation, all facilities (whether these are low, medium, or high risk) will be covered by some level of the new requirements. Many of these facilities may not have been designated cyber assets before, so the costs of compliance likely will increase.

[68] "[A] wide range of assets were excluded simply by avoiding the use of routable communication protocols. The result was that a broad swath of generation facilities had virtually no compliance obligations under the CIP standards." Steven Parker, "Introduction to NERC CIP Version 5," *POWER Magazine*, June 1, 2014, http://www.powermag.com/introduction-to-nerc-cip-version-5/. (Hereinafter POWERC5).

[69] Ibid.

[70] BES replaces "cyber assets" and "critical cyber assets" in NERC CIP terminology.

[71] POWERC5.

[72] "NERC CIP Version 5: One Giant Leap," *The State of Security Newsletter,* June 30, 2015, http://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip-version-5-one-giant-leap/.

[73] Celia David and Ken Lotterhos, *Transition to NERC CIP Version 5: The Bumpy Road Ahead*, Navigant Consulting, March 2014, http://www.navigant.com/~/media/WWW/Site/Insights/Energy/EN_TransitionToNERCCIPVersion5_TL_0314.ashx.

# Government and Industry Cooperation on Grid Cybersecurity

Cooperation between the federal government and the electric power sector now extends beyond mandatory and enforceable industry standards for the bulk electric system. However, such cooperation has not always been typical. Companies apparently were not aware of other government efforts. Reports began to emerge in 2010 that the federal government has been developing the capability to detect cyber intrusions on private critical infrastructure company networks. The program dubbed *Perfect Citizen* reportedly was designed to detect cyber intrusions using sensors in computer networks that would be activated by "unusual activity."[74]

While a number of voluntary structures now exist for information sharing and cybersecurity strategies, the degree of adoption by electric utilities and the overall effectiveness of these programs is unknown. The FY2016 budget proposes $14 billion in cybersecurity funding for "critical initiatives and research" across the federal government.[75]

Several of the key organizations and their missions with regard to electric power sector cybersecurity are profiled below.

## Department of Energy

The Department of Energy (DOE) is home to a number of voluntary initiatives and programs for electric sector cybersecurity, with the Office of Electricity Delivery and Energy Reliability (OE) having the lead role. DOE considers the security and resilience of the electric sector to be paramount " ... since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services."[76] Several of these programs are described below.

### *National Electric Sector Cybersecurity Organization (NESCO)*

In 2009, under the FY2010 Energy and Water Appropriations Act (P.L. 111-85), Congress directed DOE to form a national organization which would serve as the National Electric Sector Cybersecurity Organization resource.

> ...[T]he Secretary shall establish an independent national energy sector cyber security organization to institute research, development and deployment priorities, including policies and protocol to ensure the effective deployment of tested and validated technology and software

[74] Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," *Wall Street Journal*, July 8, 2010, http://www.wsj.com/articles/SB10001424052748704545004575352983850463108.

[75] The budget proposes $149 million for current federal programs focused on improving the cybersecurity of private sector partners of government programs. It includes another $243 million to support research and development at civilian agencies for innovative cybersecurity technologies. See White House, "Middle Class Economics: Cybersecurity," *The President's Budget FY2016* , 2015, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity.pdf.

[76] DOE, Office of Electricity Delivery and Energy Reliability, *Cybersecurity*, 2015, http://energy.gov/oe/services/cybersecurity.

controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid.[77]

DOE selected two organizations to form the National Electric Sector Cybersecurity Organization (NESCO): EnergySec and the Electric Power Research Institute (EPRI).[78] EnergySec provides support for "information sharing, professional development and collaborative programs and projects that improve the cyber security posture of all participating organizations." EPRI serves as the research and analysis resource for NESCO. NESCO's mission is to improve the "cybersecurity posture of the electric sector by establishing a broad-based public-private partnership for collaboration and cooperation" by providing a forum for cybersecurity experts, developers, and systems users. [79]

### *Electricity Subsector Cybersecurity Capability Maturity Model*

The Cybersecurity Capability Maturity Model (C2M2) was developed by DOE-OE, the Department of Homeland Security (DHS), and industry as a self-evaluation survey tool for any organization to address cybersecurity vulnerabilities. The C2M2 asks users to assess cybersecurity control implementation across 10 areas of cybersecurity "best practices" based on an evaluation of the maturity of a specific cybersecurity function.[80] The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) goes one step further, specifically tailoring the core C2M2 survey for the electricity subsector with a "maturity model, an evaluation tool, and DOE facilitated self-evaluations."[81]

Additionally, in 2006, DOE released a report titled *Roadmap to Secure Control Systems in the Energy Sector*. It outlined a strategic framework to be developed by industry, vendors, academia and government stakeholders to "design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber-incident while sustaining critical functions." The plan called for a 10-year implementation timeline focusing on barriers and recommended strategies for achieving effective grid cybersecurity. A five-year update released in 2011 highlighted what had been achieved to date, discussing ongoing efforts with respect to short- to long-term goals.[82]

## Department of Homeland Security

DHS has a broad mission to make the United States safe and resilient against terrorism and other potential threats.[83] The cyber and physical security of the grid are encompassed in this mission, and DHS has several initiatives in pursuit of these goals.

---

[77] P.L. 111-85. See Title III, DOE Energy Programs.

[78] See http://energy.gov/oe/services/cybersecurity/nesco.

[79] See http://www.energysec.org/services/advisory-services/.

[80] See http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program.

[81] See "Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1" at http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

[82] The update discussed roadmaps for improving areas such as intrusion detection and development of metrics for measuring security improvements. See U.S. Department of Energy, Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

[83] DHS was established by the Homeland Security Act of 2002 (P.L. 107-296).

## National Protection and Programs Directorate

The National Protection and Programs Directorate (NPPD) coordinates national efforts to protect critical infrastructure, working with partners "at all levels of government, and from the private and non-profit sectors" to share information to make critical infrastructure more secure. Under NPPD are several offices focused on cybersecurity, critical infrastructure protection, and resiliency:[84]

- The Office of Cyber and Infrastructure Analysis (OCIA) uses information received from public and private sources to conduct consequence modeling, simulation, and analysis to inform cyber and physical security risk management for U.S. critical infrastructure.
- The Office of Infrastructure Protection (IP) helps critical infrastructure owners and operators to understand and address risks to critical infrastructure. The office provides tools and training to critical infrastructure owners to help them manage risks to their assets, systems, and networks.
- The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. A major priority of the office is the reduction of cyber risks to federal and private Internet domains from terrorist attacks, natural disasters, or other emergencies. CS&C is also the home of the National Cybersecurity and Communications Integration Center (NCCIC).

NCCIC is focused on "cyber situational awareness, incident response, and management."[85] NCCIC acts as an information sharing forum for the public and private to improve understanding of cybersecurity and communications vulnerabilities and incidents, and mitigation and recovery from cyber events. NCCIC's mission is to reduce the likelihood and severity of incidents that may "significantly compromise the security and resilience of the Nation's critical information technology and communications networks."[86]

> 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.[87]

Two critical branches of NCCIC with functions important to electric grid cybersecurity are the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

[84] DHS, "About the National Protection and Programs Directorate - Divisions," http://www.dhs.gov/about-national-protection-and-programs-directorate.

[85] DHS, "About the National Cybersecurity and Communications Integration Center," November 4, 2014, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center. (Hereinafter NCCIC).

[86] Ibid.

[87] Ibid.

> US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.[88]
>
> ICS-CERT reduces risk to the nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for Critical Infrastructure and Key Resources stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.[89]

US-CERT developed the Einstein 2 intrusion detection system used by the National Cybersecurity Protection System (NCPS).

> NCPS intrusion detection capabilities alert DHS to the presence of malicious or potentially harmful computer network activity transiting to and from participating in federal executive branch civilian agencies' information technology networks. This capability is deployed via EINSTEIN 2 and provides for improved detection and notification capabilities to provide near real time response to cyber threats.[90]

ICS-CERT coordinates responses to control systems-related security incidents and facilitates information sharing[91] among federal, state, and local agencies and organizations; the intelligence community; and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

## Science and Technology Directorate

The Science and Technology Directorate (S&T) was created to provide science and technology in support of DHS's mission. Since DHS assists in efforts for the security and resiliency of the grid, the Smart Grid with characteristics of self-healing from power disturbance events, and operating resiliently against physical and cyber threats is of particular interest.[92]

S&T also has a Cyber Security Division whose mission is to enhance the security and resilience of the nation's critical information infrastructure and the Internet by[93]

[88] See https://www.us-cert.gov/.

[89] See https://ics-cert.us-cert.gov/.

[90] See DHS, *National Cybersecurity Protection System*, Detection, April 2, 2014, http://www.dhs.gov/national-cybersecurity-protection-system-ncps.

[91] See CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, by Andrew Nolan.

[92] See http://www.dhs.gov/science-and-technology.

[93] See http://www.dhs.gov/science-and-technology/cyber-security-division.

1. developing and delivering new technologies, tools and techniques to enable the United States to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks;
2. conducting and supporting technology transition; and
3. leading and coordinating cybersecurity research and development for department customers, and with government agencies, the private sector and international partners.

Since recovery from cyberattacks is seen as a part of S&T's resiliency focus, S&T is working on several electric power sector specific initiatives. These include the *Resilient Electric Grid* (an effort to "keep the lights on" in the event of a power outage by enabling distribution level power substations to share power with one another), and the *Recovery Transformer* (a program developing a prototype large power transformer to enable a quicker recovery [i.e., within days instead of months or years] from an event which might damage key transformers).[94] S&T is currently managing an effort to assess the state of the Smart Grid concept, as well as specific technologies needed to achieve goals of ensuring Smart Grid security and resiliency.[95]

## National Institute of Standards and Technology

The Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140) defined attributes of a Smart Grid and plans for its development. EISA also gave the National Institute of Standards and Technology (NIST) the role of coordinating the development of a framework to enable the development of the Smart Grid in a safe and secure manner. Because cybersecurity threats were perceived as "diverse and evolving," NIST advocated a defense-in-depth strategy with multiple levels of security and asserted no single security measure could counter all types of threats.[96] The key to NIST's suggested approach is the determination of risk (i.e., the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences) as quantified by the threat (e.g., event, actor or action with potential to do harm), the vulnerability (e.g., weakness in the system), and the consequences (e.g., physical impacts) to the system.[97]

NIST published its *Guidelines for Smart Grid Cybersecurity*[98] as a comprehensive, voluntary framework for organizations to use in developing effective cybersecurity strategies "tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities."

---

[94] DHS considers the development and testing of the recovery transformer to be a success. See U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *The DHS and DOE National Labs: Finding Efficiencies and Optimizing Outputs in Homeland Security Research and Development*, 112th Cong., 2nd sess., April 19, 2012, H. Hrg.112-84 (Washington: GPO, 2013), pp. 7-11. DOE is now looking at the need to develop a stockpile of transformers for use in an EMP event (See http://www.eenews.net/energywire/stories/1060014919).

[95] See http://www.dhs.gov/science-and-technology/about-st.

[96] National Institute of Standards and Technology, Smart Grid Interoperability Panel Cyber Security Working Group, Introduction to NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, September 2010, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf. (Hereinafter NISTIR).

[97] NISTIR, p. 9.

[98] NIST first published the report in 2010. The current version was released in September 2014 as NISTIR 7628 Revision 1. See http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.

According to NIST, deliberate attacks are not the only threat to Smart Grid cybersecurity.

> Smart grid cybersecurity must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. The Smart Grid Interoperability Panel (SGIP) Cybersecurity Committee (SGCC) ... is moving forward in FY14 to address the critical cybersecurity needs in the areas of Advanced Metering Infrastructure security requirements, cloud computing, supply chain, and privacy recommendations related to emerging standards. This project will provide foundational cybersecurity guidance, cybersecurity reviews of standards and requirements, outreach, and foster collaborations in the cross-cutting issue of cybersecurity in the smart grid.[99]

NIST established the Smart Grid Interoperability guidelines with a primary goal of developing a cybersecurity risk management strategy to enable secure "interoperability"[100] of technologies across different Smart Grid domains and components.

NIST was asked in 2013 by Presidential Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity,"[101] to lead the development of a "Cybersecurity Framework" to reduce cyber risks.[102] The framework was based on industry methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks, incorporating "voluntary consensus standards and industry best practices to the fullest extent possible." The first version of the Framework was released on February 12, 2014.[103] Sector-specific federal agencies (such as DOE) are to report annually to the President on the extent to which owners and operators of critical infrastructure at greatest risk are participating in the program.[104]

NIST also hosts the National Cybersecurity Center of Excellence, which is focused on getting better adoption of secure, commercially available cybersecurity technologies by both the public and private sectors.[105]

## North American Electric Reliability Corporation

NERC's Critical Infrastructure Protection Committee (CIPC) is responsible for its physical security and cybersecurity initiatives. CIPC consists of both NERC-appointed regional representatives and technical subject matter experts, and serves as an expert advisory panel to the

[99] NIST, *Cybersecurity for Smart Grid Systems*, January 24, 2014, http://www.nist.gov/el/smartgrid/cybersg.cfm.

[100] Interoperability can be defined as the capability of two or more networks, systems, devices, applications, or components to share and readily use information securely and effectively with little or no inconvenience to the user. GridWise Architecture Council, Interoperability Path Forward Whitepaper, November 30, 2005, http://www.gridwiseac.org/pdfs/interoperability_path_whitepaper_v1_0.pdf.

[101] See http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[102] CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

[103] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[104] See https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[105] See http://nccoe.nist.gov/.

NERC Board of Trustees. It has standing subcommittees in the areas of physical security and cybersecurity. The CIPC also oversees the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).[106]

### *Electricity Sector Information Sharing and Analysis Center (ES-ISAC)*

ES-ISAC seeks to establish situational awareness, incident management, coordination and communication capabilities within the electricity sector through timely information sharing. The ES-ISAC works with DOE and the Electricity Sector Coordinating Council (ESCC) to share critical information with the electricity sector, enhancing its ability to "prepare for and respond to cyber and physical threats, vulnerabilities and incidents."[107]

> The Electricity Sector Information Sharing and Analysis Center ... which was established in 1998 under Presidential Decision Directive 63 (President Bill Clinton), called for the establishment of an ISAC for each of the eight infrastructure industries deemed critical to our national economy and public well-being.[108]

NERC members who are "registered entities"[109] can report information regarding cyber incidents to ES-ISAC via a secure Internet exchange, and also receive information on threats.[110]

### *Electricity Sub-Sector Coordinating Council (ESCC)*

NERC also serves as the home to the Electricity Sub-Sector Coordinating Council which seeks to coordinate sector-wide, policy-related activities and initiatives including physical and cyber security infrastructure. [111] The ESCC represents the electricity sub-sector (as part of the Energy Critical Infrastructure sector)[112] under DHS's National Infrastructure Protection Plan (NIPP).[113] Among ESCC's duties[114] is the responsibility for explaining the electricity sector's "unique characteristics and operating model" as it relates to other NIPP critical infrastructures sectors.

---

[106] See http://www.nerc.com/comm/CIPC/Pages/default.aspx.

[107] See NERC, *ES-ISAC*, 2013, http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

[108] See https://www.esisac.com/SitePages/FAQ.aspx.

[109] NERC members must apply to ES-ISAC to become registered entities. "The ES-ISAC is reviewing its policy regarding integrating potential external parties and their expertise and capabilities with the ES-ISAC." See https://www.esisac.com/SitePages/FAQ.aspx.

[110] "All registered entities in the North American electricity sector may be participants in the ES-ISAC. Although the ISAC framework is a U.S. government construct, the ES-ISAC extends across all of NERC's territory, which includes both Canada and portions of Mexico.... Registered entities who are members of the ES-ISAC received private-level information on security threats, including alerts; remediation; various task forces; events calendars; and other security-specific resources." See https://www.esisac.com/SitePages/FAQ.aspx.

[111] See http://www.nerc.com/pa/CI/Pages/ESCC.aspx.

[112] The Energy Critical Infrastructure sector includes the electricity, petroleum, and natural gas subsectors. See http://www.dhs.gov/critical-infrastructure-sectors.

[113] See http://www.dhs.gov/national-infrastructure-protection-plan.

[114] NERC, *Electricity Sub-Sector Coordinating Council Charter*, August 16, 2012, http://www.nerc.com/comm/Other/Documents/Electricity%20Sub-Sector%20Coordinating%20Council%20ESCC/ESCC%20Charter.pdf.

## Edison Electric Institute

The Edison Electric Institute (EEI) as the trade association for investor-owned electric utilities has been involved with the formation of industry partnerships on cybersecurity issues with a number of federal agencies. Information sharing between public and private entities is an issue the industry considers critical in protecting the grid against cyber-threats.[115] The industry is involved in several information sharing efforts including the ES-ISAC, ESSC, and NCCIC.

# Evaluating and Improving Electricity Subsector Cybersecurity

As noted above, the bulk electric system has mandatory standards for critical infrastructure cybersecurity that NERC proposes, and FERC approves (or may modify and remand back to NERC). Industry compliance with these standards may be enough to prevent fines, but the question is whether existing mandatory standards result in a cybersecure grid. The grid has reportedly experienced intrusions to SCADA systems, which could possibly compromise systems operations. While the exact details and location have not been revealed, the cyberattacks demonstrate potential threats to grid reliability. Although some may believe the risks of a major cyberattack on the grid are small, FERC is obligated to consider CIP and cybersecurity as part of its reliability mandate. This section will summarize current concepts for evaluating and improving electricity subsector cybersecurity.

## NESCO Cybersecurity Failure Scenarios

In 2013, NESCO released the results of an analysis intended to help electric utilities plan for cybersecurity risks. The "Electric Sector Failure Scenarios and Impact Analyses"[116] report focuses on specific events in which the "failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or distribution of power." The report organizes the failure scenarios according to six categories, corresponding to the domains identified by the National Institute of Standards and Technology.[117]

1. Advanced Metering Infrastructure (AMI)[118]

[115] Edison Electric Institute, *Electric Power Industry Initiatives To Protect The Nation's Grid From Cyber Threats*, October 2014, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Cybersecurity%20Backgrounder.pdf.

[116] National Electric Sector Cybersecurity Organization ,Technical Working Group 1, *Electric Sector Failure Scenarios and Impact Analyses*, September 2013, http://assets.fiercemarkets.com/public/sites/energy/reports/300200-NESCORFailureScenariosA-9-13Final.pdf. (Hereinafter NESCFAIL).

[117] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Special Publication 1108, January, 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[118] Advanced Metering Infrastructure (AMI) is intended to "implement residential demand response and to serve as the chief mechanism for implementing dynamic pricing. It consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. AMI provides customers real-time (or near real-time) pricing of electricity, and it can help utilities achieve necessary load reductions." NESCFAIL.

2. Distributed Energy Resources (DER)[119]
3. Wide Area Monitoring, Protection, and Control (WAMPAC)[120]
4. Electric Transportation (ET)[121]
5. Demand Response (DR)[122]
6. Distribution Grid Management (DGM)[123]

A seventh, generic cross-cutting scenario was also identified which could impact any of these categories. The failure scenarios are "high-level" examples, so as not to present a cyberattacker with ideas on how to carry out an attack. The focus is on cybersecurity events, not other events which could potentially cause similar issues. Mitigations and options are suggested for the various scenarios, with a scheme for prioritization of solutions for securing control systems. The report was designed to "support risk assessment, policies, planning, procedures, procurement, training, tabletop exercises and security testing."[124]

**Figure 4** lists what NESCO considered as some of the top potential failure scenarios. NESCO teams ranked the scenarios, with the darker bands indicating the potential higher risk failures. A relatively large number of potential failures came from the WAMPAC domain, a significant number from AMI, and a moderate number came from the DGM domain. Few were selected from DER or DR, and none were selected from the ET domain.

[119] "DER systems are "cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution system. DER systems can be generators, storage devices, and even electric vehicles if their chargers are capable of managing the charging and discharging processes. Generally DER systems are small," but they are becoming prevalent in the distribution system (potentially there will be thousands if not millions of DER systems interconnected with the distribution system)." Ibid.

[120] "Wide Area Monitoring, Protection, and Control (WAMPAC) ... systems constitute a suite of different system solutions aimed at meeting various wide-area application requirements. WAMPAC systems often center around synchrophasor technology and the devices that generate, receive, and utilize this synchrophasor data. WAMPAC systems should be setup to include all components from the Phasor Measurement Unit (PMU) to the WAMPAC applications leveraging that data, including other intermediate devices such as the servers that manage the PMUs, devices that provide alignment services like Phasor Data Concentrators (PDCs), phasor gateways, phasor data stores, and other such components." Ibid.

[121] "Electric Transportation (ET) ... systems are setup to include components starting 'from the Electric Vehicle (EV) and the Electric Vehicle Supply Equipment (EVSE) to the EV Management Server hat communicates with the EVSEs. The EV may have an in-vehicle system that is connected to the battery through the vehicle's Car Area Network (CAN) that exchanges data with the EVSE via a wireless channel or PLC.… ET systems also include other intermediate devices. A meter measures power usage for each EVSE. A gateway collects data from the meters and the EVSEs and transmits the data to the EV Management Server.'" Ibid.

[122] "Demand Response (DR) communications cover interactions between wholesale markets and retail utilities and aggregators, as well as between these entities and the end-load customers who reduce demand in response to grid reliability or price signals. […] Price (often with the time that the price is effective), grid integrity signals (e.g., event levels of low, medium, high), and possibly environmental signals (e.g., air quality) are components of DR communications." Ibid.

[123] Distribution Grid Management (DGM) "focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system." Ibid.

[124] NESCFAIL.

**Figure 4. Draft List of Top Potential Failure Scenarios**

| | |
|---|---|
| AMI.1 | Authorized Employee Issues Invalid Mass Remote Disconnect |
| AMI.3 | Invalid Access Used to Install Malware Enabling Remote Internet Control |
| AMI.23 | Meter Authentication Credentials are Compromised and Posted on Internet |
| AMI.24 | Weak Encryption Exposes AMI Device Communication |
| AMI.25 | Known but Unpatched Vulnerability Exposes AMI Infrastructure |
| DER.1 | Inadequate Access Control of DER Systems Causes Electrocution |
| DER.16 | DER SCADA System Issues Invalid Commands |
| WAMPAC.1 | Denial of Service Attack Impairs NTP Service |
| WAMPAC.2 | Networking Equipment used to Spoof WAMPAC Messages |
| WAMPAC.3 | Improper PDC Configuration Interferes with Relay of Measurement Data |
| WAMPAC.4 | Measurement Data Compromised due to PDC Authentication Compromise |
| WAMPAC.5 | Improper Phasor Gateway Configuration Obscures Cascading Failures |
| WAMPAC.6 | Communications Compromised between PMUs and Control Center |
| DR.1 | Blocked DR Messages Result in Increased Prices or Outages |
| DR.4 | Improper DRAS Configuration Causes Inappropriate DR Messages |
| DGM.3 | Malicious Code Injected into Substation Equipment via Physical Access |
| DGM.5 | Remote Access used to Compromise DMS |
| DGM.13 | Poor Account Management Compromises DMS and Causes Power Loss |
| Generic.1 | Malicious and Non-malicious Insiders Pose Range of Threats |
| Generic.2 | Inadequate Network Segregation Enables Access for Threat Agents |
| Generic.3 | Portable Media Enables Access Despite Network Controls |

**Source:** Table 4. NESCO, *Electric Sector Failure Scenarios and Impact Analyses*. See http://assets.fiercemarkets.com/public/sites/energy/reports/300200-NESCORFailureScenariosA-9-13Final.pdf.

**Notes:** See *Electric Sector Failure Scenarios and Impact Analyses* for further descriptions of failure scenarios.

In the report, each failure scenario is accompanied by a descriptive example of an action causing the breach, the relevant vulnerabilities and impacts. A possible mitigation of the AMI.24 scenario above is shown in the example of **Figure 5**.

## *Integrating Electric Subsector Failure Assessments into a Risk Assessment Methodology*

Using the potential cybersecurity failure scenarios put forward by NESCO, DOE and EPRI issued a voluntary risk assessment process[125] for utilities to consider in developing and implementing a plan to manage risks from the six failure scenarios developed by NESCO. Utility strategies for framing, assessing, responding to, and monitoring risk on a continual basis are at the center of the process. NESCO's risk assessment approach is based on DOE's ES-C2M2 model, and risk management is focused on DOE's systems security approach[126] specific to risks from operating IT and IC systems.

[125] DOE, EPRI, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*, 3002001181, December 2013, http://energy.gov/sites/prod/files/2014/04/f14/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology.pdf.

[126] DOE, *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*, May 2012, http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

**Figure 5. Example of a NESCO Failure Scenario Path and Its Mitigation**

**AMI.24 Weak Cryptography Exposes AMI Device Communication**

**Description:** An AMI vendor implements weak cryptography that is easy to crack, allowing access to and modification of configuration or data on that interface.

**Relevant Vulnerabilities:**

- Implementation of weak or unapproved cryptography.

**Impact:**

- Cost to upgrade or to replace all devices, if upgrade is not feasible. This impact is expected whether or not a threat agent ever uses this vulnerability to launch an attack,
- Loss of customers' private information, and associated costs,
- Mass disconnect of meters potentially causing circuit breaker trips, resulting in temporary outages until power on the grid can be rebalanced.

**Potential Mitigations:**

- *Require approved cryptographic algorithms*,
- *Define procedure* in change and configuration management policies and procedures to allow future cryptographic changes,
- *Define procedure* to include security, including cryptography, in the purchasing process,
- *Perform security testing* of security controls during system acceptance testing.

**Source:** NESCO, *Electric Sector Failure Scenarios and Impact Analyses*. See http://assets.fiercemarkets.com/public/sites/energy/reports/300200-NESCORFailureScenariosA-9-13Final.pdf.

## Potential Mitigation of Cyber Threats

The electric power industry is mostly in a defensive mode regarding cybersecurity threats. One potential area of increasing importance is intrusion detection, since some reports state that cyber attackers may be on an enterprise's system for years before they are detected.[127]

Much of what is emerging from the collaborative efforts of government, industry and academia appears to be focused on changing the way the electric sector views and operates as an enterprise. Protection of the sector from deliberate disruption was not necessarily a high priority for most utilities, especially before Internet connectivity became common. Cyber and physical security are essential if the enterprise is to fulfil its function, and protection of critical infrastructure of the bulk electric system is a mandatory part of utility system operations.

[127] Paz Eshel, Bucky Moore, and Shiran Shalev, *Why Breach Detection Is Your New Must-Have, Cyber Security Tool*, TechCrunch, September 6, 2014, http://techcrunch.com/2014/09/06/why-breach-detection-ss-your-new-must-have-cyber-security-tool/.

Because many cybersecurity actions are reactive to the last threat discovered, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks. [128] Therefore, they suggest that higher-level cybersecurity postures are thus said to require looking beyond whether "something bad" is happening, and shifting to understanding who authored the malicious software and why.[129] Finding an answer to these issues means understanding the reason for the attack, and then the appropriate resources can be gathered in building an effective defense. The Financial Services Information Sharing and Analysis Center (FS-ISAC) reportedly uses a team of threat analysts who base cyberattack defenses on safeguarding what they think the attackers are after. FS-ISAC operates "a centralized threat repository and an automated network for rapid distribution of threat information from government and industry sources."[130] The ES-ISAC performs a similar function to the FS-ISAC for the electricity subsector, but is said not to match FS-ISAC in technical capabilities yet.

> The automated, machine-to-machine information exchange that currently exists at FS-ISAC enables a faster, finer-grained identification and analysis of suspected Internet addresses, malicious software code and other threat indicators than the ES-ISAC currently can achieve. That gives FS-ISAC the potential for advanced search and analysis capabilities, including greater insights into identities and methods of various actors. In other words, FS-ISAC has a great capability to "connect the dots" that reveal critical information about an attack and its authors, according to participants in the programs
>
> ...Adoption of faster, more automated threat processing technologies by the electric power sector's vendors may be the best hope of improving cybersecurity defenses among the hundreds of smaller utilities that can't afford in-house cyberdefense expertise.[131]

NCCIC expects to have such "machine-to-machine sharing of online threat data" capabilities available soon.[132]

### *Resilience and Recovery*

Renewable electricity in distributed generation[133] installations and microgrids[134] have the potential to resist disruptions to the grid, whether from natural occurrences or cyberattacks, by

[128] Peter Behr, "In fighting cyber crimes, experts call for focus on attackers, not attacks," *EnergyWire*, June 17, 2014, http://www.eenews.net/energywire/2014/06/17/stories/1060001405. (Hereinafter FOACS).

[129] Ibid.

[130] Ibid.

[131] Ibid.

[132] NPPD Under Secretary Suzanne Spaulding and NPPD Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck, *Hearing on Examining the President's Cybersecurity Information Sharing Proposal*, House Committee on Homeland Security, Building Capacity to Accelerate Automated Sharing of Cyber Threat Indicators, February 25, 2015, http://www.dhs.gov/news/2015/02/25/written-testimony-nppd-under-secretary-and-deputy-under-secretary-cybersecurity.

[133] DOE defines distributed generation as "electric generation that feeds into the distribution grid, rather than the bulk transmission grid, whether on the utility side of the meter, or on the customer side." Distributed generation encompasses a wide range of technologies including solar photovoltaic (PV) panels, combined heat and power systems, backup generators powered by a variety of fuels, small wind turbines, fuel cells, microturbines, and energy storage devices. DOE, *The Potential Benefits of Distributed Generation and Rate-Related Issues that May Impede Their Expansion*, February 2007, http://www.ferc.gov/legal/fed-sta/exp-study.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp_o=12,100000,0.

[134] "A microgrid is a localized grouping of electricity sources and loads that normally operates connected to and synchronous with the traditional centralized grid (macrogrid), but can disconnect and function autonomously as (continued...)

continuing to generate power if the grid is brought down.[135] Microgrids can be a partial solution to larger scale resilience as they are sized to meet the power needs of a local community or institution, and they may also be useful in a major cyber event as a staging point for power outage and recovery workers. But they are also another potential point of access to the grid by a cyberattacker.

The Department of Defense looked at how distributed generation can harden its capabilities to maintain its mission and functions in the case of a major cybersecurity event affecting the Grid. A project called the *Smart Power Infrastructure Demonstration for Energy Reliability and Security* (SPIDERS) program was undertaken to help secure military installations if grid power supplies are disrupted. [136] One of the goals of the SPIDERS project was to transition military bases from reliance on diesel generators for back-up purposes to other on-site renewable electricity technologies and hydrogen fuel cells. Thus, military facilities could function in the event of a major cyber event and serve as centers for recovery efforts.

### *Using Distributed Computing for Grid Security*

In 2013, NIST initiated the *SmartAmerica Challenge*[137] to address grid vulnerabilities with a focus on using novel approaches. Since the grid relies on control centers to manage power flows in each area of operation, if that control center's operations are disrupted, reductions in service quality or power outages may occur. One SmartAmerica effort is looking at how a distributed computing approach could make the grid more resilient against both physical and cyberattacks.

> Because having a single control center for each section of the grid creates a significant vulnerability threat, the NC State and UNC group within the Smart Energy [Cyber-Physical Systems] team is pursuing the idea of creating a distributed computing system that would disseminate monitoring and control functions across multiple virtual machines in a cloud computing network that overlays the grid.[138]

According to a researcher leading the effort, the advantage of using distributed computing methods is "that if one element of the computing system gets compromised, the other virtual

(...continued)

physical and/or economic conditions dictate." DOE, Berkeley Laboratory, "About Microgrids," 2015, https://building-microgrid.lbl.gov/about-microgrids.

[135] Smart inverters allow these systems to continue providing generated power to the connected host even if the grid is not operational.

[136] SPIDERS was led by Sandia National Laboratories, under a partnership between the Department of Defense and the Department of Energy that involves numerous other federal laboratories, agencies and military commands. Tina Casey , *In First Test, U.S. Military's SPIDERS Microgrid Uses 90% Renewable Energy*, CleanTechnica, February 12, 2013, http://cleantechnica.com/2013/02/12/u-s-militarys-new-spiders-renewable-energy-microgrid/.

[137] "The SmartAmerica Challenge brings together organizations with Cyber-Physical Systems (CPS) technology, programs, and test beds to demonstrate the potential to improve safety, sustainability, efficiency, mobility, and overall quality of life. Cyber-Physical Systems—sometimes referred to as the Internet of Things (IoT)—involves connecting devices and systems in diverse sectors like transportation, energy, manufacturing, and healthcare in fundamentally new ways." See http://www.nist.gov/el/smartamerica.cfm.

[138] Matt Shipman, "Researchers test distributed computing as defense against cyberattacks on power grids," PhysicsOrg, May 21, 2014, http://phys.org/news/2014-05-defense-cyberattacks-power-grids.html.

machines could step in to protect the system and coordinate their efforts to keep the Grid functioning."[139]

Preparation for recovery from a potential cyberattack requires consideration of the resiliency of the system. Cyber resiliency can be defined as "the coordinated set of enterprise wide activities designed to help organizations respond to and recover from a variety of cyber incidents, while reducing the cost, impact to business operations, and brand damage."[140] But for electric utilities, the overall goal is system reliability, and the expenditures that may be required to ensure that the grid is functional are just beginning to be understood.

> Responsible entities must protect High- and Medium-Impact BES Cyber Assets and BES Cyber Systems under the access restriction provisions of the CIP rules. In some cases, this may require significant investment, such as creating secure enclosures that meet access restriction requirements. Even where capital investment is not required, resources will be needed to implement and validate protective measures as well as to manage and monitor access and, in some cases, configuration.[141]

## Cybersecurity-Related Concerns of Electric Utilities

While mandatory and enforceable reliability standards exist for BES critical infrastructure protection, electric utilities are concerned about the potential for a major cybersecurity event to result in liability concerns that could have financial ramifications.

### *Liability from a Potential Major Cyber Event*

As businesses involved in a commercial enterprise, utilities are aware that they may be vulnerable from a liability standpoint. While adherence to mandatory standards provides a measure for a "standard of care," it may not be enough to protect companies from legal actions. The American Public Power Association (APPA) summarized the issue as follows:

> APPA is concerned that electric utilities may not be sufficiently protected from liability for negligence claims in failing to protect against such attacks even when they have taken every known precaution. Some states are considering legislation that could protect utilities from liability for cyber attacks, but no state or federal statutes currently exist to insulate electric utilities, including public power entities, from legal action in response to a cyber incident.... This and previous Congresses have considered legislation focusing on cybersecurity proposals which have included provisions that would grant liability protections to critical infrastructure owners and operators affected by cyber incident, but no such protections have been enacted into law.[142]

---

[139] Aranya Chakrabortty, an assistant professor of electrical engineering who is leading the project from NC State. Ibid.

[140] Deloitte Consulting, "From Cyber Incident Response to Cyber Resilience," *Wall Street Journal*, February 24, 2015. "Cyber resilience—the coordinated set of enterprise-wide activities designed to help organizations respond to and recover from a variety of cyber incidents, while reducing the cost, impact to business operations, and brand damage..."

[141] Celia David and Ken Lotterhos, *Transition to NERC CIP Version 5: The Bumpy Road Ahead*, Navigant Consulting, March 2014, http://www.navigant.com/~/media/WWW/Site/Insights/Energy/EN_TransitionToNERCCIPVersion5_TL_0314.ashx.

[142] American Public Power Association, *In Support of Appropriate Liability Protection for Electric Utilities Related to Cyber Attacks*, Resolution 14-08, June 17, 2014, http://publicpower.org/files/PDFs/Resolution%2014-08%20—%20Liability%20Protection%20for%20Utilities%20Related%20to%20Cyber%20Attacks%20—%20FINAL.pdf.

EEI also voiced its concern over liability protection, and additionally considered the potential for unexpected costs for utilities arising from a potential major cyber event.

> Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.[143]

Various federal, state and other jurisdictions may allow utility companies to recover costs of cyber and physical security investments. And, in the event of a major cyber or physical security attack, electric utilities also may seek recovery of these costs from their customers in a public utility commission rates filing.

### *Cybersecurity Insurance*

According to DHS, cybersecurity insurance is generally designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. DHS believes "a robust cybersecurity insurance market could help reduce the number of successful cyberattacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection." DHS goes on to state that many companies (including electric utilities) choose not to carry insurance policies, citing the perceived high cost of those policies and confusion about what they cover. [144]

> In recent years, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has brought together a diverse group of private and public sector stakeholders—including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists—to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.... An October 2012 workshop focused on the challenges facing the "first-party" market which covers direct losses to companies arising from cyber-related incidents—including cyber-related critical infrastructure loss.... Based on what it had learned, NPPD hosted an insurance industry working session in April 2014 to assess three areas where it appeared progress could lead to a more robust first-party market: the creation of an anonymized cyber incident data repository; enhanced cyber incident consequence analytics; and enterprise risk management evangelization.[145]

Some electric utilities companies view the likelihood of a major cyberattack as a potentially low risk event.[146] However, in the opinion of one insurance industry broker, "[a] major energy catastrophe—on the same scale as ... Exxon Valdez or Deepwater Horizon—could be caused by a

[143] Edison Electric Institute, *EEI Principles for Cybersecurity and Critical Infrastructure Protection*, September 9, 2010, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Principles.pdf.

[144] DHS, *Cybersecurity Insurance*, 2015, http://www.dhs.gov/publication/cybersecurity-insurance.

[145] Ibid.

[146] See Ron Brown, "Utilities can Prepare for Disasters More Efficiently," *Electric Light & Power*, July 17, 2013, http://www.elp.com/articles/powergrid_international/print/volume-18/issue-7/features/utilities-can-prepare-for-disasters-more-efficiently.html.

cyberattack, and, crucially, that cover for such a loss is generally not currently provided by the energy insurance market."[147]

Most insurance products available to utilities reportedly cover "relatively minor" occurrences such as data losses, or downtime caused by IT issues "but not major events like explosions at multiple facilities triggered remotely by hackers."[148] The lack of coverage is said to arise from a clause in the insurance agreements of a number of energy sector companies which specifically exclude damage caused by software, viruses or malicious computer code. The lack of coverage will likely continue as long as the exclusionary clause is in effect. However, the clause is reported to remain because cybersecurity "is not well-understood by the insurance industry, making it difficult to design comprehensive products."[149] Moreover, appraisers from the large insurance provider Lloyds of London are also reported to have found cybersecurity protection measures as "too weak" for a policy to be offered to power companies.[150]

# Issues

The electric utility industry is composed of many different companies of various sizes and various ownership and financial structures.[151] Many utilities seem at present to view the potential for a major cybersecurity event as a low probability concern and to want to balance cybersecurity efforts and expenditures with the perceived risks. NERC's CIP Version 5 seeks to address that thinking by shifting the focus of utilities to provide the necessary levels of security for BES assets with low, medium, or high system impacts. However, many other joint federal and industry cybersecurity activities are cooperative, with voluntary adoption of the measures and metrics developed. The effectiveness of strategies developed and the levels of adoption of recommendations may require congressional evaluation.

Even with mandatory standards, the six failure scenario domains identified by NESCO[152] illustrate the continuing potential vulnerability of the grid to cyber and physical attacks, or a combination of both. While improved cyber intrusion detection measures are a high priority, these are more likely to come from government-industry partnerships than from the utility industry's efforts alone. However, the advice of several initiatives and observers is essentially for electric utilities to embrace cybersecurity as part of their strategic business planning and operations.[153] Cyber intrusions of the grid are believed to be happening, which may be seen as an indication that

[147] "Energy Firms Unprotected for Major Cyber Events: Willis," *Insurance Journal*, April 15, 2014, http://www.insurancejournal.com/news/national/2014/04/15/325848.htm.

[148] Ibid.

[149] Ibid.

[150] Mark Ward, "Energy firm cyber-defence is 'too weak', insurers say," BBC, February 27, 2014, http://www.bbc.com/news/technology-26358042.

[151] As of 2007, there were 210 investor-owned electric utilities, 2,009 publicly owned electric utilities, 883 consumer-owned rural electric cooperatives, and 9 federal electric utilities. Energy Information Administration (EIA), "Electric Power Industry Overview," 2007, http://www.eia.doe.gov/electricity/page/prim2/toc2.html.

[152] See "NESCO Cybersecurity Failure Scenarios," above.

[153] For example, NERC CIP Version.5 requires BES owners to focus on improving security, not just compliance with standards, and the FS-ISAC focuses on what it perceives as "most valuable to attackers in order to understand where to build defenses." FOACS.

that more needs to be done by electric utilities to make the system secure. Whether electric utilities can make the investment financially (and recruit staff) for such a mission is also an issue.

The threats facing the grid are evolving, and with each new intrusion or cyberattack, priorities to protect the system can shift. But that does not mean previous attacks can be considered past issues. SCADA and other control systems infected by worms such as HAVEX are also vulnerable to other actors who may take advantage of such incursions, using or modifying them for their own purposes. This can be a particular concern if, for example, a worm originated from a nation-state. The threat of retaliation would likely be a deterrent from its use by a nation-state, but a terrorist or similar organization would likely be undeterred by such a consequence, and may use the worm for its own purposes. Given the potential for damage to the nation's economy from a major cyberattack on the grid, some might suggest a greater focus on recovery is needed and should become as much a part of a cybersecurity strategy as are efforts to secure the system.

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 only one of 16 critical infrastructure sectors identified by DHS. Given that the grid relies on several of the others (for example, for 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.

Additionally, FERC still asserts that it does not have the ability to react to a "fast moving or imminent" cyberattack. Congress may want to consider whether FERC should have more authority to deal with cybersecurity threats in real time.

Congress enacted provisions in EPACT giving the Federal Energy Regulatory Commission responsibility for the reliability of the grid. EPACT specifically restricted FERC from exercising its reliability authority over distribution systems. Even with the recent redefinition of the BES, there are many points to access the grid beyond those covered by CIP standards from which a potential cyberattack could be launched. Congress may want to consider whether further protection of the grid is necessary, especially along the seams between the newly revised BES and distribution systems beyond FERC's reliability authority. Such actions may include standards (voluntary or mandatory) or defined best practices for facilities connecting to the grid at, for example, a specified voltage level below the bright-line threshold of 120 kV.

Congress may want to consider ways to help companies deal with the costs of critical infrastructure protection. All BES designated facilities (whether these are low, medium or high risk) under CIP Version 5 will be covered by some level of the new requirements. Since the regulatory jurisdictions and financial structures of companies in the electric power industry can differ considerably, Congress may want to look at ways to lessen possible financial strains on electric utility systems with legitimate cost-compliance burden concerns.

Congress may also want to consider liability protection for electric utilities in the event of a major cyberattack. The coverage extended by insurance company products currently available may not extend to damage caused by a cyberattack.

# Selected Pending Legislation[154]

The following bills are related to cybersecurity issues presented in this report. While not specific to electric utilities, they address information sharing generally between federal and private sector companies. Electric utility companies would argue that the protections and two-way information sharing of the types proposed by these bills would likely promote disclosure of cyber incidents, thus potentially improving cybersecurity for all participants.[155]

**Table 1. Pending Legislation 114th Congress**

| Bill No. | Title | Committee(s) | Date Introduced | Latest Major Action | Date |
|---|---|---|---|---|---|
| H.R. 1731 | National Cybersecurity Protection Advancement Act of 2015 | Homeland Security | April 13, 2015 | Referred to the House Committee on Homeland Security | April 13, 2015 |
| H.R. 234 | Cyber Intelligence Sharing and Protection Act | Armed Services, Homeland Security, Intelligence (Permanent), Judiciary | January 8, 2015 | Referred to the Subcommittee on the Constitution and Civil Justice. | February 2, 2015 |
| H.R. 85 | Terrorism Prevention and Critical Infrastructure Protection Act of 2015 | Homeland Security | January 6, 2015 | Referred to Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. | January 23, 2015 |
| S. 456 | Cyber Threat Sharing Act of 2015 | Homeland Security and Governmental Affairs | February 11, 2015 | Referred to the Committee on Homeland Security and Governmental Affairs. | February 11, 2015 |

**Source:** Compiled by the Congressional Research Service from Congress.gov.

H.R. 1731 among other actions would amend the Homeland Security Act of 2002 (P.L. 107-296) to enhance multidirectional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections. The bill would allow for sharing of cyber threat indicators and other information related to cybersecurity risks and incidents with federal and nonfederal entities, including across sectors of critical infrastructure. The National Cybersecurity and Communications Integration Center (NCCIC) may enter into a voluntary information-sharing relationship with any consenting nonfederal entity for the purpose of sharing of cyber threat

[154] For further information on recently introduced bills addressing cybersecurity issues, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.

[155] For additional discussion of current and proposed cybersecurity legislation, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

indicators and defensive measures. A nonfederal entity, not including a state, local, or tribal government that shares cyber threat indicators or defensive measures through the NCCIC, shall be deemed to have voluntarily shared such information.

H.R. 234 among other actions would direct the federal government to provide for the real-time sharing of actionable, situational cyber threat information between all designated federal cyber operations centers to enable integrated actions to protect, prevent, mitigate, respond to, and recover from cyber incidents. The bill also would allow the federal intelligence community to share cyber threat intelligence with private-sector entities and utilities possessing appropriate certifications or security clearances.

H.R. 85 among other actions would direct DHS to (1) work with critical infrastructure owners and operators and other state and local authorities to take proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure against terrorist attacks; (2) establish terrorism prevention policy to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States; (3) establish a task force to conduct research into the best means to address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect critical infrastructure's interconnectedness and interdependency; (4) establish the Strategic Research Imperatives Program to lead DHS's federal civilian agency approach to strengthen critical infrastructure security and resilience; and (5) make available research findings and guidance to federal civilian agencies for the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure to assist in the prevention, mediation, and recovery from terrorism events. The bill also directs DHS to facilitate the timely exchange of terrorism threat and vulnerability information as well as information that allows for the development of a situational awareness capability for federal civilian agencies during terrorist incidents.

S. 456 among other actions would permit private entities to (1) disclose lawfully obtained cyber threat indicators to a private information sharing and analysis organization and the NCCIC; and (2) receive indicators disclosed by private entities, the federal government, or state or local governments. Liability protection would be given to entities that voluntarily share lawfully obtained indicators with NCCIC or a private information sharing and analysis organization if the organization self-certifies that it has adopted the best practices identified by the DHS-selected private entity.

## Author Contact Information

Richard J. Campbell
Specialist in Energy Policy
rcampbell@crs.loc.gov, 7-7905

## Acknowledgments

Amber Wilhelm contributed to the graphics in this report.