Cybersecurity for Energy Delivery Systems: DOE Programs

Updated August 28, 2017

Congressional Research Service
https://crsreports.congress.gov
R44939

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

While physical threats to the U.S. power grid and pipelines have long worried policymakers, cyber threats to the computer systems that operate this critical infrastructure are an increasing concern. Cybersecurity risks against the power and pipeline sectors are similar, as both use similar control systems, and there appears to be a broad consensus that cyber threats to this infrastructure are on the rise. Furthermore, with ever-greater physical interdependency between electricity generators and the natural gas pipelines that supply their fuel, many in Congress recognize that grid and pipeline cybersecurity are intertwined. In 2015, the Fixing America's Surface Transportation Act (the FAST Act) provided the Secretary of Energy with new authority to protect or restore the power grid during a grid security emergency, including a cyber incident. Congress is considering additional legislation to fund and expand the Department of Energy's cybersecurity programs.

The Department of Energy (DOE) is the lead agency for the protection of electric power, oil, and natural gas infrastructure—cooperating with the Department of Homeland Security, the lead agency for pipelines. DOE's cybersecurity activities are led by its Office of Electricity Delivery and Energy Reliability (OE) and structured around three areas: (1) cybersecurity preparedness, (2) cyber incident response and recovery, and (3) research, development, and demonstration. Although nominally applicable to energy delivery systems across the electric power, oil and natural gas, and pipeline sectors, OE's cybersecurity activities to date appear to have been focused primarily on the grid. Publicly available examples of DOE-supported activities specifically focused on pipeline cybersecurity are limited. Rather, pipeline cybersecurity efforts appear to be included as part of broader national cybersecurity efforts.

Several bills potentially affecting DOE's cybersecurity activities for power grid and pipeline infrastructure have been introduced in the 115th Congress. These include the Defense, Military Construction, Veterans Affairs, Legislative Branch, and Energy and Water Development National Security Appropriations Act, 2018 (H.R. 3219) and the Energy and Water Development and Related Agencies Appropriations Act, 2018 (S. 1609), both of which would modestly increase funding for OE in FY2018. The Energy and Natural Resources Act of 2017 (S. 1460) would establish and fund a DOE program for energy sector cybersecurity research, development, and demonstration (RD&D) to be carried out for advanced applications to identify and mitigate cyber vulnerabilities. The Enhancing State Energy Security Planning and Emergency Preparedness Act of 2017 (H.R. 3050) would authorize DOE to provide financial and technical assistance to states for assessing cybersecurity threats to energy infrastructure.

As federal cybersecurity oversight and legislative debate continue, Congress may focus on several key issues. Given the ever-changing cybersecurity environment in the energy sector, Congress may continue to examine OE's cybersecurity resources to ensure that they are adequate and being deployed appropriately to address the most important energy delivery risks. Congress may also seek a more-informed basis for considering whether to adjust the provisions of the FAST Act or clarify the authorizations it contains. How OE's programs and expertise could best be used to inform analysis of electric power and natural gas infrastructure interdependency from a cybersecurity perspective may also be of interest to Congress. Finally, Congress may examine how OE's cybersecurity activities fit in, and coordinate with, the other various roles in energy cybersecurity for electricity, oil and natural gas pipelines. In particular, Congress may examine how OE's RD&D programs and work with the National Labs in electric power sector cybersecurity supports federal and private sector efforts in pipeline cybersecurity.

Contents

Tables

Appendixes

Contacts

Introduction

The U.S. electric grid consists of over 700,000 miles of transmission lines and over 55,000 substations linking over 7,000 power plants to around 150 million customers.[1] Likewise, the U.S. energy pipeline network is composed of over 2.9 million miles of pipeline transporting natural gas, oil, and hazardous liquids; the natural gas transmission pipelines feed approximately 1,400 local distribution systems serving over 67 million customers.[2] These vast networks comprise the critical backbone of U.S. energy supply, supporting the vast majority of U.S. economic activity and playing a vital role in national defense. Consequently, the secure operation of both the power grid and pipelines are national priorities.

While physical threats to the U.S. power grid and pipelines have long worried policymakers, cyber threats to the computer systems that operate this critical infrastructure are an increasing concern. [3] Especially over the past decade, cyber threats against energy infrastructure have grown in frequency and severity. While most of these threats have been against the electric subsector, pipeline systems have also faced growing risk to their information communications technology. Both the Departments of Energy and Homeland Security have been directed to assess impacts of a cyberattack against the energy sector.[4] Furthermore, with ever greater physical interdependency between electricity generators and the natural gas pipelines which supply their fuel, many in Congress recognize that grid and pipeline cybersecurity are intertwined.[5]

The Department of Energy (DOE) is the lead agency for the protection of electric power, oil, and natural gas infrastructure—cooperating with the Department of Homeland Security (DHS), the lead agency for pipelines. DOE's energy sector cybersecurity activities are led primarily by its Office of Electricity Delivery and Energy Reliability (OE). In 2015, the Fixing America's Surface Transportation Act (the FAST Act) provided the Secretary of Energy with additional authority to order measures to protect or restore the reliability of the power grid during a grid security emergency, including "a malicious act using electronic communication."[6] The 115th Congress is considering additional legislation to fund and expand DOE's cybersecurity programs, including appropriations in the Defense, Military Construction, Veterans Affairs, Legislative Branch, and Energy and Water Development National Security Appropriations Act, 2018 (H.R. 3219) and the

[1] U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, p. 1-3.

[2] Pipeline and Hazardous Materials Safety Administration, "Annual Report Mileage Summary Statistics," web tables, July 11, 2107, https://www.phmsa.dot.gov/portal/site/PHMSA/menuitem.7c371785a639f2e55cf2031050248a0c/?vgnextoid=3b6c03347e4d8210VgnVCM1000001ecb7898RCRD&vgnextchannel=3b6c03347e4d8210VgnVCM1000001ecb7898RCRD&vgnextfmt=print.

[3] See, for example, U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Energy, *The Electricity Sector's Efforts to Respond to Cybersecurity Threats*, 115th Cong., 1st sess., February 1, 2017, Serial No. 115-3 (Washington: GPO, 2017), and the U.S. Senate Committee on Energy and Natural Resources, "Hearing to Examine Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats," hearing website, April 4, 2017, at https://www.energy.senate.gov/public/index.cfm/2017/4/the-purpose-of-the-hearing-is-to-examine-efforts-to-protect-u-s-energy-delivery-systems-from-cybersecurity-threats.

[4] The White House, "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, February, 12, 2013, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; and The White House, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," executive order 13800, May 11, 2017, at https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[5] Senator Maria Cantwell, Senate Committee on Energy and Natural Resources Nomination Hearing to Consider DOE, FERC Nominees, "Questions for the Record," May 25, 2017, question 12.

[6] P.L. 114-94 §61003.

Energy and Water Development and Related Agencies Appropriations Act, 2018 (S. 1609). The Energy and Natural Resources Act of 2017 (S. 1460) and the Enhancing State Energy Security Planning and Emergency Preparedness Act of 2017 (H.R. 3050) would authorize additional DOE funding for cybersecurity research and assistance to states, respectively.

This report examines the energy sector cybersecurity program administered by DOE's Office of Electricity Delivery and Energy Reliability as it applies to the electric power and pipelines subsectors.[7] The report summarizes risks to the computer-based control systems used in these subsectors, threats to those systems, and recent cyberattacks. The report reviews the legislative authorities and policy guidance that have directed OE's cybersecurity program and its activities, including its relationship to the national laboratories and other federal agencies with cybersecurity roles. The report concludes with a discussion of key policy issues for Congress.

Cybersecurity Risks

Federal security officials and industry analysts have long identified the grid and pipelines in the United States as potential targets for intentional disruption, although the nature and degree of cyber risk has been steadily evolving.[8] For example, a 2011 DHS pipeline threat assessment concluded that "terrorist groups have discussed attacks on unspecified [supervisory control and data acquisition] systems, but it is uncertain whether al-Qa'ida or any other group has the capability to conduct a successful cyberattack on these systems."[9] However, in 2016, the President of the Association of Oil Pipe Lines testified before a congressional committee that cybersecurity threats to pipelines were increasing and that "there is a great concern about … being prepared for cyber attacks" in the pipeline industry.[10] In January 2017, the DOE similarly concluded that "Cybersecurity is a particular concern for national and homeland security.… Malicious cyber activity against the electricity system and its suppliers is growing in sophistication."[11] While the threat of terrorist groups seeking to employ cyber tools against critical infrastructure persists, terrorist organizations have not yet demonstrated a capability to attack U.S. critical infrastructure in this manner.

Generally, the electricity grid and energy pipelines are under the same types of cybersecurity risks as other industries, such as financial services or transportation. However, different adversaries may choose to employ similar cyber tools to focus on different targets at different moments in time based on their unique motivations. Cybersecurity risks thus reflect both general threats to the energy sector as a whole and specific threats to industrial control systems as the focus of attack.

[7] Cybersecurity is also a concern for other critical energy infrastructure such as nuclear power plants and hydroelectric facilities, overseen by the Nuclear Regulatory Commission and the Department of Homeland Security, as well as refineries and oil and gas production and storage, overseen by the Department of Energy. These energy subsectors are outside the scope of this report.

[8] "Already Hard at Work on Security, Pipelines Told of Terrorist Threat," *Inside FERC*, McGraw-Hill Companies, January 3, 2002; Jennifer Alvey, "Cyber Security: A 'Virtual' Reality," *Public Utilities Fortnightly*, September 15, 2003.

[9] Transportation Security Administration, Office of Intelligence, *Pipeline Threat Assessment*, January 18, 2011, p. 3.

[10] Andrew Black, President and CEO, Association of Oil Pipe Lines, testimony before the House Committee on Homeland Security, Transportation and Protective Security Subcommittee hearing on Pipelines: Securing the Veins of the American Economy, April 19, 2016.

[11] U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, p. 1-32.

Industrial Control System Security Risks

Software-based industrial control systems (ICS) are used to monitor and control many aspects of network operation for railways, power grids, water and sewer systems, and pipeline networks. One category of ICS widely used in electric grid and pipelines networks—supervisory control and data acquisition (SCADA) systems—collect data (e.g., voltage, line pressure) in real time from sensors throughout a network, displaying those data to human operators in remote network control rooms. These operators can send computerized commands from SCADA workstations to control geographically dispersed equipment such as electric switches, pipeline valves, pumps, and many other network components. The SCADA system provides continuous feedback about conditions throughout the network, generating safety alarms when operating conditions fall outside prescribed levels.[12] Communications links may employ dedicated telephone landlines, wireless communications (satellite, microwave, and radio), cellular telephone service, Wi-Fi, and the Internet. As SCADA technology has matured, system control has become more intelligent and more automated, requiring less human intervention.[13]

Historically, SCADA systems employed highly customized proprietary software and were physically isolated from outside communications and computer networks. Because many of these systems were largely unique to a specific operator, it would have been difficult for malicious individuals outside the company to access a SCADA system and know what to do with it. However, due to advancements in computer technology and the ongoing development of communications and Internet-based control system applications, SCADA systems have become much more vulnerable to outside intrusion and manipulation.[14] Specific SCADA security weaknesses include the adoption of standardized control system technologies with known vulnerabilities, increased connection to external networks, insecure communication connections, and the public availability of sensitive information about control systems and infrastructure.[15]

Once accessible to a knowledgeable attacker, a SCADA system can be exploited in a number of specific ways to carry out a cyberattack:

- issuing unauthorized commands to control equipment;
- sending false information to a control-system operator that initiates inappropriate actions;
- disrupting control system operation by delaying or blocking the flow of information through the control network;
- making unauthorized changes to control system software to modify alarm thresholds or other configuration settings; and

[12] National Transportation Safety Board, *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines*, NTSB/SS-05/02, November 29, 2005, pp. 1-2.

[13] General Accounting Office (GAO), *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, March 2004, p. 11.

[14] Tobias Walk, "Cyber-Attack Protection for Pipeline SCADA Systems," *Pipelines International Digest*, January 2012, p. 6; Rose Tsang, Cyberthreats, "Vulnerabilities and Attacks on SCADA Networks," working paper, University of California, Goldman School of Public Policy, 2009, p. 2, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf.

[15] GAO, 2004, pp. 12-13; Eric Byres, "Next Generation Cyber Attacks Target Oil and Gas SCADA," *Pipeline & Gas Journal*, February 2012; Robert O'Harrow Jr., "Cyber Search Engine Exposes Vulnerabilities," *Washington Post*, June 3, 2012.

- rendering resources unavailable by propagating malicious software (e.g., a virus, worm, Trojan horse) through the control network.[16]

Depending upon the configuration of a particular system, such cyberattacks could potentially disrupt service, cause a hazardous release into the environment, or damage equipment. An example of the latter was a proof-of-concept attack hosted by the DHS in 2007 known at the Aurora Project. In this experiment, researchers working with DHS sent two sets of commands to a diesel-fueled electric generator. The first set of commands told the generator to repeatedly open and then rapidly close circuits in a manner that would cause failure. The second set of commands sent outputs to the operator-readable control panel that the generator was operating normally. The result was that the generator spun in such a manner that it destroyed itself without the operators knowing.[17]

Recently, reports of harmful software (malware) known as CrashOverride emerged as the latest example of destructive malware that can be used against the energy sector. CrashOverride reportedly includes capabilities allowing an attacker to disrupt ICS operations by opening and closing electric circuit breakers (degrading operations), denying access to communication ports on devices, and wiping modules to render devices inert. While there is no reported case of CrashOverride residing on U.S.-based systems, an updated version of the malware reportedly was used in a 2016 attack against the Ukrainian electric grid.[18]

Most of the cyberattacks that have been made public in the past few years have been against electricity generation and delivery infrastructure. However, in March 2012, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) within DHS identified an ongoing series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011. According to the agency, various pipeline companies described targeted spear-phishing[19] attempts and intrusions into multiple natural gas pipeline sector organizations that were "positively identified … as related to a single campaign."[20]

In 2010, the Stuxnet computer worm was first identified as a threat to industrial control systems. The Stuxnet software initially spreads indiscriminately, but the software includes a highly specialized industrial process component targeting specific Siemens industrial SCADA systems.[21] Furthermore, the capabilities demonstrated during the Aurora Project and the CrashOverride malware described above are also applicable against other ICS, including those for pipelines.

[16] Tobias Walk, 2012, pp. 7-8.

[17] Joe Weiss, "Chapter 6: Aurora Generator Test," in *Handbook of SCADA/Control Systems Security*, ed. Robert Radvanovsky and Jacob Brodsky, 2nd ed. (Boca Raton, FL: CRC Press, 2016), pp. 107-114.

[18] US-CERT, "CrashOverride Malware," Alert (TA17-163A), June 14, 2017, at https://www.us-cert.gov/ncas/alerts/TA17-163A.

[19] "Spear-phishing" involves sending official-looking emails to specific individuals to insert harmful software programs (malware) into protected computer systems; to gain unauthorized access to proprietary business information; or to access confidential data such as passwords, social security numbers, and private account numbers.

[20] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Gas Pipeline Cyber Intrusion Campaign," *ICS-CERT Monthly Monitor*, April 2012, p.1, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

[21] Tobias Walk, 2007, p. 7.

DOE's Authority in Energy Delivery Cybersecurity

DOE has authority and responsibilities for the cybersecurity of energy delivery systems from both presidential action memoranda and law. A chronologic perspective provides some insight on how energy security policy has evolved.

Federal Actions in Energy Infrastructure Cybersecurity

The Clinton Administration released Presidential Decision Directive 63 (PDD-63) in 1998.[22] For the first time in executive branch operations, PDD-63 established national policy for critical infrastructure protection from both physical and cyber threats. The directive discussed using a public-private partnership to reduce vulnerability to critical infrastructure from attacks, with lead federal agencies responsible for coordinating government efforts for specific sectors. PDD-63 established 15 critical infrastructure sectors and four special functions. DOE was assigned responsibility for (1) the electric power, and (2) the oil and natural gas production and storage sector.

The George W. Bush Administration built on the work of PDD-63, superseding it in 2003 with Homeland Security Presidential Directive 7 (HSPD-7) on "Critical Infrastructure Identification, Prioritization, and Protection."[23] HSPD-7 shifted the doctrine by removing "special functions" and expanding the sectors. In some cases, the expansion also included the addition of subsectors, as in transportation and energy. The transportation sector identified pipelines as a subsector; the energy sector identified an electric power subsector, and an oil and natural gas subsector. Lead agencies were replaced by Sector Specific Agencies (SSA), which had to collaborate with other federal agencies in a similar way as in PDD-63, but were also given responsibility for vulnerability assessments and assisting in risk management. In HSPD-7, DHS was named as the SSA for the transportation sector, including pipelines; DOE was assigned responsibility for the energy sector, as well as being the federal coordinator for all critical infrastructure protection efforts. In implementing HSPD-7, DHS pursued a risk-based approach to focus federal resources in areas of greatest risk, based on assessments as well as stakeholder (e.g., companies and state officials) input.

Congress passed legislation on the cybersecurity of energy delivery systems during the George W. Bush Administration with the Energy Policy Act of 2005 (EPACT).[24] EPACT included the Electricity Modernization Act of 2005, which directed the Federal Energy Regulatory Commission (FERC) to establish an "Electric Reliability Organization" (ERO, a role which the North American Electric Reliability Corporation [NERC] currently fulfills) to develop "reliability standards" for the "reliable operation" of the bulk power system.[25] The authority allowed for standards to address "cybersecurity protection" and also defined a "cybersecurity incident" as a unique incident which disrupted the "programmable electronic devices and communications networks ... essential to the reliable operations of the bulk power system."[26] FERC's authority under EPACT applies only to the bulk power system, and that authority is limited to review of the

[22] National Security Council and National Security Council Records Management Office, "PDD-63—Critical Infrastructure Protection," *Clinton Digital Library*, May 20, 1998.

[23] George W. Bush White House Archives, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive/HSPD-7, December 17, 2003.

[24] P.L. 109-58, enacted August 8, 2005.

[25] Ibid.

[26] Ibid.

ERO's standards. FERC cannot author standards independently, but can remand ERO-drafted standards back for reconsideration. While FERC also has regulatory authority over interstate natural gas pipelines under the Natural Gas Act (P.L. 75-688), its role is limited to siting and rate regulation, not safety or security.[27]

The Obama Administration superseded HSPD-7 with Presidential Policy Directive 21 (PPD-21) on "Critical Infrastructure Security and Resilience" in 2013.[28] "Resilience" was a term adopted in the Obama Administration as a way of recognizing that critical infrastructure is inherently vulnerable and will be disrupted at some point (historically, by severe weather, and potentially by an intentional attack), and that the infrastructure's degree of resilience will affect response time and eventual recovery. PPD-21 sought to further integrate cybersecurity as part of critical infrastructure protection by clarifying federal roles for security and resilience; establishing baseline information exchange requirements; and integrating analysis to inform planning, operations, and critical infrastructure decisions. PPD-21 retained the SSAs from HSPD-7, with DOE continuing as the SSA for the energy sector (electric power, and oil and natural gas). DHS was named the co-chair with the Department of Transportation (DOT) on the transportation sector and its subsectors, including pipelines.

Congress further legislated on energy sector cybersecurity in 2015 with the Fixing America's Surface Transportation Act (FAST Act).[29] Division F of the FAST Act on "Energy Security" included the designation of DOE as the SSA for cybersecurity for the energy sector. With this authority, DOE was directed to work with DHS in collaboration with electric infrastructure owners and operators for prioritization of activity, incident management, and vulnerability identification. While the law broadly states that DOE has a responsibility for the energy sector, the specific activities for collaboration refer only to the electricity subsector.[30]

The Trump Administration has not released a presidential memorandum superseding PPD-21, so that directive remains in effect. However, on May 11, 2017, the Administration issued Executive Order 13800 (E.O. 13800) on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[31] E.O. 13800 requires DOE and DHS to assess U.S. readiness to manage the consequences of a prolonged power outage as a result of a significant cyber incident. DOE also worked on a similar plan in accordance with a FAST Act directive on strategic transformer reserve options, although that plan is not focused on a specific type of threat, addressing the effects of any disruption on power delivery.[32]

Key Policy Guidance for Energy Delivery Cybersecurity

In addition to executive action and legislation, numerous federal policy documents over the last two decades from various presidential administrations have addressed cybersecurity for energy infrastructure. This policy guidance, together with the related presidential directives and

[27] FERC, "Gas Pipelines," August 1, 2017, https://www.ferc.gov/industries/gas/indus-act/pipelines.asp.

[28] Barack H. Obama White House Archives, "Critical Infrastructure Security and Resilience," Presidential Policy Directive-21, February 12, 2013.

[29] P.L. 114-94, enacted December 4, 2015.

[30] Ibid.

[31] The White House, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Executive Order 13800, May 11, 2017. For more details, see CRS Insight IN10707, *A Little Old, a Little New: The Cybersecurity Executive Order*, by Chris Jaikaran.

[32] U.S. Department of Energy, "Strategic Transformer Reserve," report to Congress, March 2017, at https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

executive orders discussed above, has resulted in DOE's energy delivery cybersecurity program in its current form. Key guidance documents over this period are briefly discussed below.

The comprehensive federal program for cybersecurity in energy delivery originated largely in 2000 under the *National Plan for Information Systems Protection*, which identified the electric power system and pipelines as critical infrastructure "that could be a target for significant cyber or physical attacks."[33] In particular, the plan stated

> The cyber nation of our infrastructures has created an intense reliance upon an underlying fabric of telecommunications and information networks. The infrastructures also rely heavily upon the Nation's energy production and distribution networks, especially through the I&C [information and communications] infrastructure's energy requirements.[34]

It is noteworthy that this passage refers broadly to "energy distribution networks," although I&C energy requirements imply an emphasis on reliable electricity supply. The plan reiterated DOE's role as the lead agency under PDD-63 for protection of electric power and oil and gas production and storage infrastructure, and DOT as the lead agency for pipelines.

In 2003, the *National Strategy to Secure Cyberspace* also identified the energy sector (electric power, oil and gas production, storage, and pipelines) as critical infrastructures dependent upon computer systems and vulnerable to cyber threats, reaffirming the lead agency roles under PPD-63. The strategy placed a particular emphasis on securing digital control systems (DCS) and SCADA, which are particularly important in the electric power and pipeline sectors.[35] Due to the ubiquity of these systems, the strategy explicitly called for coordination among DHS, DOE, other concerned agencies, and private industry in addressing DCS and SCADA cybersecurity.[36]

In 2006, DOE and DHS released their jointly-developed *Roadmap to Secure Control Systems in the Energy Sector* to provide "a strategic framework for investment and action in industry and government."[37] The *Roadmap* stated that the agencies were collaborating on energy sector critical infrastructure protection—citing specifically "the U.S. electric grid and oil and gas pipeline networks."[38] The overarching energy sector vision stated in the *Roadmap* was as follows: "In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function."[39]

In 2011, the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* was published by the Energy Sector Control Systems Working Group (ESCSWG),[40] sponsored by DOE as an update to the 2006 *Roadmap*.[41] The infrastructure scope of the 2011 *Roadmap* encompassed the "electricity, oil, and natural gas sectors," specifically including the "production, transmission, distribution,

---

[33] The White House, *National Plan for Information Systems Protection*, February 2000, p. 22.

[34] Ibid., pp. 133-134.

[35] Department of Homeland Security, *National Strategy to Secure Cyberspace*, February 2003, p. 32.

[36] Ibid.

[37] Department of Energy and Department Homeland Security, *Roadmap to Secure Control Systems in the Energy Sector*, January 2006, p. 6.

[38] Ibid.

[39] Ibid., p. 15.

[40] The Energy Sector Control Systems Working Group included staff from DOE (Office of Electricity Delivery and Energy Reliability), DHS (Science and Technology Directorate, National Protection and Programs Directorate), Federal Energy Regulatory Commission (Office of Electric Reliability), and representatives from the electric power, pipeline, and refining industries.

[41] Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, 2011.

and delivery of energy to consumers."[42] The stated vision of the 2011 *Roadmap* includes a reference to resiliency similar to that of the 2006 report: "By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions."[43] This vision statement also is directed at "energy delivery systems" as a specific type of infrastructure. Appendix D of the *Roadmap* defines "energy delivery systems" as:

> A network of processes that produce, transfer, and distribute energy and the interconnected electronic and communication devices that monitor and control those processes. Energy delivery systems include control systems—the sensors and actuators that physically monitor and control the energy processes, the computer-based systems that analyze and store data, and the communication networks that interconnect the process and computer systems.[44]

The *Roadmap* includes under this umbrella: generation, transmission, and distribution in the electric power sector, and drilling, processing, refining, and pipelines in the oil and natural gas sector.[45]

Pipeline Cybersecurity at DOE

In 2015, DOE—in coordination with DHS—released its most recent *Energy Sector-Specific Plan* (SSP) "to help guide and integrate the sector's continuous effort to improve the security and resilience of its critical infrastructure."[46] The SSP places an "increased emphasis on the Energy- and cross-sector interdependency issues and the integration of cyber and physical security efforts."[47] Notably, the SSP defines the "Energy Sector" as:

> three interrelated segments or subsectors—electricity, oil, and natural gas—to include the production, refining, storage, and distribution of oil, gas, and electric power, except for hydroelectric and commercial nuclear power facilities and pipelines.[48]

This explicit exclusion of pipelines from the energy sector under the 2015 SSP appears to be a difference from the other DOE cybersecurity policy guidance discussed above. However, this divergence may be specific to the National Infrastructure Protection Plan (NIPP) under which the SSPs are derived, as pipelines are under the purview of the transportation sector in the NIPP. The SSP also states that DOE and DHS, as co-chairs of the Energy Government Coordinating Council, are engaged in the security and resilience efforts of "other" critical infrastructure sectors, including pipeline, maritime, chemical, and dams.[49] The SSP also states that DOE and DHS work together with Canadian agencies "to coordinate matters related to pipeline safety and security."[50] Based on these statements, the degree of DOE attention to pipeline cybersecurity is unclear but appears limited. Among the electricity subsector priorities stated in the SSP are "deploying proprietary government technologies on utility systems that enable machine-to-machine

[42] Ibid., p. 1.

[43] Ibid., p. 9.

[44] Ibid., p. 61.

[45] Ibid., pp. 61-66.

[46] Department of Energy, *Energy Sector-Specific Plan*, 2015, p. 1.

[47] Ibid.

[48] Ibid., p. 3.

[49] Ibid., p. 10.

[50] Ibid., p. 23.

information sharing and improved situational awareness of threats to the grid" and implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[51]

Other Cybersecurity Authorities

Along with the DOE, two other federal agencies play significant roles in cybersecurity for energy infrastructure. Both FERC and the Transportation Security Administration (TSA) have statutory authority to regulate cybersecurity for energy infrastructure under their relative jurisdictions, but they exercise it differently, due to different requirements underlying their respective authorities.

FERC's Bulk Power Cybersecurity Standards

The bulk electric power system[52] has mandatory and enforceable standards for cybersecurity. As stated earlier, EPACT gave FERC authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). The North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for critical infrastructure protection, which are updated based on the status of reliability and cybersecurity concerns for the grid. FERC views grid security as a high priority, having separately established the Office of Energy Infrastructure Security (OEIS) to deal with cyber and physical security. OEIS has a mission to provide expertise to FERC to "identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyberattacks and such physical threats as electromagnetic pulses."[53]

TSA Pipeline Security Authority

The federal program for U.S. pipeline security began under DOT immediately after the terror attacks of September 11, 2001. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established the Transportation Security Administration within the DOT, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). TSA was transferred to DHS, newly created under the Homeland Security Act of 2002 (P.L. 107-296). HSPD-7 maintained DHS as the lead agency for pipeline security, and instructed DOT to "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)." The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). Thus, TSA has primary responsibility and regulatory authority for the security of natural gas and hazardous liquid (e.g., oil, refined products, and carbon dioxide) pipelines in the United States.

Although DHS has regulatory authority for pipeline security, its activities to date have relied upon voluntary industry compliance with the agency's security guidance and best practice

[51] Ibid., p. 4.

[52] 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.

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

recommendations.[54] Cybersecurity is also an element of voluntary security standards developed by the pipeline industry.[55]

Department of Transportation

The Department of Transportation (DOT) regulates the safety of oil and natural gas pipelines under the Natural Gas Pipeline Safety Act of 1968 (P.L. 90-481) and the Hazardous Liquid Pipeline Act of 1979 (P.L. 96-129). DOT's federal pipeline safety program is administered by the Pipeline and Hazardous Materials Safety Administration (PHMSA). Although DOT regulates safety, some aspects of its regulations, such as facility access requirements, can be related to pipeline security. In particular, the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (P.L. 109-468) mandated new requirements for control room management—including human factors, response to SCADA alarms, and review of reportable incidents—which could have cybersecurity impacts.[56]

DOE's Energy Delivery Security Program

As noted above, the DOE's energy delivery cybersecurity activities are led by its Office of Electricity Delivery and Energy Reliability (OE) within the Office of the Under Secretary for Science and Energy. A 2008 OE report stated that "OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid."[57] According to the agency's website, a current "top priority" for OE is:

> to make the nation's electric power grid and oil and natural gas infrastructure resilient to cyber threats.… The vision of OE's cybersecurity program is that, by 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.[58]

This vision and the OE programs supporting it are intended to align closely with the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity*[59] with an apparent focus on electric power, as discussed below.

---

[54] Transportation Security Administration, *Pipeline Security Guidelines*, April 2011, and *Pipeline Security Smart Practice Observations*, September 19, 2011.

[55] The Interstate Natural Gas Association of America (INGAA), a trade association for gas pipeline companies, maintains its own extensive cybersecurity guidelines for natural gas pipeline control systems: INGAA, *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, Washington, DC, January 31, 2011. Likewise, the American Petroleum Institute (API), a trade association within the oil industry, maintains a standard for oil pipeline control system security: API, *Pipeline SCADA Security*, Second Edition, API Std. 1164, Washington, DC, June 2009.

[56] Department of Transportation, "Pipeline Safety: Control Room Management/Human Factors," 74 *Federal Register* 63310-63329, December 3, 2009.

[57] Department of Energy, Office of Electricity Delivery and Energy Reliability (Hereinafter OE), *National SCADA Test Bed Program, Multi-Year Plan FY2008-2013*, January 2008, p. 7.

[58] OE, "Cybersecurity for Critical Energy Infrastructure," June 6, 2017, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure. It is interesting to note that the OE's public communications also refer to its mission in the context "energy delivery control systems (EDS)" rather than "energy delivery systems," perhaps to clarify the agency's focus. See, for example, OE, "Cybersecurity for Energy Delivery Systems (CEDS) Peer Review to Be Held December 7-9, 2016," news release, November 10, 2016.

[59] DOE, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

OE Cybersecurity Program Structure

The OE's cybersecurity program for energy delivery systems is structured around three areas: (1) cybersecurity preparedness; (2) cyber incident response and recovery; and (3) research, development, and demonstration.[60]

Cybersecurity Preparedness

OE's activities in cybersecurity preparedness address situational awareness and information sharing (taken together) and risk analysis. For the former, OE works with energy sector companies "to better detect risks and mitigate them more rapidly by fostering industry assessment capabilities, developing operational threat analysis tools, and working with the intelligence community to better share actionable threat and intelligence information."[61] A key component of these efforts is co-funding the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership managed by the Electricity Information Sharing and Analysis Center (E-ISAC), to facilitate timely, two-way sharing of threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.[62] Another effort, OE's Cybersecurity for the Operational Technology Environment (CYOTE) pilot program, focuses on two-way data sharing and analysis for energy sector operational technology (OT).[63] OE also supports the National Association of Regulatory Utility Commissioners in producing its cyber security primer for state utility regulators.[64] With OE support, experts from national laboratories have trained over 2,300 employees from over 200 utilities in cybersecurity, including live test bed exercises.[65]

OE's risk activities seek to develop better cyber risk analysis tools, practices, and guidelines for energy sector infrastructure. To this end, OE has worked with industry to develop the Cybersecurity Capability Maturity Model (C2M2), which helps infrastructure operators evaluate their cybersecurity capabilities and prioritize improvements.[66] OE has released an initial version for the electricity sector, and a derivative version for the oil and natural gas sector.[67] The latter applies to "the exploration, gathering, production, processing, storage, and transportation of petroleum liquids and natural gas," including pipelines.[68] The C2M2 model has been used for over 40 self-assessments among electricity, oil, and natural gas companies since its release in

[60] U.S. Department of Energy, "Cybersecurity for Critical Energy Infrastructure," website, at https://energy.gov/oe/cybersecurity-critical-energy-infrastructure.

[61] OE, "Energy Sector Cybersecurity Preparedness," June 8, 2017, https://energy.gov/oe/energy-sector-cybersecurity-preparedness-0.

[62] Ibid.

[63] Operational technology (OT), commonly found in industries, such as water, oil and gas, and energy, consists of hardware and software systems for monitoring and controlling equipment and processes. OT includes supervisory control and data acquisition (SCADA) systems, among others, often collectively referred to as industrial control systems (ICS). See Derek R. Harp and Bengt Gregory-Brown, *IT/OT Convergence: Bridging the Divide*, NexDefense, white paper, 2014, https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

[64] National Association of Regulatory Utility Commissioners, *Cybersecurity: A Primer for State Utility Regulators*, Version 3.0, January 2017, https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

[65] Department of Energy, *Strategic Plan 2014-2018*, March 2014, p. 9.

[66] OE, "Energy Sector Cybersecurity Preparedness," June 8, 2017.

[67] OE, *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model*, Version 1.1, February 2014, https://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf.

[68] Ibid., p. 4.

2012.[69] In 2015, the agency also published guidance to help energy sector companies align their cyber risk management efforts with the NIST Cybersecurity Framework.[70] The NIST Framework is voluntary guidance (based on existing standards, guidelines, and practices) to reduce critical infrastructure cybersecurity risk.[71] Working with NIST and NERC, OE has also developed a cybersecurity Risk Management Process (RMP) guideline for the electricity sector "to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector."[72]

Cyber Incident Response and Recovery

In the event of a cyber incident, two documents outline the framework under which the federal government will respond. Presidential Policy Directive 41 (PPD-41) on "United States Cyber Incident Coordination" establishes the policy of concurrent lines of effort in response. [73] In these lines of effort, DHS leads asset response, which focuses on restoring the victim entity; the Federal Bureau of Investigation (FBI) leads threat response, which seeks to identify and respond to the culprit of the attack; and the Intelligence Community leads a supporting line of effort to assist DHS and the FBI with intelligence support.[74] PPD-41 provided the policy for the National Cyber Incident Response Plan (NCIRP) along with additional detail for how that response will work following incident response and emergency management doctrine in the National Response Framework.[75]

The NCIRP dictates that, in response to a cybersecurity incident, a Cyber Unified Coordination Group (Cyber UCG) will be established at the direction of the National Security Council to manage the incident and coordinate the delivery of federal resources and capabilities to victim entities. The Cyber UCG is a body consisting of federal, state and local, private sector, and other relevant parties with an appropriate role for the specific incident's response activities. The Cyber UCG is to form at DHS's National Cybersecurity and Communications Integration Center (NCCIC) and operate there or virtually, depending on the incident. In the event that such a significant cyber incident occurs in the energy sector, OE is likely to play a large role in the Cyber UCG, given its FAST Act authorities. However, CRS is not aware of any public record of a Cyber UCG standing up and operating for a cyber incident in the energy sector, so the concept of operations prescribed in the NCIRP appears still untested in real-world response.

---

[69] Department of Energy, March 2014, p. 9.

[70] OE, *Energy Sector Cybersecurity Framework Implementation Guidance*, January 2015.

[71] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014.

[72] "The authors recognize that risk management processes in an organization are not executed in a vacuum. Regulatory requirements already exist to include North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, Nuclear Regulatory Commission (NRC) requirements, and a host of other Federal and State requirements. These requirements serve an important role in ensuring reliability, resilience, public safety, individual privacy, and protection of critical infrastructure." OE, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012, p. 1.

[73] Barack H. Obama White House Archives, "United States Cyber Incident Coordination," Presidential Policy Directive–41. July 26, 2016, at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[74] The Intelligence Community is composed of 17 organizations across the Executive branch coordinated by the Director of National Intelligence. More information may be found at https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

[75] Department of Homeland Security, "National Cyber Incident Response Plan," plan, December 2016, at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

Specific to pipeline security, DOE works with TSA and PHMSA to monitor flows and throughput of pipelines and facilitate information sharing among the federal government and private sector entities.[76] This is in accordance with the "Pipeline Security and Incident Recovery Protocol Plan" which TSA drafted in response to the Implementing Recommendations of the 9/11 Commission Act of 2001. However, the plan is from 2010 and has not been updated to conform to PPD-41 or the NCIRP for cyber incidents.

Research, Development, and Demonstration

OE administers a cybersecurity research, development, and demonstration (RD&D) program aligned with the 2011 *Roadmap* "to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems."[77] One of the program's principal activities is co-funding selected RD&D projects with National Laboratories, universities, and industry partners. The agency has invested over $210 million since 2010 on 35 projects and other efforts related to cybersecurity tools and technology (see **Appendix**).[78] These projects span many aspects of cybersecurity, including control system hardening, monitoring, software maintenance, cyber incident response, and overall system design.[79] The OE-funded projects appear to be predominantly focused on electric power applications (based on the specific technologies involved, industry partners, or stated objectives) but a number of them could also involve oil, natural gas, or pipeline-specific applications.

In addition to the focused RD&D projects, OE funds the National SCADA Test Bed (NSTB) in partnership with Idaho National Laboratory, Sandia National Laboratories, and other national laboratories to address control system security challenges in the energy sector. Among other things, the NSTB offers testing and research facilities and advanced visualization and modeling tools in facilities that recreate real-world energy delivery control systems, infrastructures, and networks.[80] A key service of the NSTB has been the cyber security assessment of over 30 commercial SCADA systems in the electricity sector since 2003.[81] The NSTB's *FY2009 Work Plan* listed several pipeline operators among its technical advisors for specific projects, although pipeline company participation more recently is not reported.[82] OE is investing in an expansion of the power grid test bed at Idaho National Laboratory that is to increase its capabilities to support technology research, testing, and demonstration for electric transmission and substation cyber threats.[83] In cooperation with the DHS Science and Technology Directorate (S&T), OE also funds

[76] Transportation Security Administration, "Pipeline Security and Incident Recovery Protocol Plan," plan, March 2010, at https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf.

[77] OE, *Cybersecurity Research, Development and Demonstration (RD&D) for Energy Delivery Systems*, web page, June 13, 2017, https://energy.gov/oe/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems.

[78] Patricia Hoffman, Principal Deputy Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Department of Energy, testimony before the Senate Committee on Energy and Natural Resources hearing on Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats, April 4, 2017.

[79] DOE-funded national laboratories also participate in cybersecurity activities funded by other entities. One example is the Idaho National Laboratory's work on the California Energy Systems for the 21st Century (CES-21) Program, sponsored by the California Public Utilities Commission in partnership with California utilities.

[80] OE, January 2008.

[81] Department of Energy, March 2014, p. 9.

[82] OE, *DOE/OE National SCADA Test Bed Fiscal Year 2009 Work Plan*, July 31, 2009. Pipeline operators included El Paso Corporation, Alyeska Pipeline, and utilities with both electric and natural gas operations including Alliant Energy and NiSource.

[83] Andrew A. Bochman, Idaho National Laboratory, testimony before the Senate Committee on Energy and Natural

collaborative teams of academic institutions to develop and implement multidisciplinary cybersecurity tools and technologies to be shared with the energy sector through academic outreach. For example, the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) focuses on the trustworthy operation of low-level devices, communications, and data systems in the power grid.[84]

OE's Pipeline-Related Cyber Activities

Asset owners across the electricity, oil, natural gas, and pipeline sectors often have similar operational and network communication needs—in some cases using the same types of hardware and software systems (e.g., SCADA) to meet them. Thus, cybersecurity programs, tools, and technologies developed in one sector have potential applicability to the others. However, effectively transferring general cyber practices or technology across sectors typically requires consideration or adaptation of cyber capabilities to fit the distinctive needs of a particular sector—such as "smart grid" metering requirements in electric power, or providing real-time operating pressure data in refineries and pipelines. Such sector customization, in turn, usually involves program participation by asset owners in a given sector, and pilot projects or demonstration in sector-specific installations.

Industry representatives have asserted that natural gas pipeline companies "work closely" in cybersecurity with DOE as the Energy SSA, which "actively engages with government and industry partners to develop cybersecurity practices, tools, and guidelines that address relevant cybersecurity risks and threats."[85]

Although OE's cybersecurity focus appears to be primarily on the electric power sector, CRS is aware of some OE-funded projects with explicit pipeline sector participation in development or application. As noted above, OE modified a version of its C2M2 model specifically for use in oil, gas, and pipeline operations. The Safe Active Scanning for Energy Delivery Systems (SASEDS) project included the pipeline sector in its literature survey.[86] Pipeline companies have participated in certain SCADA projects at the NSTB. Other OE-funded projects (e.g., *Chess Master*, a research and development program to identify next generation cybersecurity tools) have been led by technology developers serving multiple energy delivery sectors or in collaboration with industry partners that own multiple types of assets (e.g., the San Diego Gas & Electric utility company). In such cases, new technology may be transferred from the electric sector to the oil and gas or pipeline sectors by the vendor as a commercial product or service, or could potentially be transferred from the electric side of a utility to its natural gas operations.[87] Because references to pipelines in the OE-related published material are few and anecdotal, CRS is unable to better determine the extent of such transfer to the pipeline sector.

Resources hearing on Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats, April 4, 2017.

[84] Department of Homeland Security, "Trustworthy Cyber Infrastructure for the Power Grid," June 18, 2017, https://www.dhs.gov/science-and-technology/csd-tcipg.

[85] Dave McCurdy, American Gas Association, testimony before the Senate Committee on Energy and Natural Resources hearing "Protecting the U.S Energy Delivery Systems from Cyber Threats," April 4, 2017, pp. 11-12.

[86] Jovana Helms et al., Lawrence Livermore National Laboratory, "Safe Active Scanning for Energy Delivery Systems," presentation at the Cybersecurity for Energy Delivery Systems Peer Review, December 7-9, 2016, p. 8, https://controlsystemsroadmap.pnnl.gov/Documents/LLNL_SASEDS_Peer_Review_2016.pdf.

[87] See, for example, Schweitzer Engineering Laboratories, Inc., "Oil, Gas, and Petroleum Industry Applications: Electric Power System Solutions," marketing materials, 2012, https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/Petroleum%20Ind_PF00157.pdf?v=20150812-085146.

Cybersecurity Collaboration with Other Agencies

As discussed above, FERC and TSA have statutory authority to regulate cybersecurity in the bulk power and pipeline systems, respectively. Although OE participates in some of the same high-level groups as these two agencies (e.g., Energy Sector Government Coordinating Council), there is little discussion in published materials as to what extent OE collaborates directly with FERC or TSA on specific cybersecurity RD&D programs in their respective infrastructure sectors.[88] OE's statement before FERC's 2016 Reliability Technical Conference does not mention RD&D collaboration, although it does discuss OE's leadership of electric grid emergency preparedness exercises, such as North American Electric Reliability Corporation's Grid Ex III.[89] OE also stated that it views grid reliability standards, including security standards, as "a topic that is not ultimately part of OE's portfolio, and is best addressed by NERC and FERC." [90]

Although OE collaborates with DHS S&T on grid cybersecurity, the ongoing level of cooperation between OE and TSA in the area of pipeline security is difficult to determine from published materials. In 2016 testimony before a congressional committee regarding its cybersecurity activities, a TSA official did not specifically mention working with DOE (although the official did mention coordination with FERC).[91] A 2014 presentation by TSA's pipeline security director mentioned coordination "with DHS and DOE to harmonize existing cybersecurity risk management programs" as well as TSA and DOE cooperative participation in security assessments of six cross-border pipelines.[92] A 2010 Government Accountability Office (GAO) report stated that TSA and DOE "worked closely on pipeline security issues, programs, and activities, such as efforts to enhance reliability and resiliency."[93] In 2007, GAO reported that the national laboratories coordinated activities funded through the DHS Control Systems Security Program with those funded by DOE through the NSTB, including vendor SCADA assessments and site assessments.[94] The report states that the DOE-funded assessments were in the electricity sector, but provides no further information about the DHS-funded ones.[95]

In 2016, DOT issued an Advisory Bulletin recommending that pipeline companies monitor their SCADA systems for abnormal operations, unauthorized access, or interference with safe operations. DOT stated that it had "coordinated with several components within DHS and the Department of Energy" on the bulletin.[96] CRS has not found more specific documentation of

[88] Department of Homeland Security, Energy Sector Government Coordinating Council Charter, updated November 2014, p. 2, https://www.dhs.gov/sites/default/files/publications/Energy-GCC-Charter-2014-508.pdf.

[89] Patricia Hoffman, Assistant Secretary for Electricity Delivery and Energy Reliability, Department of Energy, statement to the Federal Energy Regulatory Commission, Reliability Technical Conference, June 1, 2016.

[90] L. Devon Streit, Deputy Assistant Secretary for Infrastructure Security and Energy Restoration, Office of Electricity Delivery and Energy Reliability, Department of Energy, statement to the Federal Energy Regulatory Commission, Reliability Technical Conference, May 27, 2016, p. 5.

[91] Sonya Proctor, Transportation Security Administration, testimony before the United States House of Representatives Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications hearing on Pipelines: Securing the Veins of the American Economy, April 19, 2016.

[92] Jack Fox, Transportation Security Administration, *Pipeline Security: An Overview of TSA Programs*, slide presentation, May 5, 2014, http://c.ymcdn.com/sites/www.houstonpipeliners.net/resource/resmgr/meeting_presentations/pipeline_programs_-_may_8-20.pdf.

[93] Government Accountability Office, *Pipeline Security*, GAO-10-867, August 2010, p. 11.

[94] Government Accountability Office, *Critical Infrastructure Protection*, GAO-07-1036, September 2007, p. 44.

[95] Ibid., p. 45.

[96] Department of Transportation, "Pipeline Safety: Safeguarding and Securing Pipelines From Unauthorized Access," 81 *Federal Register* 89183-89184, December 9, 2016.

collaboration between OE and DOT. Although DOT administers its own pipeline safety RD&D program, its recent projects do not involve direct work in control systems, SCADA, or cybersecurity.[97]

Pending Legislation

On July 27, 2017, the House passed the Defense, Military Construction, Veterans Affairs, Legislative Branch, and Energy and Water Development National Security Appropriations Act, 2018 (H.R. 3219), providing appropriations for DOE for the fiscal year ending September 30, 2018. The bill would appropriate $218,500,000 for OE, available until expended, except for $27,500,000 to be available until September 30, 2019 for program direction (Title III). The corresponding Senate bill, the Energy and Water Development and Related Agencies Appropriations Act, 2018 (S. 1609), reported by the Committee on Appropriations on July 20, 2017, would appropriate $213,141,000 for OE, available until expended, except for $27,000,000 to be available until September 30, 2019 for program direction (Title III).

Cybersecurity of energy infrastructure is addressed in Title II of S. 1460, the Energy and Natural Resources Act of 2017. Although titled "Enhanced Grid Security," Section 2002 of the bill also addresses security for other energy infrastructure.

- It would establish a program for energy sector cybersecurity RD&D to be carried out by DOE, in consultation with other agencies, states, and the energy sector, for advanced applications to identify and mitigate cyber vulnerabilities. A key focus would be on the interdependencies of critical infrastructure sectors. The bill would authorize appropriations of $65 million for each fiscal year from FY2018 through FY2026 for the program.
- The cybersecurity of devices and third-party control systems in the supply chain would also be a central focus of the proposed RD&D efforts. The bill would authorize appropriations of $65 million for each fiscal year from FY2018 through FY2026 for the program.
- Additionally, S. 1460 would require DOE to provide operational support for a cyber-resilience program, to enhance and periodically test the emergency response capabilities of DOE and the Electricity Sector Information Sharing and Analysis Center and their ability to monitor the status of the energy sector. The bill would authorize appropriations of $10 million for each fiscal year from FY2018 through FY2026 for this program.
- DOE would also develop modeling and risk assessment tools for a cyber-resilience program to secure energy networks, including electric, natural gas, and oil exploration, transmission, and delivery. The bill would authorize appropriations of $10 million for each fiscal year from FY2018 through FY2026 for the development of tools to advance energy sector security risk management and resiliency from human threats and natural hazards (including electromagnetic pulse and geomagnetic disturbances) programs.

Under the provisions in S. 1460, the proposed programs would need to leverage existing programs and be consistent with goals of the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity* for developing a resilient energy sector infrastructure by 2020.

[97] Department of Transportation, Pipeline and Hazardous Materials Safety Administration, "Research & Development," web page, June 19, 2017, https://primis.phmsa.dot.gov/rd/.

On July 18, 2017, the House passed the Enhancing State Energy Security Planning and Emergency Preparedness Act of 2017 (H.R. 3050), which would authorize DOE to provide states $90 million in financial assistance annually through FY2022 to assess cybersecurity threats to energy infrastructure, among other possible uses of funding. The act would offer governors information and technical assistance in the development, implementation, or revision of a state energy security plan. Supporting such plans, especially with respect to cybersecurity, could fall under OE's purview.

Possible Issues for Congress

Several key issues related to OE's energy delivery cybersecurity program have been included in legislative proposals or have otherwise been the subject of congressional oversight and debate. These issues are summarized below.

OE Cybersecurity Funding

The Trump Administration's FY2018 budget request for OE appropriations was $123 million, approximately 41% less than the agency's estimated direct obligations of $208 million in FY2017.[98] Within OE, the budget request would fund Cybersecurity for Energy Delivery Systems at $42 million compared to an estimated $62 million in FY2017, a reduction of approximately 32%.[99] Given recent assertions by federal agencies (including DOE) and the private sector about an increase in energy sector cybersecurity risks, some analysts have expressed concern about this proposed reduction in OE's cybersecurity budget.[100]

As noted above, the House and Senate appropriations bills would fund OE at $218.5 million and $213.1 million, respectively, both an increase from FY2017 funding. If OE's appropriation is enacted above its current level, the agency presumably could continue its current cybersecurity program on its current trajectory—and potentially fund some additional cybersecurity activities if they emerge as agency priorities. Additional authorizations under S. 1460 and H.R. 3050, if enacted and funded, would significantly expand resources for DOE's energy delivery cybersecurity initiatives beyond historical levels. Given the ever-changing cybersecurity environment in the energy sector, Congress may continue to examine OE's cybersecurity resources to ensure that they are adequate and being deployed appropriately to address the most important energy delivery risks.

FAST Act Implementation

As discussed earlier, the FAST Act includes a variety of provisions concerning the general security of energy systems. These provisions include considerations for cyber as well as physical attacks and electromagnetic pulse attacks. The provisions include requirements for the Secretary of Energy to examine the strategic transformer reserve, coordinate energy sector security as the

[98] Office of Management and Budget, *Appendix, Budget of the U. S. Government, Fiscal Year 2018*, May 23, 2017, p. 383, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/doe.pdf.

[99] Ibid.

[100] Peter Behr and Rod Kuckro, "Trump Fiscal 2018 Plan Scrubs DOE of Obama-Era Priorities," *Energywire*, May 24, 2017.

SSA, and prepare for energy supply disruptions. Congress may consider how effectively DOE is implementing the law, and whether additional authorities or changes to the law may be needed.[101]

The FAST Act does not require the DOE Inspector General (IG), the Comptroller General, or another agency to review the implementation of DOE's authorities and its progress in carrying out the direction of Congress.[102] However, Congress may still oversee DOE's efforts by holding hearings, requiring new reports from the IG or Comptroller General, or requesting specific reports or information from the agency itself. With DOE-provided or independently provided information, Congress may have a more-informed basis for considering whether to adjust the provisions of the FAST Act or clarify, expand, or contract the authorizations it contains.

Gas-Electric Cyber Interdependency

The operational interdependency of the electric power and natural gas sectors, especially with respect to reliability and cybersecurity, has been a growing concern among many federal agencies, Members of Congress, and industry groups. The second installment of DOE's Quadrennial Energy Review (QER), published in January 2017, states that

> the electricity sector's increasing reliance on natural gas raises serious concerns regarding the need to secure natural gas pipelines against emerging cybersecurity threats. Thus, the adequacy of cybersecurity protections for natural gas pipelines directly impacts the reliability and security of the electric system.[103]

Among its recommendations, the QER calls for assessment of natural gas and electricity infrastructure interdependencies to cybersecurity protection.[104] Likewise, some Members of Congress have expressed concern about the increased interdependency of electric power and natural gas in the security context.[105] The president of NERC reportedly also has expressed concern about the possibility of multiple natural gas facilities being intentionally disrupted, and the associated effects on the electric system.[106]

Executive Order 13636 (§9) directs DHS, in consultation with the SSAs (e.g., DOE) and other relevant agencies, to examine and identify critical infrastructure at risk of causing a catastrophic impact due to a cybersecurity incident.[107] It is not clear, however, whether the required risk analysis would only account for direct impacts to an infrastructure experiencing a cyberattack, or would include impacts to infrastructure with which it is interdependent. While a single electric or natural gas facility may not meet the criteria to be considered critical and vulnerable to a catastrophic cyber disruption, it is possible that the combination of direct and indirect impacts

[101] See, for example, Governor Rick Perry, U.S. Senate Committee on Energy and Natural Resources January 19, 2017, Department of Energy Secretary Nomination Hearing: Responses to Questions for the Record, February 6, 2017, pp. 54-55, https://www.eenews.net/assets/2017/02/06/document_pm_01.pdf.

[102] Congress may still request GAO to perform investigations through direct letters. Brian Dabbs, "Energy Grid Security Risks Need Assessment, Democrats Say," Bloomberg BNA, article, July 18, 2017, at http://news.bna.com/clln/CLLNWB/split_display.adp?fedfid=116904823&vname=ccrnotallissues&jd=0000015d55d5d721a1ddf7d7d6d60000&split=0.

[103] U.S Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review*, January 2017, p. 4-32.

[104] Ibid., p. S-20.

[105] See, for example: Senator Maria Cantwell, Statement before the Senate Committee on Energy and Natural Resources, *Hearing to Examine the Status and Outlook for U.S. and North American Energy and Resource Security*, July 18, 2017.

[106] Blake Sobczak et al., "Cyber Raises Threat Against America's Energy Backbone," *E&E News*, May 23, 2017, https://www.eenews.net/energywire/stories/1060054924/.

[107] The White House, "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, February 12, 2013.

could elevate the potential risks associated with that facility. How OE's cybersecurity programs and expertise in energy delivery systems could best be used to inform such analysis may be of interest to Congress.

Energy Cybersecurity Coordination

In addition to DOE, other federal agencies, notably FERC and DHS (particularly TSA), state regulators, and energy companies have roles and responsibilities for the cybersecurity of the energy sector. However, federal coordination for sector cybersecurity appears fragmented among these entities depending on the nature of a given scenario. For instance, DHS is the lead for overall critical infrastructure protection and national cybersecurity incident coordination; it also has statutory authority to regulate pipeline security. However, DOE is the SSA for the energy sector, part of which is regulated by FERC and state agencies. Additionally, it is the private sector which adopts trade practices for ICS technology and contracts with ICS vendors for cybersecurity products and services. The effect of the dispersed cybersecurity responsibility at the federal level has been the subject of congressional interest, but has not been studied to understand the effect on all energy cybersecurity stakeholders.[108] Congress may examine how OE's cybersecurity activities fit in, and coordinate with, the other various roles in energy cybersecurity for electricity, oil and natural gas pipelines, and other related energy infrastructure. In particular, Congress may examine how OE's RD&D programs and other work with the National Labs in electric power sector cybersecurity supports federal and private sector efforts in pipeline cybersecurity.

[108] See, for example, U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Energy, *The Electricity Sector's Efforts to Respond to Cybersecurity Threats*, 115th Cong., 1st sess., February 1, 2017, Serial No. 115-3 (Washington: GPO, 2017), and the U.S. Senate Committee on Energy and Natural Resources, "Hearing to Examine Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats," hearing website, April 4, 2017.

Appendix. Cybersecurity RD&D Projects

Table 1. Selected Office of Electricity Delivery and Energy Reliability Co-Funded Projects

Project Name	Lead Institution(s)	Objective	Primary Subsector
Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CODEF)	ABB	Distributed security domain layer that enables grid protection and control devices to collaboratively defend against cyberattacks	Electric
Cyber Attack Resilient HVDC System	ABB	Studying potential cyber-physical threats that could affect power dispatch across high-voltage direct current connections	Electric
Multi-layered Resilient Microgrid Networks	ABB	Measurement, control, and detection strategies to protect microgrids from adverse weather or cyber events	Electric
Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CODEF)	ABB	Distributed security domain layer enabling transmission and protection devices to defend against cyberattacks	Electric
A Resilient Self-Healing Cyber Framework for Power Grid	Argonne National Laboratory	Holistic security and cloud outsourcing framework for power grid applications	Electric
A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications	Argonne National Laboratory	Cyberattack-resilient wide-area monitoring, protection, and control framework	Electric
Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters	Argonne National Laboratory	Attack-resilient architecture and layered cyber-physical solution portfolio to protect distributed energy resources	Electric
Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)	Brookhaven National Laboratory	Online tool for utilities to assess impact and evaluate response to cybersecurity issues on forecasting data used to operate their systems	Electric
A Metamorphic Cybersecurity Educational Platform	Cybati	Cybersecurity educational program on energy delivery systems that targets energy sector professionals and students	Multi
Secure Policy-Based Configuration Framework (PBCONF)	Electric Power Research Institute	Framework allowing utilities to centrally manage the remote configuration of energy delivery system devices more securely	Electric

Project Name	Lead Institution(s)	Objective	Primary Subsector
Lemnos Interoperable Security	EnerNex	Interoperability configuration profile for secure communications between control system networks operated by different vendors	Multi
Patch and Update Management Program for Energy Delivery Systems	Foxguard Solutions	Cyber secure patching and updating of industrial control system devices	Electric
Cyber-Attack Detection and Accommodation for Energy Delivery Systems	GE Global Research	Automatic cyberattack anomaly detection and accommodation (ADA) system for power plants	Electric
Cyber-Physical Modeling and Simulation for Situation Awareness (CYMSA)	Georgia Tech Research Institute	Situational awareness technology suite to detect manipulation of power grid components and communications networks	Electric
ARMORE: Applied Resiliency for More Trustworthy Grid Operations	Grid Protection Alliance	Framework for secure information exchange in critical infrastructure to increase grid operation security and resiliency	Electric
Validation and Measuring Automated Response (VMAR)	Idaho National Laboratory	Cyber incident response comparison and enabling industry to select response technologies	Electric
Enhanced Security in Power System Edge	Intel Federal	Securely connect energy infrastructure devices to the cloud to allow the devices to interact	Electric
Autonomous Tools for Attack Surface Reduction	Iowa State University	Framework to continually assess and autonomously reduce the potential points of attack for grid control	Electric
Supporting Cyber Security of Power Distribution Systems by Detecting Differences Between Real-time Micro-Synchrophasor Measurements and Cyber-Reported SCADA	Lawrence Berkeley National Laboratory	Measurement network to detect and report the impact of cyber security attacks on the distribution system network	Electric
Safe Active Scanning for Energy Delivery Systems (SASEDS)	Lawrence Livermore, Idaho	Literature survey and interviews to understand whether active scanning techniques may be safely applied to energy delivery systems	Multi
Quantum Security Modules for the Power Grid	Los Alamos National Laboratory	Devices to encrypt control data with quantum keys for secure transmission over computer networks like the Internet	Electric

Project Name	Lead Institution(s)	Objective	Primary Subsector
Energy Sector Security Through a System for Intelligent Learning Network Configuration Management and Monitoring (ESSENCE)	National Rural Electric Cooperative Association	Provide electric cooperatives with cybersecurity tools for mapping networks, analyzing traffic, and learning expected traffic flow to inform human operators	Electric
NRECA REACT	National Rural Electric Cooperative Association	Tool to rapidly detect cyberattacks and compromised utility systems	Electric
Timing Authentication Secured by Quantum Correlations (TASQC)	Oak Ridge National Laboratory	System of ground-based timing and communication beacons enhancing security with geographically distributed quantum correlations	Electric
Cliques: Certificate Revocation List (CRL)-less Revocation and Anonymous Authentication for the Smart Grid	Oak Ridge National Laboratory	Secure revocation and provision of cryptographically secured authorizations in a publish-subscribe controlled micro-grid	Electric
Improving Situation Assessment/Awareness for Utility Operators and Cybersecurity Professionals	Pacific Northwest National Laboratory	Visualizations for cybersecurity professionals to maintain situational awareness during unfolding cyber events	Electric
Energy Delivery Systems Forensics	Pacific Northwest National Laboratory	Evaluating existing Live Analysis monitoring and detection tools for energy delivery systems	Multi
MultiSpeak Secure Protocol Enterprise Access Kit (MS-SPEAK)	Pacific Northwest National Laboratory	Enterprise service bus for better interoperability and cybersecurity of the MultiSpeak data standard	Electric
Automated Disruption Tolerant Key Management (ADTKM)	Pacific Northwest National Laboratory	Key management system for device identity, authentication, and authorization in electric distribution systems	Electric
Artificial Diversity and Defense Security (ADDSec)	Sandia National Laboratory	Use software-defined networking to introduce randomness to control system networks, protecting against cyberattack	Multi
Watchdog	Schweitzer Engineering Laboratories	Develop a managed switch that performs deep packet inspection using a whitelist approach for allowed communications	Electric

Project Name	Lead Institution(s)	Objective	Primary Subsector
Software Defined Networking (SDN)	Schweitzer Engineering Laboratories	Flow controller to monitor, configure, and maintain network traffic flows of all energy control system local area networks	Multi
Secure Software-Defined Radio	Schweitzer Engineering Laboratories	Flexible platform for secure wireless communications to utility distribution automation devices	Electric
Chess Master Project	Schweitzer Engineering Laboratories	Operational networks that deny-by-default unexpected cyber activity with pre-engineered response to intrusions	Multi
Padlock	Schweitzer Engineering Laboratories	Security gateway to sense physical tampering to distribution level field devices and take cyber actions to respond to intrusion	Electric
Integration of Renewables with Building & Electric Power (INGRESS)	United Technologies Research Center	Techniques to secure the integration of distributed energy resources to the grid	Electric
Cybersecurity for Secure Evolvable Energy Delivery Systems (SEEDS)	University of Arkansas	Research and to develop energy sector cyber security technologies, tools, and methodologies	Multi
Cyber Resilient Energy Delivery Consortium (CREDC)	University of Illinois	Consortium of universities and national labs to improve resilience and security primarily in electric, oil, and gas cyber networks	Multi

Sources: OE, *Peer Review: Cybersecurity for Energy Delivery Systems (CEDS) 2016*, December 7-9, 2016, Arlington, VA, https://energy.gov/sites/prod/files/2017/03/f34/CEDS%20Peer%20Review%20Program_12.01.16.pdf; OE, "Cybersecurity for Energy Delivery Systems (CEDS) Fact Sheets," web page, June 12, 2017, https://energy.gov/oe/downloads/cybersecurity-energy-delivery-systems-ceds-fact-sheets; Information Trust Institute, "Valdes Receives Two Grants to Improve Resiliency in Energy Systems," press release, March 31, 2017; Energy Sector Control Systems Working Group, *ieRoadmap*, online database, June 15, 2017, https://www.controlsystemsroadmap.net/efforts/Pages/default.aspx; CRS analysis.

Notes: Primary subsector categorization by CRS is based on explicit project descriptions, project partners, technology applications, or specific testing applications.

Author Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Richard J. Campbell
Specialist in Energy Policy

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer