By: Susan Lindberg
August 2022

Introduction

Energy infrastructure is a prime target for cyberattacks. Adversaries may launch ransomware or other types of attacks on the computer systems of pipelines or power grids with the aim of causing physical or economic damage, extracting a ransom payment, or both. The first cyberattack to have a significant public impact in the U.S. was the May 2021 ransomware attack on Colonial Pipeline. Colonial shut down its 5,500 mile diesel, gasoline, and refined products pipeline -- the largest fuels pipeline in the U.S. -- in response to the attack. This resulted in significant disruption in fuel supply along the East Coast. The shutdown was necessary to address the attack, notwithstanding that Colonial paid the nearly $5 million ransom demanded by the attackers. The incident underscored the increase in reported ransomware attacks on U.S. companies resulting in data compromise or disruption of service, and the increase in the size of ransoms demanded and (often) paid. According to one report, in the first half of 2021, the average cost of recovery and ransom associated with a ransomware attack was twice the 2020 average. While the energy sector comprised just 3% of ransomware attack victims in early 2021 (compared to 39% in manufactured goods and 18% in technology and technology services), the importance of a secure energy infrastructure to public safety and economic well-being has caused the executive branch, lawmakers, and regulators to intensify their focus on energy cybersecurity, and cybersecurity generally.

Cybersecurity regulation is not new. Security of critical infrastructure, which includes energy infrastructure, has been a focus of the U.S government for decades. Regulation has mostly been limited to either providing government resources to private industry, and securing the government's own systems. Over the years, a series of presidential executive orders created an infrastructure protection function in what is now the Department of Homeland Security (DHS).[1] Meanwhile, the security of U.S. infrastructure for producing, transporting, storing, and distributing energy, most of which is privately owned, remained at the discretion of the owners and operators of that infrastructure. Regulation has been inconsistent among different sectors of the industry. For the oil and gas industry, until recently, the government has largely depended on private industry to adopt voluntary security measures security assessment, mitigation measures, and incident response. The electric power industry, on the other hand, has more established cybersecurity regulation.

While government agencies have made efforts to encourage energy companies to adopt certain practices for risk assessment and mitigation, and to share information regarding cyberattacks, compliance with many of those recommendations has been voluntary. With the increase of cyberattacks by foreign operatives and others on key players in private industry, collaborative efforts to share information on threats and attacks is now the subject of intense focus. So, while federal government focus on cybersecurity isn't new, the recent move towards a mandatory regulatory model from a voluntary one is new to many companies, and is requiring changes in company processes.

---

[1] See Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, Fed. Reg. vol. 66, No. 202, Oct. 18, 2001, p. 53063. Order 13231 established the Critical Infrastructure Protection Board, which coordinated with the office of Homeland Security on information infrastructure protection functions.

This paper will address:

- Regulatory structure for voluntary cybersecurity activity
- Recent developments
- Industry specific cybersecurity requirements
  - pipelines
  - bulk electric system
  - nuclear power generation
  - oil and gas exploration and production
- Securities regulation

Regulatory structure for voluntary cybersecurity activity

Information Sharing and Analysis Centers (ISACs), NIST publications on cybersecurity, and services and information available from CISA and other agencies are examples of the federal government's efforts to encourage private industry to utilize resources made available to improve cybersecurity. Companies sharing information with the government about cyber threats and attacks are offered specific legal protections. Additionally, the government has an inter-agency system for responding to cybersecurity incidents.

ISACs

In an early effort to encourage industry and government to share information on cyber threats and vulnerabilities, Presidential Decision Directive 63, issued in 1998, established a framework for information sharing and analysis centers (ISACs).[2] ISACs collect information securely from private industry, process and anonymize the data, and communicate sector-specific vulnerability, threat, and other information to industry participants. Reporting to an ISAC is mandatory only in rare instances (for example, bulk power industry participants must report certain data to E-ISAC). Voluntary reporting to ISACs in most industries has not been robust, so ISACs have been of limited usefulness. ISAC reporting presents a chicken-and-egg problem: industry participants complain that the service is not as useful or reliable as it could be, and so they are reluctant to take the time to report, while at the same time the utility and reliability of an ISAC depends largely on the data they receive from companies. There are several ISACs in the energy industry. The oil and gas ISAC (ONG-ISAC) has recently renewed its efforts to educate the industry about its services and to encourage reporting. ONG-ISAC, which is available on a membership basis, provides technology tools, notifications, technology support, and other services to the upstream, integrated oil, natural gas, energy services, midstream, and downstream oil and gas companies. Another energy ISAC is the Downstream Natural Gas ISAC (DNG-ISAC).

NIST

The NIST Cyber Security Framework (CSF) is a publication intended to provide organizations with practical guidance on how to prevent, detect, and respond to cyberattacks. It is widely adopted

[2] See Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, Fed. Reg. vol. 63, No. 150, p. 41804, Aug. 5, 1998 https://www.govinfo.gov/content/pkg/FR-1998-08-05/pdf/98-20865.pdf

and used in connection with other standards.[3] NIST, or the National Institute of Standards and Technology, is part of the U.S. Department of Commerce and is a well-known example of a statutorily mandated and funded resource intended to assist industry in assessing and managing cyber risk.[4] While NIST publications on cybersecurity primarily target the government sector, many of them are useful in private critical infrastructure industries. The NIST CSF was created as a general resource for use by government and the private sector alike in response to Executive Order 13636.[5] At least one energy industry association has endorsed the NIST CSF as "the pre-eminent standard for companies' cybersecurity programs and for policymaking globally because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across the natural gas and oil industry and other industry sectors." [6]

DHS Initiatives and Services; Department of Energy

The Cybersecurity and Infrastructure Security Agency (CISA) is part of the U.S. Department of Homeland Security. One of CISA's primary purposes is to lead the sharing of cyber threat information between government and the private sector.[7] CISA provides cybersecurity technical assistance and incident response assistance, upon request. CISA also makes services available for a fee: it will conduct assessments such as Vulnerability Scanning, Validated Architecture Design Review, Risk and Vulnerability Assessment, or a Phishing Campaign Assessment.[8] Cyber incidents may be reported to CISA through an online Incident Reporting System, which it describes as a "secure web-enabled means of reporting computer security incidents." Incidents may also be reported by phone. The CISA website contains practical information such as alerts on specific threats, a compilation of legal references, and a CISA Cyber Essentials Starter Kit.

The Transportation Security Administration (TSA), another agency of the Department of Homeland Security, is probably best known for its role in airport security, but the TSA is also the primary resource for cybersecurity of surface transportation, including pipelines. The TSA has voluntary programs for pipelines, and in 2021 and 2022 issued security directives imposing significant requirements on the owners and operators of pipelines. These are described more fully in the section on pipeline regulation.

---

[3] Other cybersecurity standards include ISACA, Control Objectives for Information Technologies, http://www.isaca.org/COBIT/Pages/default.aspx American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731; ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785 International Organization for Standardization, Information technology – Security techniques – Information security management systems – Requirements: https://www.iso.org/standard/54534.html

[4] NIST operates under the authority of the National Institute of Standards and Technology Act (15 U.S.C. 271), which amends the Organic Act of March 3, 1901 (ch. 872), that created the National Bureau of Standards (NBS) in 1901.

[5] Executive Order 13636 of Feb. 12, 2013 – Improving Critical Infrastructure Security, Fed. Reg. vol. 78, No. 33, Feb. 19, 2013, p. 11739. The Executive Order mandated the NIST Cyber Security Framework as a baseline framework to reduce risk to critical infrastructure, and directed the DHS and DoD to expand the voluntary information sharing program in which classified cyber threat and technical information is provided to eligible critical infrastructure companies.

[6] Defense in Depth: Cybersecurity in the Natural Gas and Oil Industry, Oil and Natural Gas Subsector Coordinating Council and Natural Gas Council (2018) accessed at https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

[7] CISA was established by the Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C.§ 659.

[8] Cybersecurity and Infrastructure Security Agency, National Cybersecurity Assets and Technical Services, https://us-cert.cisa.gov/resources/ncats.

The Department of Energy (DOE) plays a less significant role in cybersecurity than DHS. The DOE organization includes an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Like CISA, CESER offers resources to the industry. After the Colonial attack and the threats to critical infrastructure prior, the Department of Energy has reportedly requested $201 million for the 2022 fiscal year to invest in cybersecurity efforts.

Safe Harbor for Information Sharing

The Cybersecurity Information Sharing Act of 2015[9] required the Department of Homeland Security to establish a capability and process for sharing cyber threat indicators with both the federal government and private sector entities. Importantly, the statute includes protections for private companies that share information with the government through DHS. Notwithstanding any other law, companies reporting certain cybersecurity information to DHS receive liability protections, privileges are maintained, proprietary information is protected, information is not disclosed in response to Freedom of Information Act requests, and other protections.[10] These aspects are further detailed in guidance documents.

Federal Agency Coordination for Incident Response

When there is a cyberattack on energy infrastructure, the federal government response is managed pursuant to Presidential Policy Directive 41.[11] Threat response and action against the adversary is addressed by the FBI. CISA is in charge of asset response, and mitigating the immediate impact of a breach. Other agencies may be involved depending on their mandate. For example, DOE was involved in the response to the Colonial Pipeline incident because fuel supply, an area of DOE responsibility, was the main impact of that particular incident.[12]

Recent Developments

Executive Order: Improving the Nation's Cybersecurity

Soon after the Colonial Pipeline ransomware attack, President Biden issued an Executive Order calling for improved information sharing between the U.S. government and the private sector on cyber issues.[13] While the Executive Order is broad reaching, it does not mandate disclosure of cyberattacks, nor does it place any other requirements on private companies. It ordered DHS to create a Cyber Safety Review Board (CSRB) by DHS.[14] The CSRB's mandate is to "provide recommendations to the Secretary

---

[9] 6 U.S.C. §§1501-1533.

[10] For example, the statute contains an antitrust exemption for exchange of cyberthreat or defensive information or providing assistance between two private parties, *Id.* at § 1503(e), exemption from waiver of privilege or trade secret protection *Id.* at § 1504(d)(2), and exemption from disclosure under 5 U.S.C. § 552 (FOIA), *Id.* at § 1504(d)(3).

[11] *See* Presidential Policy Directive 41 (PPD-41) -- United States Cyber Incident Coordination, July 26, 2016.

[12] DOE's Energy Information Agency commented that, in response to the Colonial incident, was in contact with state and local agency to assess fuel supply and impacts due to the pipeline's shutdown.

[13] Exec. Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity, 86 FR 93, May 17, 2021. This is not the first time a President has called for improved cybersecurity information sharing. In 2015, Executive Order 13691 -- Promoting Private Sector Cybersecurity Information Sharing, established Information Sharing and Analysis Organizations (ISAOs) to gather, analyze, and disseminate industry-specific cyber threat information. Exec. Order 13691 of Feb. 20, 2015, Promoting Private Sector Cybersecurity Information Sharing, 80 FR 34, Feb. 20, 2015.

[14] Authority: Section 871 the Homeland Security Act of 2002 (6 U.S.C. (451)

of Homeland Security for improving cybersecurity and incident response practices."[15] The CSRB has been established and a charter issued. The CSRB has issued its first report: a review of the December 2021 Log4j event. The May 12, 2021 Executive Order contains directives for improving information security in the U.S. government. These include steps toward zero trust architecture, securing cloud services, improving security of the software supply chain, and improving detection of vulnerabilities and incidents on federal government networks.

DOJ Civil Cyber-Fraud Initiative

In October 2021, the U.S. Department of Justice announced a Civil Cyber-Fraud Initiative. The DOJ intends to use the False Claims Act to bring civil lawsuits against entities that commit fraud on the government by violating their legal obligations with regard to cybersecurity. Specifically, the DOJ will pursue individuals or companies that put government systems or information at risk by knowingly: a) providing deficient cybersecurity products or services, b) misrepresenting their cybersecurity protocols, or c) violating obligations to monitor and report cybersecurity incidents and breaches. The DOJ has already brought and settled three cases. While these cases involved the healthcare and aviation industries, action by the DOJ is possible against any entity, including an energy company, contracting with the government. The False Claims Act also allows private citizens with evidence of fraud to file a *qui tam* suit on behalf of the government, and to collect a portion of the damages if the suit is successful.[16]

Legislation

The U.S. Legislature has frequently considered cybersecurity legislation, and, although most bills fail to progress, a significant cybersecurity bill was signed into law in 2022. The Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), enacted March 15, 2022, requires critical infrastructure companies to report cybersecurity incidents to CISA within 72 hours, and ransom payments within 24 hours.[17] The requirements will become effective when CISA issues new regulations implementing the statute. CISA has until March 2024 to propose rules and another 18 months after that to finalize them. Affected companies will have the opportunity to comment during the CISA rulemaking process.

CIRCIA acknowledges the need to reconcile disparate cybersecurity regulations. CISA is required to establish and lead an interagency Cyber Incident Reporting Council to "coordinate, deconflict, and harmonize" existing incident reporting requirements. The Council must analyze disclosure regulations to ensure that requirements do not conflict, or that they are not duplicative or burdensome.

CISA has not yet proposed rules. Generally, the statute requires covered entities to report "covered cyber incidents." At a minimum, these are:

---

[15] Exec. Order 14028 at Sec. 5. While some have expressed optimism that CSRB would share lessons learned and make specific recommendations for change, similar to the National Transportation Safety Board in the aviation industry (See S. Bellovin and A. Shostack, "Finally! A Cybersecurity Safety Review Board," *Lawfare*, June 7, 2021, https://www.lawfareblog.com/finally-cybersecurity-safety-review-board#), such activity is not specifically mentioned in the CSRB's charter.

[16] See False Claims Act, 31 U.S.C. § 3279, *et seq.*

[17] The new law amends Title XXII of the Homeland Security Act of 2002, 6 U.S.C. § 651, *et seq*.

- a cyber incident that leads to substantial loss of confidentiality, integrity or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;
- a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack or exploitation of a zero day vulnerability; or
- unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

The new statute directs CISA to clearly describe the types of incidents that are "covered cyber incidents." Ransom payments in connection with a covered cyber incident must also be reported.

Reported information will be anonymized, aggregated, and shared among various government agencies in order to improve cybersecurity, identify and track attackers, and assist companies in addressing ongoing threats and vulnerabilities.

Sector-Specific Cybersecurity Regulation

Pipelines

The Transportation Security Administration (TSA) of the Department of Homeland Security oversees the security of surface transportation, and is the main agency overseeing pipeline cybersecurity.[18] TSA's publication, Pipeline Security Guidelines, provides a framework for risk assessment and control implementation.

In May 2021, under its emergency authority granted by a federal statute that authorizes the TSA Administrator to issue a regulation or security directive immediately in order to protect transportation security, the TSA issued Security Directive Pipeline-2021-01 (SD-1). Applicable to pipeline Owners/Operators[19], SD-1 requires: 1) reporting of cybersecurity incidents within 24 hours[20] to CISA, 2) designation of a Cybersecurity Coordinator to be available around the clock to coordinate with TSA and CISA, and 3) review and report to TSA and CISA the pipeline's current state of cybersecurity, as compared to Section 7 of TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021), within 30 days of the Directive. While the TSA issued this and several subsequent Security Directives without notice and comment rulemaking, the TSA has engaged in a dialogue with Owners/Operators, including allowing Owners/Operators to submit proposed alternative measures for approval as they work to comply with the requirements. Additionally, TSA acknowledged in a subsequent Security Directive that its emergency regulations and security directives are required to be reviewed and ratified by the Transportation Security Oversight Board (TSOB). See SD-2B. The TSOB ratified the TSA's directives in May 2022. The non-SSI Security Directives in the series are available on TSA's website.

---

[18] The Homeland Security Act of 2002 (Pub. Law 107-296) established the DHS and set forth the primary mission of the Department. The Aviation and Transportation Security Act established the Transportation Security Administration in November 2001 (Pub. Law 107-71).

[19] The Directive applies to TSA-specified Owners/Operators; the Directive defines Owner/Operator as a person who owns or maintains operational control over pipeline facilities or engages in the transportation of hazardous liquids or natural gases *and* who has been identified by TSA as one of the most critical.

[20] TSA changed the deadline for making the report to 24 hours in Security Directive Pipeline - 2021-01B (SD1B) on May 29, 2022. Originally, the deadline was 12 hours.

When it issued SD-1, the TSA stated that it issued the Directive to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. The TSA and CISA intend to use information gained from Owners/Operators for vulnerability identification, trend analysis, or to generate tools to prevent other cybersecurity incidents.[21] The requirements of the Directive have a common theme of pipeline and TSA or CISA coordination and collaboration in response to a security incident.

Information reported to TSA under the Security Directives is Sensitive Security Information (SSI), meaning that it is subject to certain protections. The TSA's regulations protect sensitive information and contain very specific requirements on the marking, communication, and secure storage of SSI.[22] Information submitted by Owners/Operators will be shared among TSA, CISA, the National Response Center "and other agencies as appropriate." So, a pipeline's SSI should remain secure, as long as the various agencies follow their own security rules.

In July 2021, the TSA issued a second Security Directive, Security Directive Pipeline-2021-02. SD-2 was designated as SSI and distributed on a limited basis. In December 2021, TSA issued Security Directive Pipeline-2021-02B, and in July 2022 the SSI designation was removed from that Security Directive. SD-2B contains very specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems. It requires pipelines to develop and implement a cybersecurity contingency and recovery plan, and to conduct a cybersecurity architecture design review.

In July 2022, TSA issued Security Directive Pipeline-2021-02C, which supersedes and replaces SD-2B. SD-2C includes requirements for covered Owner/Operators to 1) establish and implement a TSA-approved Cybersecurity Implementation Plan, 2) develop and maintain a Cybersecurity Incident Response Plan to reduce the risk of operational disruption, and 3) establish a Cybersecurity Assessment Program, and submit an annual plan that describes how the pipeline will assess the effectiveness of cybersecurity measures. Until a pipeline's Cybersecurity Implementation Plan is approved by TSA, it must continue to implement the specific measures from SD-2B, as identified in the Attachment to SD-2C, and modified by any TSA approved alternative measures and/or action plans.

The Federal Energy Regulatory Commission (FERC) plays a less significant role than the TSA in pipeline cybersecurity. FERC has regulatory authority over interstate natural gas pipelines under the Natural Gas Act of 1938, and over interstate oil pipelines (as common carriers) under the Interstate Commerce Act. FERC has incorporated business practice standards from groups like the North American Energy Standards Board (NAESB) into its regulations to enhance the natural gas industries' system and software security measures.[23] For example, NAESB standards require evaluation of software fixes or patches for known vulnerabilities within 30 days and implementing the fix or patch as soon as reasonably practicable, and using HTTPS to protect information in transit."[24] While FERC references these best practices, they are guidelines only. As discussed in the next section, FERC has a more substantial role in cybersecurity regulation of the electric power industry.

---

[21] Presidential Policy Directive (PPD) 41 requires Federal agencies to rapidly share incident information to achieve unity of governmental effort. *See* PPD-41 § III.D ("Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident").

[22] Protection of Sensitive Security Information, 49 C.F.R. § 1520.5, *et seq.*

[23] Standards for pipeline business operations and communications, 18 C.F.R. § 284.12.

[24] *Id*.

Bulk Electric System

The North American Electric Reliability Corporation (NERC) was designated by FERC as the U.S.'s Electric Reliability Organization (ERO), pursuant to FERC's authority under the Energy Policy Act. FERC has authority to approve mandatory cybersecurity reliability standards for the bulk power system. NERC's mandate as an ERO is "to establish and enforce reliability standards for the bulk-power system, subject to Commission review."[25] A reliability standard is "a requirement . . . to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection . . . ."[26] Further:

> 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.[27]

The Bulk Electric System (BES) subject to reliability standards includes all elements and facilities necessary for the reliable operation and planning of the interconnected bulk power system. A relevant cybersecurity incident is "a malicious act or suspicious event that disrupts, or was an attempt to disrupt the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."[28]

NERC has issued more than 95 Critical Infrastructure Protection (CIP) reliability standards for the BES pertaining to cybersecurity. Of those, the following are active:

NERC Reliability Standards for Critical Infrastructure Protection

Title	Standard	Description
BES Cyber System Categorization	CIP-002-5.1a	Identify and categorize Cyber Assets for the application of cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those Cyber Systems could have on the reliable operation of the BES
Security Management Controls	CIP-003-8	Consistent and sustainable security management controls that establish responsibility and accountability
Personnel & Training	CIP-004-6	Personnel risk assessment, training, and security awareness for protecting Cyber Systems
Electronic Security Perimeters	CIP-005-6 (current) CIP-005-7 (effective October 1, 2022)	Manage electronic access to Cyber Systems by specifying a controlled Electronic Security Perimeter
Physical Security of BES Cyber Systems	CIP-006-6	Manage physical access to Cyber Systems by specifying a physical security plan
System Security Management	CIP-007-6	Manage system security by specifying select technical, operational, and procedural requirement
Incident Reporting and Response Planning	CIP-008-6	Mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements

[25] 16 U.S.C. § 824o(a)(2).

[26] *Id* § 824o(a)(3).

[27] *Id* § 824o(a)(4).

[28] *Id* § 824o(a)(8).

Recovery Plans for BES Cyber Systems	CIP-009-6	Recover reliability functions performed by Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES
Configuration Change Management and Vulnerability Assessments	CIP-010-3 (current) CIP-010-4 (effective October 1, 2022)	Prevent and detect unauthorized changes to Cyber Systems by specifying configuration change management and vulnerability assessment requirements
Information Protection	CIP-011-2	Prevent unauthorized access to Cyber System Information by specifying information protection requirements
Communications between Control Centers	CIP-012-1	Protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between Control Centers. Control Center owner/operator must implement a documented plan
Supply Chain Risk Management	CIP-013-1 (current) CIP-013-2 (effective October 1, 2022)	Security controls for supply chain risk management
Physical Security	CIP-014-2	Identify and protect critical transmission stations and transmission substations, and associated primary control centers

BES owners/operators must notify the E-ISAC and National Cybersecurity and Communications Integration Center (NCCIC) of certain cyber incidents. The NCCIC (within DHS) assists asset owners in mitigating vulnerabilities, identifies other entities that might be at risk, and shares information across public and private sectors. Notifications must meet specific requirements.[29]

FERC and NERC have the power to impose civil penalties for failure to comply with electric reliability standards, including CIP standards.[30]

Nuclear Power Generation

Nuclear power generation facilities are regulated by the Nuclear Regulatory Commission.[31] The NRC specifically requires assurance of cybersecurity at nuclear facilities,[32] and notification of cybersecurity events.[33] The NRC published detailed guidance in 2015 about notification requirements, timing, purpose, and use of the information. Consistent with PPD-41, the NRC shares reports of cybersecurity activities with DHS, federal law enforcement, and the intelligence community. The NRC's guidance contains instructions for treating reports as classified National Security Information or Restricted Data.[34]

Oil and Gas Exploration and Production (Offshore)

Except for oil and gas operations in the U.S. Outer Continental Shelf (OCS), there are no specific federal cybersecurity regulations for the exploration and production (upstream) industry. For the OCS, the U.S. Coast Guard (USCG) and the Bureau of Safety and Environmental Enforcement (BSEE) dedicate resources to cybersecurity.

---

[29] *See* Reliability Standard CIP-008-6.

[30] 16 U.S.C. § 824o(e).

[31] *See* 10 CFR Part 73.

[32] Protection of Digital Computer and Communication Systems and Networks, 10 CFR § 73.54.

[33] Cyber Security Event Notification, 10 CFR § 73.77.

[34] *Id.* at ¶¶ 3.2, 4.1.

USCG oversees security, both physical and cyber. for OCS operations.[35] It may conduct activities jointly with BSEE. USCG regulates all marine terminals used to load or unload vessels that transport unrefined petroleum, petroleum products, or liquefied natural gas (LNG). OCS operators are required 1) to perform facility security assessments (FSA), which must include measures to protect computer systems and networks,[36] and 2) have a facility security plan that considers cybersecurity.[37] Operators must notify USCG of suspicious activity and breaches of security, including cybersecurity. An incident that does not have physical or pollution effects may be reported to the NCCIC,[38] while certain other incidents, such as those that result in significant loss of life, environmental damage, transportation system disruption or economic disruption in a particular area (Transportation Security Incidents), must be reported to the USCG's National Response Center without delay.[39] Reports are considered SSI.[40]

The USCG's Cyber Command includes a Marine Cyber Readiness Branch. This function was created to maintain and update strategy and cyber policy in collaboration with industry.

For the offshore energy industry, including renewable energy, BSEE is in charge of improving safety and ensuring environmental protection. BSEE monitors safety issues including cybersecurity in the OCS, and posts alerts on its website. BSEE's Offshore Safety Improvement Branch collaborates with DHS, CISA, DOE, TSA, and USCG on cybersecurity matters.

Securities regulations

Many of the sizeable owners and operators of critical energy infrastructure are publicly traded. While current regulations of the U.S. Securities and Exchange Commission (SEC) do not contain specific requirements for cybersecurity, the SEC has issued guidance regarding material cybersecurity matters. Additionally, the SEC has proposed specific rules pertaining to cybersecurity.

The SEC's Statement and Guidance on Public Company Disclosures discusses a registrant's obligations to make disclosures in periodic reports, registration statements, current reports and other contexts, and addresses policies and procedures and other governance requirements. [41]

If a cybersecurity incident is material, it may need to be reported:

- On Form 10-K under management's discussion and analysis of financial condition and results of operations (MD&A), financial statements (for example, to the extent costs were incurred), and legal proceedings (if applicable).
- Form 10-Q under MD&A, financial statements, and updated risk factors, as applicable.

---

[35] See Maritime Transportation Security Act of 2002; Outer Continental Shelf Lands Act, 43 U.S. Code 1331, et seq. See also BSEE & Coast Guard Confront Offshore Cyber Attack Issues, Aug. 4, 2015, https://www.bsee.gov/blog-post/8042015.

[36] 33 CFR § 106.305(c)(v).

[37] 33 CFR § 106.400, *et seq.*

[38] *See* United States Coast Guard, *Reporting Suspicious Activity and Breaches of Security*, CG-5P Policy Letter, Dec. 2016, *available at* https://www.dco.uscg.mil/Portals/10/Cyber/Cyber-Readiness/CG-5P%20Policy%20Letter%2008-16%20-%20Reporting%20Suspicious%20Activity%20and%20BoS.pdf?ver=2020-05-26-173911-100&timestamp=1590758815625.

[39] *Id.*

[40] *Id.* at ¶. 2-f.

[41] See *Commission Statement and Guidance on Public Company Disclosures*, 17 CFR Parts 229 and 249, Release Nos. 33-10459; 34-82746, Feb. 26, 2018.

- Supplementing previous reports: registrants must provide further material information, as needed, to make previous required disclosures "not misleading." The SEC also expects that material cybersecurity risks be discussed under risk factors, and that the risk factors be updated to reflect any material incidents.[42]

The Commission has cautioned that an ongoing investigation or development of facts does not on its own provide a basis for avoiding disclosure of a material cybersecurity incident. They have also clarified that they do not expect disclosures so detailed that they would compromise security efforts (providing a roadmap for attackers).[43] Companies are not expected to disclose "specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident."[44] Cybersecurity risk must be covered in required risk factor disclosures, if it is among the risks that make investments in the company's securities speculative or risky. The SEC further notes that required discussion of financial condition, changes in financial condition, and results of operation should take into consideration the cost of security, and the many types of costs that may be incurred as a consequence of cyberattacks. The guidance goes on to cover other types of required disclosures such as description of business, legal proceedings, financial statements, and board risk oversight.

The SEC encourages comprehensive cyber policies and procedures, regular assessment of compliance, and sufficient processes regarding cybersecurity disclosure.[45] It acknowledges that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws."[46]

The SEC's guidance document emphasizes that directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge of a significant cybersecurity incident. The SEC encourages companies to cover this in their insider trading policies, and suggests that "while companies are investigating and assessing significant cybersecurity incidents. . .they should consider whether and when it may be appropriate to implement restrictions on insider trading. . .."[47]

If material nonpublic information, including such information pertaining to a cybersecurity incident, is disclosed to a Regulation FD covered person, the information must be publicly disclosed contemporaneously (or promptly – within 24 hours – in the case of inadvertent disclosure). [48] If a company selectively discloses information about a cybersecurity incident that is material, public disclosure is required via Form 8-K or any other broad, non-exclusionary means of public disclosure. Additionally, the NYSE rules for listed companies require timely disclosure to the public "any news or information which might reasonably be expected to materially affect the market for its securities," and that companies act promptly to dispel unfounded rumors that result in unusual market activity.

---

[42] See *In re Alphabet Securities Litig.* (9th Cir. 2021).

[43] *Commission Statement* at 11.

[44] *Id.*

[45] Including sufficient controls and procedures for processing and reporting of cybersecurity risks and incidents to the appropriate personnel "including up the corporate ladder, to enable senior management to make disclosure decisions and certifications." Exchange Act Rules 13a-15 and 15d-15 require companies to maintain disclosure controls and procedures, and for management to evaluate their effectiveness. 17 CFR 240.13a-15; 17 CFR 240.15d-15.

[46] *Commission Statement* at 18.

[47] *Id.* at 22.

[48] *Id.* at 23. *See also* 17 CFR 243.100(b)(1).

Finally, the guidance points out that there may be Regulation FD disclosure obligations in connection with cybersecurity matters if they amount to material nonpublic information and are selectively disclosed to certain persons.

The SEC has proposed a new rule entitled Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The proposed regulations would affirmatively require registrants to make the following disclosures regarding cybersecurity incidents:

- Disclosure on Form 8-K of cybersecurity incidents within four days of a determination that the incident is material.
  - materiality determination must be made "as soon as reasonably practicable"
  - what constitutes "materiality" will not change
  - disclosure to include (i) when the incident was discovered and whether it is ongoing, (ii) a brief description of the nature and scope of the incident, (iii) whether data was compromised, and if so, how, (iv) the effect on company's operation's, and (v) whether the incident has been remediated or is currently being remediated.
- Updated disclosure on Forms 10-Q and 10-K about previously reported cybersecurity incidents.

The proposed rule also requires all registrants to disclose information pertaining to cybersecurity governance, such as internal policies and board cybersecurity expertise.

Numerous representatives of the energy sector submitted comments on the proposed rule by the May 9, 2022 deadline. The SEC has indicated that it expects to issue a final rule in April 2023. It is not known what modifications the SEC will make to the proposed rule in response to comments, or when the rule would become effective.

Susan Lindberg
918-595-4826
slindberg@gablelaw.com

Energy | Cybersecurity | Digital Assets