Congressional Research Service
Informing the legislative debate since 1914

Critical Infrastructure Risk Management: Securing the Oil and Gas Supply Chain

December 13, 2021

Congressional Research Service
https://crsreports.congress.gov
R46987

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46987

December 13, 2021

Brian E. Humphreys
Analyst in Science and Technology Policy

Critical Infrastructure Risk Management: Securing the Oil and Gas Supply Chain

Supply-chain disruptions caused by critical infrastructure failures, targeted attacks, or pandemic disease have sparked broad congressional interest in assuring availability of essential supplies at affordable prices. Congressional deliberations have highlighted risks that these and other hazards may pose to critical supply functions, including supply of essential fuels and industrial feedstock. Disruptions to the oil and gas subsector may propagate across the entire economy, beginning with the petrochemical manufacturing and electricity generation—subsectors with key systems and assets that are often physically linked to oil and gas processing and refining facilities via an extensive pipeline network—and extend to agriculture, manufacturing, water, transportation systems, and other critical infrastructure sectors.

The Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), leads public-private partnerships for risk management and supply assurance in the energy sector, including the oil and gas subsector. The Department of Transportation (DOT) and the Transportation Security Agency (TSA), a DHS agency, lead analogous programs for pipeline safety and security. Although various components of the oil and gas subsector are subject to federal regulation in differing degrees, the federal critical infrastructure security and resilience (CISR) policy framework affords significant autonomy to private-sector stakeholders and generally favors voluntary collaboration. Federal agencies rely upon private-sector partners in the subsector to develop and implement voluntary consensus standards and best practices, and to engage in voluntary public-private partnerships for CISR-related policy coordination and information sharing.

Development of these partnerships to manage relevant categories of risk across the entire oil and gas supply chain has been uneven within the subsector. The most developed partnerships are generally found in those segments with a history of federal regulatory oversight or interest, such as offshore production facilities, long-distance pipeline transmission networks, and oil refineries. Similarly, this general pattern is observed in specific risk categories, such as process safety—and, to a lesser extent, cybersecurity. Physical security and supply-chain risk, also covered in this report, are both less regulated and less developed as consensus-driven voluntary activities within the oil and gas subsector. Federal regulatory regimes, public-private coordination programs and activities, and voluntary consensus standards within the subsector are often developed in conjunction with each other, via both formal and informal processes. Therefore, both compulsory and voluntary elements of the CISR enterprise coexist in the oil and gas subsector.

In some cases, this dynamic has spurred private-sector engagement in voluntary public-private CISR initiatives. For example, private-sector entities in the offshore exploration and drilling segment have worked with relevant federal regulatory agencies in the wake of the 2010 Deepwater Horizon oil rig explosion and spill in the Gulf of Mexico to develop coordination and information-sharing activities through industry and federal channels. In other cases—particularly in industry segments not subject to federal regulatory oversight such as onshore exploration and production—there is less substantive engagement between government and industry and shared risk information is generally less available. With few exceptions, federal voluntary information-sharing initiatives do not appear to have consistently elicited widespread interest and engagement from the oil and gas subsector, or the CISR enterprise as a whole.

The February 2021 cold weather event which disrupted power supplies across Texas, and the May 2021 ransomware attack against the Colonial Pipeline Company which disrupted fuel supplies along the East Coast, galvanized concerns in Congress regarding the CISR enterprise and its emphasis on voluntary public-private partnerships. Legislative proposals in the 117th Congress would create new authorities and oversight functions for federal agencies, new incident reporting requirements for industry, new federal capabilities for critical infrastructure risk modeling and data collection and analysis, and—in some cases—provide direct grant funding to private-sector critical infrastructure owner-operators for cybersecurity investments. Taken together, these measures presuppose a significant increase in the scope and extent of regulatory oversight within the CISR enterprise, as well as more centralized federal role in management of critical infrastructure risks.

Regarding oil and gas sector risk management, Congress may consider several issues: the role of federal agencies in industry-led standards development processes, and reliance on industry associations to provide standards used for regulatory purposes; information sharing and incident-disclosure requirements, and the structure and governance of information-sharing bodies; and optimization of regulatory, nonregulatory, or hybrid frameworks that combine voluntary guidance and public-private coordination with risk-management mandates.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

Supply-chain disruptions caused by critical infrastructure failures, targeted attacks, or pandemic disease have sparked broad congressional interest in assuring availability of essential supplies at affordable prices. Subsequent congressional hearings and legislative proposals have highlighted risks that these and other hazards may pose to critical supply functions, including supply of essential fuels and industrial feedstock. These congressional activities have raised questions about how the federal government and private-sector stakeholders manage risk in order to safeguard critical infrastructure and prevent supply disruptions that may affect national security, economic security, or public health and safety.

This report provides an overview of risk and risk management in the oil and gas subsector—part of the energy critical infrastructure sector—considering interdependencies between its various segments and a wide range of other critical supply functions.[1] Effects from disruptions to the oil and gas subsector may propagate across the entire economy, beginning with the petrochemical manufacturing and electricity generation subsectors. These subsectors have key systems and assets that are often physically linked to oil and gas processing and refining facilities via an extensive pipeline network. Disruption effects may subsequently extend to agriculture, manufacturing, water, transportation systems, and other critical infrastructure sectors.

In addition, this report analyzes the complex interdependencies between development of voluntary consensus standards, public-private partnerships, and regulatory regimes within the oil and gas subsector, and how these influence government and industry risk-management activities. This analysis may inform congressional assessments of both the overall security and resilience of the oil and gas subsector specifically, and critical supply functions more generally. Additionally, the report may provide deeper understanding of the structure and function of the national critical infrastructure security and resilience (CISR) enterprise as a whole.

Organization, Methods, and Scope of Report

The Cybersecurity and Infrastructure Security Agency (CISA), a Department of Homeland Security (DHS) agency, has established a set of 55 national critical functions as a means to improve risk management across multiple critical infrastructure sectors. CISA defines national critical functions as critical infrastructure enabled functions "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[2] CISA organizes these functions within four broad areas: connect, distribute, manage, and supply.

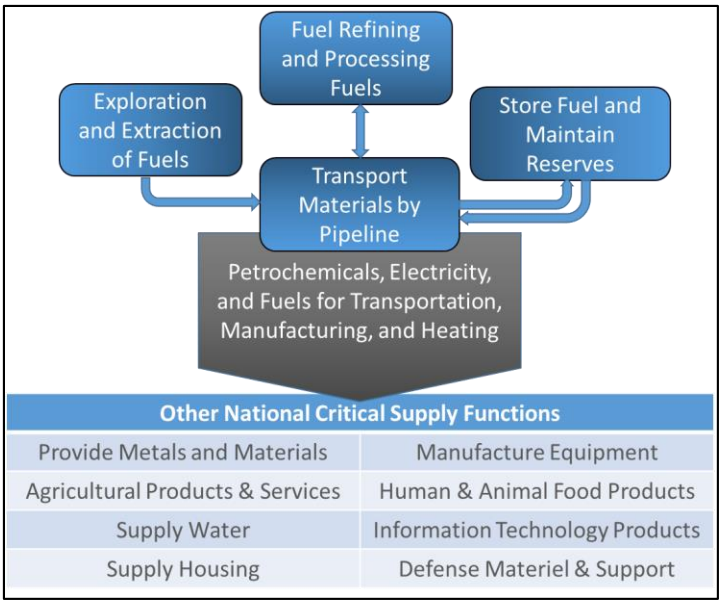
[1] The Department of Homeland Security recognizes 16 critical infrastructure sectors, and numerous associated subsectors. The Energy sector has two subsectors: oil and gas; and electricity. See Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," https://www.cisa.gov/critical-infrastructure-sectors.

[2] In 2019, CISA promulgated the National Critical Function (NCF) set to improve methods for infrastructure risk assessment and enable better collaboration across multiple CI sectors. See CISA, "National Critical Functions Set," https://www.cisa.gov/national-critical-functions-set. The definition of national critical functions parallels the statutory definition of critical infrastructure given in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (P.L. 107-56). It defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

This report focuses on management of risk to certain critical national functions in the "distribute," "manage," and "supply" areas that form the foundations of the oil and gas subsector: exploration and extraction of fuels; fuel refining and processing fuels; storage of fuel and maintenance of reserves; and transport of materials by pipeline. Together, these four national critical functions constitute a production, distribution, and supply system that provides necessary energy and chemical inputs for other national critical functions of supply outside the oil and gas subsector. These relationships are depicted below in **Figure 1**.[3]

Figure 1. The Oil and Gas Subsector

Providing Basic Inputs for National Critical Supply Functions



Source: CRS, adapted from CISA National Critical Functions Set.

Notes: See **Appendix A** for detailed graphic of connections between oil and gas supply chains and other industries and critical infrastructure.

The report begins with a policy background section that provides an overview of risk management, federal coordination and regulatory authorities for CISR-related programs and activities relevant to the oil and gas subsector, and the standards development process. This is followed by an overview of subsector risks incorporating both industry and government perspectives. Next, the report describes risk-management programs and activities in the subsector as these relate to regulatory and nonregulatory aspects of the national CISR risk-management enterprise. These programs and activities address four risk categories of particular concern in the oil and gas industry: process safety; physical security; cybersecurity; and third-party or supply-chain risk.

In this context, process safety relates to the design and safe operation of heavy industrial machinery. Physical security relates to protection of physical infrastructure systems and assets against deliberate attack, theft of materials, sabotage, or malicious use. Cybersecurity relates to protection from malicious exploitation of information and communications technology (ICT) used in information management, automated sensing, and industrial control systems. Supply chain risk management (SCRM) relates to an emerging area of risk management concerned with

[3] The Research and Development (R&D) supply function is omitted from the graphic.

external or third-party risks affecting the production and supply process as a whole, from the extraction of raw materials to manufacturing and distribution of finished products to end users.

In general, the nature, scope, and extent of coordinated risk-management programs and activities—both regulatory and nonregulatory—vary across the several segments of the oil and gas industry, from upstream production sites, to midstream storage and processing facilities, and finally to downstream refineries and marketing. The analysis in this report provides insight about this variation across oil and gas industry segments, focusing on the question of mutual influence between regulatory and nonregulatory programs and activities.

The report concludes with a discussion of potential issues for Congress.

Certain related issues are outside the scope of this report: federal authorities to directly manage and mobilize the productive resources (including energy production) of the United States for defense purposes under the Defense Production Act of 1950 (P.L. 81-774, 50 U.S.C. §§4501 et seq.); stockpiling programs such as the Strategic Petroleum Reserve; rate-setting and environmental policies that may affect industry decisions on infrastructure investments; and trade policies to encourage domestic production of strategic materials and commodities. Likewise, this report does not cover environmental protection regulations focused on prevention of spills and other impacts external to a given production or processing facility, and not directly related to national supply assurance issues. This report provides information on operational risks related to spread of pandemic disease, such as illness of key personnel or closure of facilities, but does not cover second-order effects on essential supplies caused by pandemic-related supply and demand imbalances or shocks.

Policy Background

The current federal critical infrastructure policy framework emphasizes the use of voluntary public-private partnerships for risk management. This is particularly the case in the oil and gas subsector given its unique ownership structure. In most countries, state ownership predominates in the oil and gas industry, including ownership of mineral rights. The U.S. oil and gas industry is distinctive in that both industrial enterprises and mineral rights are privately owned, and therefore development of what may be considered national resources is in private hands. However, mandatory and enforceable standards in subsector industries also play a role in the CISR risk-management enterprise. Balancing voluntary public-private partnerships for risk management and regulatory policy is an ongoing concern within the oil and gas subsector. The first section below provides a brief description of risk-management definitions and principles widely recognized by federal agencies and industry stakeholders. Sections on nonregulatory authorities, regulatory authorities, and the standards development process follow.

Risk Management Overview

CISA and other federal agencies typically assess risk as "a measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence."[4] In Congress and federal agencies, broad-based risk assessments may be used to inform planning and resource allocation decisions related to congressional appropriations and agency budgets, as well as emergency preparedness, regulatory oversight of certain industries, grant funding, and voluntary public-private partnerships. Private-sector stakeholders may use risk assessments to inform

[4] CISA, Interagency Security Committee, *The Risk-Management Process: An Interagency Security Committee Standard*, Washington, DC, 2021, p. 49, https://www.cisa.gov/sites/default/files/publications/The%20Risk%20Management%20Process%20-%202021%20Edition_1.pdf.

prioritization of capital investments, system design, and operational practices, in order to reduce the likelihood of adverse events, such as costly accidents, physical and cybersecurity breaches, and supply-chain disruptions.

Public and private-sector critical infrastructure risk managers generally seek to reduce risk to vulnerable systems, assets, and networks, rather than eliminate risk entirely, given limited resources of time, organizational capacity, and funding. Risk managers may also choose to accept certain risks or transfer them to other organizations. From this perspective, effective risk management is efficient—i.e., it achieves acceptable levels of risk at the lowest possible cost, and allows organizations to prioritize mitigation of the most serious risks to their most vital systems, assets, and networks. In practice, it may be difficult for diverse stakeholders in government, industry, and society to establish consensus on risk-management priorities when potential consequences are not confined to a single stakeholder or category of stakeholders. Potential challenges include:

- defining acceptable risk in specific contexts,
- defining acceptable criteria for transferring risk to other stakeholders,
- setting specific performance standards and goals for risk reduction,
- barriers to information sharing between key stakeholders, and
- gaps in data for assessing effectiveness of risk-management programs.

Risk Management and the Standards Development Process

Stakeholders may engage in established standards development processes to resolve challenges described above and establish consensus on risk-management standards and practices. In the United States, the standards development process encompasses both voluntary and regulatory aspects of the CISR risk-management enterprise. In theory, owner-operators mitigate risks to critical infrastructure by adopting and implementing risk-management standards that have achieved wide recognition and acceptance among diverse stakeholders—oftentimes provided by accredited standards developing organizations (SDOs). Owner-operators may adopt consensus standards for purposes of regulatory compliance or on a voluntary basis. Voluntary reasons may include:

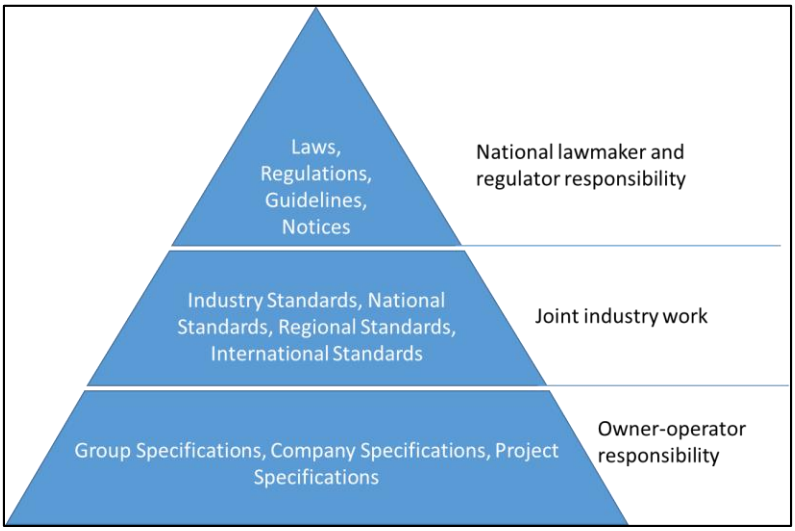
- ensuring national and global systems compatibility and interoperability,
- improving security and resilience of critical systems, assets, and networks to assure business continuity and improve overall sector security,
- providing conformity assurance to business partners and to U.S. and foreign government entities for business and legal reasons,[5]
- mitigating or avoid litigation risk, and
- forestalling or influencing increased government regulation.

Figure 2 provides a hierarchy of standards and the relationship between government regulations and industry standards. Standards regimes may combine multiple elements from one or more tiers.

[5] For example, CACI, "CACI Organization Achieves ISO® 28000 Certification for Supply Chain Security: First U.S. Company to Obtain This International Credential," https://www.businesswire.com/news/home/20130403005272/en/CACI-Organization-Achieves-ISO%C2%AE-28000-Certification-for-Supply-Chain-Security.

Figure 2. Hierarchy of Standards

The Relationship Between Regulatory and Industry Standards



Source: CRS, adapted from International Association of Oil and Gas Producers, Regulators' Use of Standards, 2010, p. 3.

Notes: Standards regimes may combine multiple elements from one or more tiers.

Oil and gas industries covered in this report develop and incorporate voluntary consensus standards into their operations to varying degree depending upon specific business imperatives, risk considerations, and the regulatory environment. In addition, regulatory agencies frequently incorporate voluntary consensus standards into federal regulations by reference. Many industry advocates argue that this allows private-sector stakeholders with relevant technical expertise and experience to develop detailed implementation guidance for regulations, relieving resource-constrained federal agencies of the burden of developing such guidance on their own.[6] Some critics, on the other hand, believe incorporation of voluntary consensus standards into the Code of Federal Regulations by reference may cede important technical aspects of federal oversight to regulated entities and thus weaken affected regulatory regimes.[7] Incorporation of voluntary consensus standards by reference into the Code of Federal Regulations gives them the legal effect of regulatory standards. For more detail on federal roles, authorities, and policies in the national standards system, see **Appendix B**.

Federal Nonregulatory Authorities

Key federal nonregulatory authorities for voluntary CISR programs date to the late 1990s.[8] After the September 11, 2001, terrorist attacks, Congress enacted the Homeland Security Act (HSA) of

[6] For example, Letter from Frank Macchiarola, Vice President, Downstream and Industry Operations, American Petroleum Institute, Christina Sames, Vice President, Operations and Engineering, American Gas Association, Dave Schryver, Executive Vice President, American Public Gas Association, et al., to Office of Electricity, U.S. Department of Energy, August 23, 2019, https://www.ingaa.org/File.aspx?id=36893.

[7] See the Bureau of Safety and Environmental Enforcement (BSEE), "Oil and Gas and Sulphur Operations on the Outer Continental Shelf—Oil and Gas Production Safety Systems," 83 *Federal Register* 49222, September 28, 2018. BSEE summarized public comments made during the rulemaking process that criticized the agency's incorporation by reference of API voluntary consensus standards.

[8] For example, see Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection," May 22, 1998, https://clinton.presidentiallibraries.us/items/show/12762.

2002 (P.L. 107-296), which expanded certain coordination authorities first established under the Clinton Administration and added others. HSA created DHS as the lead agency for implementation of the new CISR coordination authorities. HSA authorizes the Secretary of Homeland Security to create and manage private-sector advisory councils, develop public-private partnerships, provide security-related services, and assist the private-sector in the development and promotion of best practices to secure critical infrastructure.

Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," signed in 2013, directs the Secretary of Homeland Security to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure" in consultation with a wide range of governmental and private-sector stakeholders.[9] DHS created an organizational framework under the 2013 National Infrastructure Protection Plan (NIPP) to implement this guidance.[10] The various NIPP partnership councils may organize certain deliberations under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), which was first established in 2006. The CIPAC Charter has been renewed several times since then, most recently in 2020.[11]

Under certain circumstances, CIPAC provides coordinating councils organized under the NIPP framework and member organizations legal exemption from Federal Advisory Committee Act (FACA; P.L. 92-463) provisions for open meetings, chartering, public involvement, and reporting in order to facilitate discussion between critical infrastructure stakeholders on sensitive topics relating to infrastructure security.[12] The NIPP framework includes several different types of coordination and advisory bodies—organized under the CIPAC charter—to serve each of the 16 critical infrastructure sectors and numerous other subsectors recognized under PPD-21:

- Government Coordinating Councils (GCC). These enable interagency, intergovernmental, and cross-jurisdictional coordination on infrastructure issues of common concern to sector stakeholders. GCCs are comprised of federal, state, local, tribal, and territorial government agency representatives.
- Sector Coordinating Councils (SCC). These are organized and administered by private-sector stakeholders, and maintain an advisory relationship with the federal government, facilitating coordination and information sharing between industry and government.
- Information Sharing and Analysis Centers (ISAC). These independently organized organizations serve their members by providing information about common threats (including cybersecurity) and sharing best practices for mitigation.
- Multi-state and multi-sector coordination councils.

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

[10] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Executive Summary, 2013, p. 1. NIPP 2013 supersedes previous plans published in 2009 and 2006, and remains current policy as of this writing.

[11] See CISA, "Critical Infrastructure Partnership Advisory Council," https://www.cisa.gov/publication/cipac-charter.

[12] Exemptions from FACA are made by the DHS Secretary under authority of section 871(a) of the Homeland Security Act, 6 U.S.C. §451(a). For more information on FACA regulations, see CRS Report R44253, *Federal Advisory Committees: An Introduction and Overview*, by Meghan M. Stuessy.

In addition, the Secretary and certain other department or agency heads may organize federal advisory councils—subject to FACA requirements—that provide expertise from relevant stakeholders and specialists on a range of specific policy areas.

Overall government responsibility for sector coordination belongs to designated federal agencies with sector-relevant responsibilities and expertise, known as Sector Risk-Management Agencies (SRMAs). SRMAs provide sector coordination via leadership of the sector GCCs. The Department of Energy (DOE) is the SRMA for the Energy Sector. DHS and the Department of Transportation (DOT) are the SRMAs for the Transportation Systems Sector. The Transportation Security Administration (TSA), a DHS agency, is the SRMA for the Oil, Gas, and Hazardous Materials Pipeline subsector of the Transportation Systems Sector.

In 2013, following publication of the NIPP, SRMAs led development of sector-specific implementation plans. CISA announced an initiative in late 2020 for SRMAs to refresh these plans in response to a congressional mandate to refresh PPD-21 guidance and the NIPP in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283; FY2021 NDAA).[13] The FY2021 NDAA also established statutory SRMA responsibilities.[14]

Federal Regulatory Authorities

Congress has established certain regulatory authorities for the oil and gas industry. Some federal regulatory programs are based on prescriptive approaches, which mandate compliance with technical standards for equipment, testing protocols, and operating procedures. These programs may also include requirements for the reporting of known vulnerabilities and incidents. Other regulatory programs mandate adoption of risk-management programs for covered critical infrastructure owner-operators. In some cases, federal regulators mandate standards. In others, voluntary consensus standards are incorporated by reference and become mandatory. Programs may include some or all of the following: risk assessments, submission of risk-management plans, mitigation of high-priority hazards, analysis of risk events, and reporting requirements. Although specific authorities, policies, and programs vary, this latter category of regulation generally relies more heavily on the expertise, judgment, and buy-in of private-sector stakeholders in assessing and mitigating risk. As such, it frequently operates in conjunction with public-private partnership structures described in the preceding section.

Table 1 below summarizes the latter category of regulatory authorities—i.e., those that include risk-management requirements as a means of achieving CISR-related policy objectives in the oil and gas subsector. Federal regulatory programs may also adopt hybrid approaches, which include both prescriptive mandates and risk-based performance standards.[15] For example, 30 C.F.R. §250, which covers process safety of offshore oil and gas operations, includes both prescriptive and risk-based performance standards. Subpart H, "Oil and Gas Production Safety Systems," covers design, installation, use, maintenance, and testing of safety equipment, while Subpart S, "Safety and Environmental Management Systems," covers requirements for offshore owner-operators' risk-management programs.

[13] See Sec. 9002, "Sector Risk-Management Agencies."

[14] Ibid.

[15] The Occupational Safety and Health Administration (OSHA) has previously discussed benefits and drawbacks of these various approaches with oil and gas industry stakeholders. See OSHA, "Performance-based Regulatory Models in the U.S. Oil and Gas Industry, Offshore and Onshore," https://www.osha.gov/oil-and-gas-extraction/resources/performance-based-models.

Table 1. Selected Regulations with Risk-Management Requirements

CI Sector (subsector)	Selected Authorities	Implementation
Energy (Oil and Gas)	Maritime Transportation Security Act (MTSA; P.L. 107-295); 33 C.F.R. §§105, 106	Regulated maritime extraction and handling facilities incorporate security assessments into a comprehensive facility security plan.
Energy (Oil and Gas)	Outer Continental Shelf Lands Act (OCSLA; 43 U.S.C. §§1331 et seq); 30 C.F.R. §250	Regulated offshore drilling installations must develop a Safety and Environmental Management System program that includes specified API recommended practices incorporated by reference.
Energy (Oil and Gas)	29 C.F.R. §1910	Regulated facilities must implement process safety management program using "applicable" voluntary consensus standards. Onshore oil and gas exploration and production operations exempt.
Energy (Oil and Gas)	Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (P.L. 113-254). Chemical Facility Antiterrorism Standards (CFATS), 6 C.F.R. §27.230	Regulated facilities must meet risk-based performance standards for physical security and cybersecurity. In oil and gas subsector applies primarily to certain storage facilities, gas processing, and petroleum refineries in midstream and downstream segments meeting high risk criteria.
Transportation Systems (Pipelines)	TSA Security Directive Pipeline-2021-01114 under 49 C.F.R. §114	Regulated facilities must report cybersecurity incidents, designate a Cybersecurity Coordinator to coordinate with federal agencies, and report results of risk assessments to TSA and CISA.
Transportation Systems (Pipelines)	49 C.F.R. §192 Transportation of natural and other gas by onshore pipeline systems	Regulated pipeline operators must implement a process safety risk-management program under ASME voluntary consensus standard incorporated by reference.
Transportation Systems (Pipelines)	Protecting Our Infrastructure of Pipelines and Enhancing Safety (PIPES) Act of 2016 (P.L. 114-183); 49 C.F.R. §60141	Regulated underground gas storage facilities must implement risk-management program under API recommended practices incorporated by reference.

Source: CRS analysis of applicable statutes and regulations.

Notes: API=American Petroleum Institute; ASME=American Society of Mechanical Engineers.

Balancing Coordination and Regulatory Authorities

Policymakers have generally sought to limit the regulatory reach of government within the broader CISR risk-management enterprise. For example, the Clinton-era directive that established the foundations of the current PPD-21 policy framework stated, "we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded

government mandates to the private sector."[16] The Homeland Security Act subsequently created an organization—DHS—with wide-ranging responsibilities, but relatively narrow regulatory authorities.

DHS infrastructure security programs established under PPD-21 focus on enhancing voluntary collaboration with infrastructure security partners at all levels of government and the private sector through information sharing, analysis, training, and coordination, as well as provision of certain services upon request, such as voluntary on-site vulnerability assessments or cybersecurity intrusion detection. DHS and other SRMAs with dual responsibilities for regulation and coordination typically separate the two roles. Nonetheless, federal regulatory and coordination regimes often overlap and mutually influence each other.[17] For example:

- Federal regulatory agencies participate in industry-led initiatives to develop voluntary standards for critical infrastructure security and resilience.
- Federal agencies incorporate voluntary consensus standards for risk management into the U.S. Code of Federal Regulations (C.F.R.) by reference.[18]
- Federal agencies accept accredited third-party verification of private-sector firms' compliance with consensus standards as evidence of compliance with federal regulations in some cases.[19]
- Federal agencies may choose to delegate certain regulatory authorities to industry-led reliability organizations, which develop, promulgate, and enforce mandatory industry standards under federal oversight.
- Federal agencies may choose to defer or limit formal regulation of private-sector risk management in favor of coordination with, or support of, industry-led initiatives, which broadly align with national CISR policy goals.

Oil and Gas Subsector Overview

This section describes risk and risk-management issues affecting the physical and cyber systems and assets that constitute the critical infrastructure of the oil and gas subsector. The subsections below provide a summary overview of the oil and gas subsector characteristics most relevant to critical infrastructure risk management. Readers interested in a broader overview of the energy sector and relevant market and regulatory trends may reference CRS Report R46723, *U.S. Energy in the 21st Century: A Primer*, coordinated by Melissa N. Diaz.

Industry observers frequently describe the U.S. oil and gas industry as having three primary segments—an upstream segment (exploration and extraction); a midstream segment (supply of crude oil and raw gas to refineries and processing plants, and long-distance transmission pipelines); and a downstream segment (petroleum refining and fuel distribution to end users). These correspond approximately with national critical functions outlined above that are specific to the oil and gas, and pipeline subsectors: exploration and extraction of fuels; fuel refining and

[16] PDD-63, op. cit., p. 3.

[17] See ANSI, "How Do Government Agencies Incorporate Sector Standards?" https://www.standardsportal.org/usa_en/standards_system/standards_system_faq.aspx#privatesector.

[18] See 1 C.F.R. §51, "Incorporation by Reference."

[19] For example, see Center for Offshore Safety, "Find a COS-Accredited ASP," https://www.centerforoffshoresafety.org/SEMS-Audit-Providers/Find%20a%20COS%20Accredited%20ASP.

processing fuels; storage of fuel and maintenance of reserves; and transport of materials by pipeline.

Infrastructure of the oil and gas subsector consists of oil and gas wells, refineries, processing plants, and storage terminals, all of which are highly integrated with pipeline and ICT networks. Over 2.8 million miles of domestic pipeline infrastructure—along with terrestrial and maritime transport systems spanning the globe—links the three segments of the oil and gas supply chain together.[20] The critical functions of the oil and gas subsector therefore rely upon highly interconnected systems, assets, and networks for production and distribution.

Exploration and Extraction of Fuels

Many U.S. oil and gas companies have a global footprint. However, in recent years domestic producers have increased exploration and production in the United States through use of hydraulic fracturing and horizontal drilling, unlocking oil and natural gas resources from "unconventional" formations, especially shale. According to the U.S. Energy Information Administration (EIA), the United States was a net annual petroleum exporter in 2020.[21] Approximately 71% of domestically produced crude oil comes from five states, led by Texas with a 43.0% share of the national total, followed by North Dakota (10.4%), New Mexico (9.2%), Oklahoma (4.1%), and Colorado (4.0%). Offshore oil production in the Gulf of Mexico accounts for an additional 14.6% of the national total.[22]

Natural gas extraction is similarly concentrated among top producing states, with about 69% coming from five states: Texas (23.9%); Pennsylvania (21.1%); Louisiana (9.5%); Oklahoma (7.6%); and West Virginia (7.1%). Although there is significant geographic overlap with major oil production centers, there are notable differences. Offshore drilling in the Gulf of Mexico is less dominant in the gas sector, providing 2% of total domestic production.[23]

Fuel Refining and Processing of Fuels

The primary products of crude oil refineries are fuels for transportation, constituting roughly 85% of output.[24] They also provide necessary feedstock for petrochemical manufacturing, lubricants, and other products. Refining capacity is concentrated near Gulf of Mexico seaports, accounting for nearly half of national production of refined fuels. Texas alone accounts for nearly a quarter of this production, with much of its capacity concentrated in the Houston area.[25] Major refineries also exist on the West Coast and in the Midwest to serve regional markets. Between 2000 and 2018, the number of operable domestic refineries decreased from 158 to 129—an 18% drop—while total refining capacity increased by about 9%.[26] Higher utilization of fewer refining assets

[20] PHMSA, "PHMSA by the Numbers," https://www.phmsa.dot.gov/.

[21] Energy Information Administration (EIA), "Oil and Petroleum Products Explained: Oil Imports and Exports," https://www.eia.gov/energyexplained/oil-and-petroleum-products/imports-and-exports.php, accessed October 19, 2021.

[22] EIA, "Oil and Petroleum Products Explained: Where Our Oil Comes From," https://www.eia.gov/energyexplained/oil-and-petroleum-products/where-our-oil-comes-from.php, accessed October 19, 2021.

[23] EIA, "Natural Gas Explained: Where Our Natural Gas Comes From," https://www.eia.gov/energyexplained/natural-gas/where-our-natural-gas-comes-from.php.

[24] American Geosciences Institute, "Oil Refining and Gas Processing: Products of Oil Refining," https://www.americangeosciences.org/geoscience-currents/oil-refining-and-gas-processing.

[25] Greater Houston Partnership, "Data, Insight & Analysis: Gulf Coast Refining Capacity," https://www.houston.org/houston-data/gulf-coast-refining-capacity.

[26] Based on time series data from EIA, "Number and Capacity of Petroleum Refineries," https://www.eia.gov/dnav/pet/

decreases reserve capacity, while increasing the likelihood of supply disruptions, according to experts.

Natural gas usually undergoes field processing to remove associated oil and condensate near the extraction site before being transported via pipeline to gas processing plants. Processing capacity is concentrated in the Gulf Coast region (states with Gulf of Mexico shoreline), accounting for 51% of national capacity.[27] Natural gas has a variety of uses, including for electric power generation, industrial and commercial enterprises, and residential customers. Commercially valuable by-products of this process include natural gas liquids such as ethane, propane, and butane, which can be used for fuel, plastics, or petrochemical feedstock, among other uses.[28]

Pipeline Transport

The Pipeline and Hazardous Materials Safety Administration (PHMSA), a Department of Transportation (DOT) agency, regulates 2.8 million miles of pipelines.[29] Approximately 2.6 million miles of this total consists of natural gas pipelines, with the remainder used for petroleum, refined fuels, and other hazardous liquids. The U.S. natural gas industry uses thousands of miles of largely unregulated (and therefore uncounted) gathering pipelines to transport gas to gas processing plants nationwide.[30] Gathering pipelines typically have lower diameters and operate at lower pressures than long-distance transmission pipelines. After processing, a transmission pipeline network totaling nearly 300 thousand miles is used to transport gas across long distances to regional distribution nodes.[31] A distribution network totaling 2.3 million miles supplies gas to end users.

The rapid growth of U.S. natural gas and crude oil production from shale in the mid-2000s has led to a corresponding realignment and expansion of the nation's pipeline system. Between 2004 and 2019, developers added over 58 thousand miles of hazardous liquids transmission pipeline in the United States, an increase of about 35% in total reported mileage, not counting the expansion of capacity on existing pipelines. Much of this expansion was used to connect major new production regions, such as the Marcellus (Pennsylvania) for natural gas and the Bakken (North Dakota) for oil shale basins, to traditional oil and gas markets, fundamentally reconfiguring oil and natural gas flows throughout North America. During the same period, total mileage for U.S. natural gas transmission remained flat.[32] Oil production from the Bakken increased much faster

PET_PNP_CAP1_DCU_NUS_A.htm.

[27] EIA, "Gulf of Mexico Fact Sheet," https://www.eia.gov/special/gulf_of_mexico/, accessed October 19, 2021.

[28] EIA, "What Are Natural Gas Liquids and How Are They Used?" https://www.eia.gov/todayinenergy/detail.php?id=5930, April 20, 2012. Also see CRS Report R45398, *Natural Gas Liquids: The Unknown Hydrocarbons*, by Michael Ratner.

[29] PHMSA, "PHMSA By the Numbers," https://www.phmsa.dot.gov/.

[30] On November 15, 2021, PHMSA announced it was issuing a final rule, effective May 16, 2022, to require pipeline operators to report safety information for all gas gathering lines—a total of 425 thousand additional miles of pipeline. See PHMSA, "New Federal Regulations Add More Than 400,000 Miles of "Gas Gathering" Pipelines Under Federal Oversight," press release, November 15, 2021, https://www.phmsa.dot.gov/news/new-federal-regulations-add-more-400000-miles-gas-gathering-pipelines-under-federal-oversight; and PHMSA, "Pipeline Safety: Safety of Gas Gathering Pipelines," 86 *Federal Register* 63266, September 14, 2021.

[31] PHMSA, "Annual Report Mileage Summary Statistics," web tables, September 1, 2020, accessible at https://www.phmsa.dot.gov/data-and-statistics/pipeline/annual-report-mileage-summary-statistics; and "Gathering Pipelines FAQs," web page, https://www.phmsa.dot.gov/faqs/gathering-pipelines-faqs.

[32] For more information, see "Pipeline Network Expansion from the Shale Boom," in CRS Report R46723, *U.S. Energy in the 21st Century: A Primer*, coordinated by Melissa N. Diaz.

than pipeline infrastructure could be developed, so rail and trucking also have been used for some time to move significant volumes of oil to market. Natural gas from the Bakken was flared at the production site in significant quantities due to lack of infrastructure to transport it and process it economically.[33]

Fuel Storage and Reserves

Storage facilities are critical to the operation of pipeline networks, and help moderate imbalances between supply and demand in the marketplace.[34] Much of U.S. storage capacity is located in the Gulf Coast and adjacent Midwest states.[35] The United States' largest onshore oil storage and energy market hub is located in Cushing, OK, which has a working capacity of over 75 million barrels—about 13% of national storage capacity.[36] Cushing is a major pipeline terminal that connects North American oil fields with Gulf Coast refineries, and is the physical delivery point for widely-referenced West Texas Intermediate oil futures contracts.[37]

Risk in the Oil and Gas Subsector

Oil and gas production networks are potentially susceptible to a wide range of failures, such as operator error, mechanical breakdowns, design errors, sensor error or malfunction, and mismanagement of critical data. In addition, deliberate attacks or natural events may target or otherwise affect key vulnerabilities of cyber or physical infrastructure. This section describes several characteristics of the oil and gas subsector that may create structural vulnerabilities affecting process safety, physical security, cybersecurity, and supply-chain risk to varying degrees. These include:

- Complex interdependencies of oil and gas infrastructure and supply-chain (third party) risk, and prevalence of hazardous industrial processes throughout the subsector.
- Limited redundancy or spare capacity of production, storage, or transmission assets.
- Decentralized ownership and responsibility structures.
- Geographic concentration of critical systems and assets.
- Increased integration of information and communications technology (ICT) and operational technology (OT).

Exposure of industry production, processing, and distribution systems to specific intentional threats, such as cyberattacks, or generalized hazard phenomena, such as extreme weather and sea-level rise caused by climate change, or pandemic disease, may lead to supply disruptions. The

[33] Production site flaring refers to controlled combustion using flare stacks to burn off excess gas.

[34] The National Petroleum Council, *Dynamic Delivery: America's Evolving Oil and Natural Gas Transportation Infrastructure*, Chapter 2, "Infrastructure Resiliency, Mapping, and Analysis," January 25, 2021, p. 29, https://dynamicdelivery.npc.org/downloads.php.

[35] Regional designations for oil and gas infrastructure follow Petroleum Administration for Defense Districts (PADD) conventions. See EIA, "PADD Regions Enable Regional Analysis of Petroleum Product Supply and Movements," February 7, 2012, https://www.eia.gov/todayinenergy/detail.php?id=4890.

[36] Irina Slav, "The Most Critical Oil Storage in the United States," *Oilprice.com*, May 2, 2020, https://oilprice.com/Energy/Crude-Oil/The-Most-Critical-Oil-Storage-In-The-United-States.html.

[37] Ibid.

following subsections summarize the characteristics listed above and highlight potential vulnerabilities to relevant threats and hazards.

Complex Interdependencies of Oil and Gas Infrastructure and Supply-Chain Risk

The networked structures of oil and gas infrastructure may increase the probability that the local effects of accidents, attacks, and other process disruptions will affect elements of the production and distribution systems, creating supply disruptions. The nation's vast pipeline network connects many key production nodes that process corrosive and flammable hydrocarbons under high temperature and pressure and that are subject to wide variability in operating conditions. These networks are increasingly automated and rely on ICT that may be vulnerable to malicious exploitation. Likewise, in many cases the global shipping network relies upon passage of large vessels through canals and natural chokepoints, which present other hazards. Disruptions, whether intentional, accidental, or from natural causes, may propagate through the global supply chain creating instability in oil and gas markets and disrupting provision of critical inputs to other CI sectors (see text box below).

Limited Redundancy or Spare Capacity

Accidents and other disruptions are relatively commonplace in the oil and gas industry.[38] In many cases, these events affect oil and gas wells, processing plants, and refineries, and may lead to disruptions of proximate upstream or downstream infrastructure. In such cases, the networked character of oil and gas infrastructure may provide some redundancies and resilience. However, some industry observers have questioned whether levels of redundancy and resilience are truly adequate.

A 2018 aviation industry report noted that major airports had been "dangerously close to running out of fuel" after recent pipeline explosions, and that storage scarcity at product terminals had placed airports in a "precarious fuel shortage situation."[39] Independent analyses covering the subsector also identified capacity limitations as a risk factor. A 2017 analysis of 10-K filings by the largest U.S. publicly traded oil and gas companies echoed these concerns, finding that that 89% of respondents reported "insufficient refining, pipeline, storage or trucking capacity" as a

[38] According to congressional testimony by a systems safety expert in response to the Deepwater Horizon incident, "Referring to accidents as 'low probability, high consequence'" is common in the industry, despite a record that indicates otherwise. See U.S. Congress, Senate Committee on Energy and Natural Resources, Oil and Gas Development, Hearing on domestic oil and gas production, safety, and environmental protection, 112th Cong., 1st sess., May 17, 2011, S. Hrg. 112-51 (Washington: GPO, 2011), p. 54. For a searchable database of major oil and gas industry incidents investigated or under investigation by the U.S. Chemical Safety Board (CSB), see CSB, "Investigations," https://www.csb.gov/investigations/. Additionally, many law firms specialize in oil and gas personal injury cases, claiming to have won billions in damages. For example, Zehl & Associates claims over $1 billion recovered for clients in connection with the Deepwater Horizon explosion and a host of lesser known incidents. "Oil Rig Accident and Platform Explosion Lawyers," https://www.zehllaw.com/practice-areas/offshore-injuries/oil-rig-explosions/.

[39] Airlines for America, *Jet Fuel: From Well to Wing*, April 2018, p. 9, https://airlines.org/wp-content/uploads/2018/01/jet-fuel_spreads.pdf. This is an apparent reference to an October 2016 blast in Alabama that affected Colonial Pipeline facilities. See Devika Krishna Kumar, "Colonial May Open Key U.S. Gasoline Line by Saturday After Fatal Blast," *Reuters*, October 31, 2016, https://www.reuters.com/article/us-pipeline-blast-alabama/colonial-may-open-key-u-s-gasoline-line-by-saturday-after-fatal-blast-idUSKBN12V2FC. According to Reuters, a gasoline spill from the pipeline the previous month caused a 12-day interruption to supplies. According to NPC, Washington/Baltimore airports "came within hours of a stock out" as a result of the spill. See NPC, op. cit., p.40.

risk.[40] Likewise, the 2017 analysis found that 85% of respondents reported reliance on third party owned processing facilities and transportation as a concern.[41]

The National Petroleum Council (NPC), a federally chartered and privately funded advisory committee, noted in a 2021 report that there had been an increase of U.S. refinery utilization between 2009 and 2019 from 83% to 93% capacity.[42] "High utilization is preferred for operational and economic efficiency, but high utilization can be seen as a concern when viewed from the perspective of energy resiliency," it said. "With minimal slack in the system, loss of capacity can be significant and create cascading constraints on upstream production."[43]

Incidents affecting fuel delivery to electricity generation plants and gas stations have highlighted this vulnerability. A severe cold weather event in February 2021 disrupted natural gas supplies to electric power plants in Texas—one of several factors that caused extended statewide blackouts leading to loss of life. The May 2021 ransomware attack on Colonial Pipeline Company and subsequent fuel shortages highlighted the lack of spare capacity to transport fuel from the Gulf Coast states to East Coast markets.

Pandemic disease may place additional stresses on limited industry production, processing, and distribution capacity for extended periods. During the early months of the Coronavirus Disease 2019 (COVID-19) pandemic in the United States, public officials issued numerous emergency directives closing nonessential businesses and facilities, limiting travel, and instructing nonessential workers to stay home. These orders frequently exempted oil, gas, and pipeline facilities, as essential businesses. Nonetheless, countermeasures introduced to slow the spread of COVID-19 and protect the health of essential workers, as well as the unpredictable nature of serious outbreaks, presented challenges to the subsector as a whole in staffing existing essential facilities and constructing new ones.[44]

Ownership and Responsibility Structures in the Oil and Gas Subsector

According to observers, the generally fragmented ownership and responsibility structure of the oil and gas industry may present risk—particularly as global supply-chain relationships knit together a wide array of suppliers, contractors, and asset owners in a web of complex interdependencies.[45] Upstream drilling operations require as many as 45 different services, ranging from seismic surveys to facilities engineering and economic analysis.[46] Additionally, upstream operations

[40] BDO, *2017 BDO Oil and Gas Riskfactor Report*, 2017, p. 1, https://www.bdo.com/getattachment/a1bf67be-1beb-42b1-8f0c-f3db2446c6ed/attachment.aspx?2017-Oil-Gas-Riskfactor-Report-Brochure_WEB.pdf; 10-K refers to annual reports filed by publicly traded companies to the U.S. Securities and Exchange Commission, which contain information on company performance and risk factors, among other parameters.

[41] Ibid.

[42] The National Petroleum Council (NPC), *Dynamic Delivery: America's Evolving Oil and Natural Gas Transportation Infrastructure*, Chapter 2, "Infrastructure Resiliency, Mapping, and Analysis," January 25, 2021, p. 2-24, https://dynamicdelivery.npc.org/downloads.php.

[43] Ibid.

[44] CRS In Focus IF11476, *COVID-19: Response of the Oil and Gas Pipelines Sector*, by Paul W. Parfomak.

[45] For example Elizabeth Paranhos, Tracy G. Kozak, and William Boyd, *Highly Reliable Organizations in the Onshore Natural Gas Sector: An Assessment of Current Practices, Regulatory Frameworks, and Select Case Studies*, Joint Institute for Strategic Energy Analysis, NREL/SR-6A50-67941, July 2017, p. ix.

[46] Christopher M. Chima, "Supply-Chain Management Issues In the Oil and Gas Industry," *Journal of Business & Economics Research*, vol. 5, no. 6 (June 2007), p. 28.

Unmanaged Risk and Disruption of Critical Supply Functions

A series of explosions and fires at the Enterprise Products Midstream Gas Plant in Pascagoula, MS, on June 27, 2016, caused extensive damage and took the facility offline for six months. Upstream production from offshore drilling platforms was rerouted via pipeline to other processing facilities, but capacity restrictions forced curtailment of offshore gas production during this period from 400 million cubic feet per day to 330 million cubic feet per day—an 18% reduction.[48]

A report by the U.S. Chemical Safety Board (CSB), a nonregulatory accident investigation agency, determined that the proximate cause of the incident was failure of industrial equipment due to thermal stress after an unplanned production halt. The production halt itself was caused by a lightning strike downstream of the plant that disabled pipeline operations, leaving the plant unable to offload its production of natural gas liquids and fuel.

The investigation also highlighted systemic risk-management issues that may have increased the facility's vulnerability to contingent events, such as unplanned shutdowns. Although the plant operators were required to administer a process safety management program under 29 C.F.R. §1910, the regulation gave them discretion to apply "appropriate" industry standards.

Several relevant technical standards developed by different SDOs were "not fully consistent with each other and lacking in clarity." Additionally, CSB found that many oil and gas companies had systematically withheld relevant process safety data from each other in order to safeguard proprietary information and avoid potential regulatory consequences. Plant operators therefore failed to fully understand equipment vulnerabilities or their overall risk exposure.

depend upon transport of heavy industrial equipment, chemicals, concrete, and other supplies across sometimes remote and challenging geographies.[47] Separate companies—each competing within the broader sector—provide many of these services.

According to one academic analysis of supply-chain risk in the oil and gas industry, competitive business pressures may complicate collective efforts to improve security within the oil and gas sector as a whole. "One of the weaknesses of a supply-chain is that each company is likely to act in its best interests to optimize its profit," with no single entity responsible for management of the supply-chain as a whole.[49] Additionally, the prevalence of separate information systems may present management challenges and complicate information sharing. "Difficulties can arise when oil and gas companies make technology decisions independently along their supply-chains," the study states. "Thus, their information systems are neither coordinated nor compatible, and information is not readily shared back and forth along the supply-chain."[50]

Development and deployment of new ICT technology may help mitigate some of these risks. For example, ICT OT are increasingly integrated throughout the oil and gas subsector, which may enable better communication and coordination between multiple owners, managers, operators, contractors, and subcontractors managing complex projects. According to one analyst, "oil and gas companies are creating a stronger and more comprehensive connection between field operations staff and remote experts" by using "digital oilfield" technologies based on use of real-time production data and automated workflow and data management tools.[51] However, such technologies may create cybersecurity vulnerabilities, even as they may increase supply-chain transparency and coordination.

Additionally, some analysts have suggested that risks associated with fragmented ownership and responsibility structures are mitigated to a degree by vertical integration within the oil and gas

[47] Chima, ibid.

[48] Jeff Amy, "Pascagoula Natural Gas Plant Still Closed After June 27 Fire," *Tuscaloosa News*, July 8, 2016, https://www.tuscaloosanews.com/business/20160708/pascagoula-natural-gas-plant-still-closed-after-june-27-fire.

[49] Chima, ibid, p. 34.

[50] Ibid.

[51] Roberta Bigliani, *Reducing Risk in Oil and Gas Operations*, White Paper, May 2013, p. 9.

industry across industry segments, which may facilitate standardization and institution of centralized risk-management.[52] Sometimes referred to as oil majors, these companies own assets in all segments of the value chain linking oil and gas fields with end markets. However, other observers question whether corporate ownership of diverse assets across industry segments necessarily translates into increased operational integration of those assets.[53] Furthermore, some analyses indicate that current trends in the industry indicate increased specialization across segments, rather than integration—in part because specialization may be more economically efficient at the company level and provide higher returns to investors.[54]

According to the Natural Gas Council, an industry group, several operational capabilities lower supply risk due to failures of any given system, asset, or network. These include extensive networked interconnections that allow rerouting of deliveries; parallel pipelines to allow bypass if needed; "line packing" to compress excess gas in pipelines, and geographically dispersed production and storage.[55]

Geographic Concentration of Critical Systems and Assets

The concentration of oil and gas extraction, processing, and transport facilities in the Gulf Coast region raises concerns among many about exposure to increasingly frequent extreme weather events and persistent coastal flooding, which most scientists attribute to sea level rise and long-term weather patterns caused by climate change. Large-scale removal of offshore underground hydrocarbons by oil and gas drilling also increases risk of coastal flooding.[56] Hurricanes may force preemptive closure of offshore drilling assets. In addition, they may directly damage drilling platforms, refineries, and pipeline infrastructure, or indirectly affect their operations by damage to the electric grid or disruptions to local communities that provide essential workers and services. Post-storm impacts may potentially persist for weeks or months afterwards, causing fuel shortages and price spikes, prompting the industry to develop financial risk-management tools.[57]

---

[52] For an early example of this analysis, see Mead, David E. "Effect of Vertical Integration on Risk in the Petroleum Industry," *The Quarterly Review of Economics and Business*, 18, no. 1 (1978).

[53] Tyler Crowe, "Integrated Oil and Gas Isn't Really That Integrated Anymore," *The Motley Fool*, September 1, 2014, https://www.fool.com/investing/general/2014/09/01/integrated-oil-gas-isnt-really-that-integrated-any.aspx.

[54] See Kearney, *Challenging the Integrated Oil and Gas Model*, https://www.kearney.com/energy/article/?/a/challenging-the-integrated-oil-and-gas-model; and Fernando Barrera-Rey, *The Effects of Vertical Integration on Oil Company Performance*, The Oxford Institute for Energy Studies, WPM 21, October 1995, https://www.oxfordenergy.org/wpcms/wp-content/uploads/2010/11/WPM21-TheEffectsofVerticalIntegrationonOilCompanyPerformance-FBarreraRey-1995.pdf.

[55] American Petroleum Institute, American Gas Association, and Interstate Natural Gas Association of America, *Natural Gas: Reliable and Resilient*, August 2018, p. 2, http://ongsubsector.com/documents/NaturalGasResilience-Whitepaper.pdf, also NPC, op. cit., p. 60.

[56] Council on Foreign Relations, *Climate Risk Impacts on the Energy System*, June 14, 2019, https://www.cfr.org/report/climate-risk-impacts-energy-system; also The National Petroleum Council, *Dynamic Delivery: America's Evolving Oil and Natural Gas Transportation Infrastructure*, Chapter 2-Infrastructure Resiliency, Mapping, and Analysis, January 25, 2021, https://dynamicdelivery.npc.org/downloads.php. The report outlines infrastructure hardening efforts, but states "the fact remains that geographic concentration of refineries is a vulnerability and threat to resiliency," p.28. See p.78, ibid, for a description of similar vulnerabilities of Gulf Coast natural gas processing plants and natural gas liquids fractionators to hurricanes and seismic events.

[57] See Negar Dahitaleghani, "Analysis of Disruptions in the Gulf of Mexico Oil and Gas Industry Supply Chain and Related Economic Impacts," (Ph.D. Dissertation, Louisiana State University and Agricultural and Mechanical College, 2016), pp. 11-19, https://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=4966&context=gradschool_dissertations. For a recent example, see EIA, "Today in Energy: Hurricane Ida Disrupted Oil Production and Refining Activity," September 16, 2021, https://www.eia.gov/todayinenergy/detail.php?id=49576.

Weather-related disruptions may also affect the supply of petrochemicals used in the chemical and critical manufacturing sectors.[58]

Seismic events may affect infrastructure assets located well inland, but connected to the Gulf Coast refineries. A 2015 study funded through the U.S. Geological Survey's National Earthquake Hazards Reduction Program highlighted risks from man-made earthquakes to the major oil storage complex and pipeline hub in Cushing, OK, which supplies many Gulf Coast refineries (see "Fuel Storage and Reserves" section). According to the study, wastewater injection from local oil and gas production operations in Oklahoma might produce significant seismic hazards that could cause "moderate to heavy damage to storage tanks in the Cushing facility" in the event of a moderate-magnitude earthquake.[59] Significant damage or other disruptions to the complex may upset oil markets, given the role it plays in setting prices. In 2020, reports that storage facilities in Cushing, OK, were approaching capacity led to an oil price collapse during the economic downturn caused by the COVID-19 pandemic.[60]

Integration of Information and Communications Technology

As in other sectors, increased integration of electronic sensing, automation, and connectivity, may create potential attack surfaces for malicious actors.[61] A 2018 report by the Oil and Natural Gas (ONG) SCC states, "The natural gas and oil industry faces the threat of cyberattacks from a variety of malicious actors including nation states, criminal organizations and unaffiliated bad-actors seeking to steal intellectual property and/or compromise industrial control systems (ICS), among many other nefarious goals."[62] According to the report, threats include automated cyberattacks, insider attacks, cyber supply-chain tampering or disruption, and counterfeit devices with embedded malware.[63]

[58] For example, Rebecca Trager, "Polar Storm Paralyses U.S. Gulf Coast Petrochemical Sector," *Chemistry World*, February 24, 2021, https://www.chemistryworld.com/news/polar-storm-paralyses-us-gulf-coast-petrochemical-sector/4013306.article.

[59] D.E. McNamara, G.P. Hayes, and H.M. Benz, et al., "Reactivated Faulting Near Cushing, Oklahoma: Increased Potential for a Triggered Earthquake in an Area of United States Strategic Infrastructure," *Geophysical Research Letters*, vol. 42, no. 20 (October 8, 2015).

[60] "Oil Prices Collapse Again," *New York Times*, April 28, 2020, https://www.nytimes.com/2020/04/27/business/coronavirus-stock-market-tracker.html; and CRS Insight IN11354, *Crude Oil Futures Prices Turn Negative*, by Michael Ratner and Heather L. Greenley.

[61] See Lawrence Livermore National Laboratory (LLNL), *Dragonstone Strategy—State of Cybersecurity in the Oil & Natural Gas Sector*, LLNL-TR-805864, February 5, 2020, pp. 10 and 14 (hereinafter, LLNL Report). The Oil and Natural Gas (ONG) ISAC shared a 2017 cybersecurity analysis with its members that highlighted an attack, which targeted industrial control systems (ICS) and was designed to cause physical damage and shutdown operations. The sophistication of the attack indicated state sponsorship. According to the analysis, increasing integration of autonomous sensing and controls with process control and information system networks that allow remote operation of industrial processes is increasing risk. See Blake Johnson, Dan Caban, and Marina Krotofil, et al., *Attackers Deploy New ICS Attack Framework 'Triton' and Cause Operational Disruption to Critical Infrastructure*, Mandiant, December 14, 2017, https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton.

[62] Oil and Natural Gas Sector Coordinating Council (ONG SCC), *Defense in Depth: Cybersecurity in the Natural Gas and Oil Industry*, 2018, p. 8, https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

[63] Ibid, p. 8.

A 2020 report submitted by the Lawrence Livermore National Laboratory (LLNL) to DHS on the state of cybersecurity in the oil and gas sector noted several subsector-specific characteristics of the oil and gas industry that may increase vulnerability to cyber-related threats:[64]

- Wide geographic distribution, including offshore and other hard-to-access locations, heightening reliance on potentially vulnerable remote-access process monitoring and controls;
- Data networks between on and offshore facilities, and insufficient segmentation of data networks—breaches in one network may compromise others;
- Interconnected assets at all stages of production process (upstream, midstream, downstream);
- Large quantity of legacy assets lacking cybersecurity features, and widespread reliance on consumer-grade operating systems and software with known vulnerabilities;
- Use of computer technology focusing on productivity; cybersecurity is "an afterthought";
- Underdeveloped capacity to find or track malware, allowing adversaries to maintain presence in systems "for months or years to collect data and identify weaknesses";[65]
- Poor physical security of data storage facilities; and
- Limited "cybersecurity culture."[66]

Risk Management in the Oil and Gas Subsector

Coordinated risk-management programs based on voluntary consensus standards and practices in the oil and gas industry vary within critical functional areas (exploration and extraction; fuel refining and processing; storage and reserves; and pipeline transit), and risk-management category (process safety; physical security; cybersecurity; and supply-chain security and resilience). Programs and practices in each critical functional area may also be informed by formal and informal information sharing—or in some cases mandatory disclosure requirements—which also vary by segment and domain.

Federal regulation in some form is present in nearly every functional area of the subsector, but varies in how and where it is applied. (See **Table 1** above for summary of regulatory authorities.) In general, prescriptive regulatory mandates are favored across industries where incident impacts are potentially catastrophic and elicit broad public concern.[67] By contrast, industry-led efforts may apply more broadly "as risks become more privatized" and "harms are more divisible and isolated with respect to their impacts."[68]

[64] LLNL Report, p. 12.

[65] Ibid.

[66] Ibid.

[67] See P. W. Huber, "The Bhopalization of U.S. Tort Law," *Issues in Science and Technology*, 2/1, 1985, pp. 73–82; David Demeritt, Henry Rothstein, Anne-Laure Beaussier, and Michael Howard, "Mobilizing Risk: Explaining Policy Transfer in Food and Occupational Safety Regulation in the UK," *Environment and Planning*, A 47, no. 2, 2015, pp. 373-391.

[68] May, Peter J., and Chris Koski, "Addressing Public Risks: Extreme Events and Critical Infrastructures," *Review of Policy Research*, vol. 30, no. 2, 2013, p. 156.

Development of specific regulatory regimes in the oil and gas industry follow this general rule, with new regulations often mandated in the wake of widely publicized incidents that cause multiple fatalities or wide scale economic disruption. Examples include the catastrophic loss of the Deepwater Horizon offshore drilling rig in 2010, and more recently, the 2021 ransomware attack on the Colonial Pipeline that disrupted fuel supplies on the East Coast. Conversely, increased regulation has not occurred in the wake of less publicized incidents in more remote locations—particularly in onshore drilling and exploration.

Federal Regulatory Regimes

This section provides an overview of regulation-based risk-management programs within each of the functional areas of the oil and gas industry summarized in **Table 2** below.[69] Not all areas are subject to regulation, and the scope, organization, and extent of regulatory programs varies across areas.

Table 2. Oil and Gas Subsector Regulation by Risk Type and Critical Function

Lead federal regulatory agencies

	Process Safety	Physical Security	Cybersecurity	Supply Chain
Exploration and Production (offshore)	BSEE	USCG	USCG	
Exploration and Production (onshore)				
Fuel Refining and Processing	OSHA	CISA	CISA	
Storage and Reserves	OSHA	CISA	CISA	
Pipeline Transport	PHMSA	TSA	TSA	

Source: CRS analysis of federal agency sources and relevant sections of C.F.R.

Notes: Blank cells indicate no federal regulatory oversight of risk-management plans or practices. CISA oversight applies only to designated high risk facilities subject to CFATS requirements for facility security plans. TSA has not issued physical security regulations for pipelines. Abbreviations: BSEE=Bureau of Safety and Environmental Enforcement, Interior; CISA=Cybersecurity and Infrastructure Security Agency, Homeland Security; OSHA=Occupational Safety and Health Administration, Labor; PHMSA=Pipeline and Hazardous Materials Safety Administration, Transportation; TSA=Transportation Security Administration, Homeland Security; and USCG=U.S. Coast Guard, Homeland Security.

As described in the four subsections below, regulatory regimes vary in their scope and extent.

Regulation of Exploration and Production of Oil and Gas

The U.S. Coast Guard (USCG) implements regulations codified under the Maritime Transportation Security Act (MTSA). Regulations cover physical security and cybersecurity for offshore installations and related onshore (or maritime facing) facilities. USCG requires regulated entities to conduct a security assessment and submit a facility security plan every five years,

[69] Onshore and offshore exploration and production—a single function in the CISA National Critical Function Set—are shown separately here for clarity.

which covers a wide range of physical security requirements. Examples include layout and access points of the covered facility; number, reliability, and security duties of facility personnel; and procedures for controlling keys and other access prevention systems. Specific cybersecurity guidance is limited to two provisions requiring regulated entities to describe measures to protect "radio and telecommunication systems, including computer systems and networks" as part of the assessment that informs the facility security plan.[70] A subsequent USCG Navigation and Vessel Inspection Circular provided voluntary guidelines to describe how general security provisions might be specifically applied to cybersecurity.[71]

The Bureau of Safety and Environmental Enforcement (BSEE), a Department of the Interior agency, implements regulations codified under the Outer Continental Shelf Lands Act (OCSLA) that cover safety of production systems.[72] BSEE provides detailed regulatory guidance on process safety and incident reporting for offshore drilling installations, including industry-developed voluntary consensus standards incorporated by reference into the Code of Federal Regulations, which include both prescriptive specifications for equipment, testing, and operational protocols, and risk-based performance standards. Although both are mandatory, the Safety and Environmental Management System (SEMS) framework codified in subpart S of 30 C.F.R. §250 (see the "Federal Regulatory Authorities" section) aligns more closely with risk-management approaches promoted via the voluntary CISR framework outlined in PPD-21 and the 2013 NIPP.

In recent years, regulations for Oil and Gas Production Safety Systems under subpart H of 30 CFR §250, which mandates compliance with regulations, codes, and standards for process safety, have been subject to repeated rulemakings. They have generally faced greater industry resistance than subpart S, which describes risk-management mandates. BSEE characterized the most recent rulemaking in 2017—which revised an earlier 2016 rule—as necessary to simplify requirements and relieve industry of unnecessary compliance burdens.[73] Some environmental groups and industrial safety advocates raised concerns over certain revisions relaxing third-party certification requirements, incident reporting, and BSEE acceptance of revised voluntary consensus standards developed by the American Petroleum Institute (API)—which acts both as an industry advocacy group and ANSI-certified SDO.[74]

No industry-specific federal regulations for physical or cybersecurity, process safety, or supply chain risk management exist for onshore production facilities—which tend to be regulated by state agencies. However, state regulations do not necessarily address the risk categories listed above.[75] Furthermore, the onshore drilling industry is exempt from OSHA's Process Safety Management (PSM) Standard, which regulates handling of hazardous chemicals in a wide range of covered industries.[76]

---

[70] 33 C.F.R. 105.305.

[71] Admiral Karl L. Schultz, Commandant, *Navigation and Vessel Inspection Circular*, U.S. Coast Guard, No. 01-20, Washington, DC, February 26, 2020, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023.

[72] 30 C.F.R. §250.

[73] Bureau of Safety and Environmental Enforcement (BSEE), "Oil and Gas and Sulphur Operations on the Outer Continental Shelf—Oil and Gas Production Safety Systems," 83 *Federal Register* 49216, September 28, 2018.

[74] BSEE, ibid, "General Comments on Incorporation by Reference of Industry Standards," p. 49223.

[75] See U.S. Chemical Safety and Hazard Investigation Board (CSB), *Investigation Report*, "Gas Well Blowout and Fire at Pryor Trust Well 1H-9," June 12, 2019, p. 107, https://www.csb.gov/pryor-trust-fatal-gas-well-blowout-and-fire/.

[76] For discussion of regulatory history for process safety in the onshore upstream segment, see CSB, ibid., pp. 101-107, https://www.csb.gov/pryor-trust-fatal-gas-well-blowout-and-fire/.

Regulation of Fuel Refining and Processing of Fuels

OSHA requires covered entities such as oil refineries and natural gas processing facilities to develop a process safety management plan under 29 C.F.R. §1910, to be updated every five years. The plan must include process hazard analysis, employee training, incident investigation, and reporting, among other components. Physical systems covered include pressure vessels and storage tanks; piping systems and valves; relief and vent systems and devices; emergency shutdown systems; controls (including monitoring devices and sensors, alarms, and interlocks); and pumps. The regulation contains prescriptive elements, but also requires implementation of risk-management programs for process safety. It grants covered entities wide discretion in applying available standards to risk-management activities. Published implementation guidance names several industry SDOs as possible sources for standards, but does not incorporate specific standards into the regulation by reference.[77]

CISA administers the Chemical Facility Antiterrorism Standards (CFATS) program under 6 C.F.R. §27. Under the program, all facilities that store or process threshold amounts of certain "chemicals of interest" must notify CISA. CISA may designate certain facilities as high-risk, using an agency risk assessment methodology. Depending on risk tier (1-4), facility owner-operators must submit a vulnerability assessment and site security plan that meets the CISA risk-based performance standards for physical security and cybersecurity. CISA conducts inspections of regulated facilities to ensure compliance. CISA does not publicly disclose vulnerability or threat information provided by covered facilities.[78] In the oil and gas subsector, CFATS applies primarily to certain storage facilities, gas processing, and petroleum refineries in midstream and downstream segments meeting high risk criteria.[79]

Regulation of Fuel Storage and Reserves

PHMSA, a Department of Transportation (DOT) agency under 49 C.F.R. §192,[80] regulates large underground natural gas storage facilities under the Protecting Our Infrastructure of Pipelines Enhancing Safety (PIPES) Act of 2016 (P.L. 114-183). Among other provisions in the PIPES Act, Congress mandated new regulations in response to the 2015 Aliso Canyon incident in California—a large natural gas leak from an underground salt cavern being used as a storage facility that caused health hazards and "serious energy-supply challenges for the region."[81]

PHMSA issued a final rule on February 12, 2020, that modified an earlier interim final rule issued on December 19, 2016.[82] Both rules incorporated by reference two API recommended practices already in wide use.[83] The interim rule required that recommended practices in the API

[77] See 29 C.F.R. §1910.119, "Appendix C."

[78] See CISA, "CFATS Process", https://www.cisa.gov/cfats-process.

[79] Letter from Frank Macchiarola, Vice President, Downstream and Industry Operations, American Petroleum Institute; Christina Sames, Vice President, Operations and Engineering, American Gas Association; and Dave Schryver, Executive Vice President, American Public Gas Association, et al., op. cit., p. 3.

[80] CRS Insight IN11162, *PHMSA's Pipeline Safety Reauthorization: Funding Issues*, by Paul W. Parfomak.

[81] Pipeline and Hazardous Materials Safety Administration, "Pipeline Safety: Safety of Underground Natural Gas Storage Facilities," 85 *Federal Register* 8107, February 12, 2020, https://www.federalregister.gov/documents/2020/02/12/2020-00565/pipeline-safety-safety-of-underground-natural-gas-storage-facilities.

[82] Ibid, "Summary of the Major Provisions," pp. 8104-8127.

[83] See API RP 1170, "Design and Operation of Solution-Mined Salt Caverns Used for Natural Gas Storage" (First Edition, July 2015); and API RP 1171, "Functional Integrity of Natural Gas Storage in Depleted Hydrocarbon Reservoirs and Aquifer Reservoirs" (First Edition, September 2015).

documents be applied as mandatory. However, the final rule relaxed this provision, making recommended practices voluntary. PHMSA also relaxed deadlines for operators to develop integrity management programs and conduct baseline risk assessments, among other changes.[84]

Regulation of Pipeline Transport

Gathering pipelines—considered part of the midstream segment—are used to transport oil and gas from extraction sites to central collection points for processing. These are not currently regulated outside of populated areas or defined "unusually sensitive" areas that include a drinking water source or ecological resource.[85]

PHMSA regulates long-distance transmission and regional distribution pipelines, with a focus on enforcing mandatory safety standards. This regulatory mission correlates most closely with the process safety risk category (see the "Organization, Methods, and Scope of Report" section). Readers interested in further information on pipeline safety regulations may refer to CRS Report R44201, *DOT's Federal Pipeline Safety Program: Background and Key Issues for Congress*, by Paul W. Parfomak.

The Transportation Security Administration (TSA) within DHS administers the federal program for pipeline security—both physical and cyber. (Additionally, pipelines connected to certain facilities covered by CFATS are considered part of those facilities and therefore are subject to CISA regulation under 6 C.F.R. §27.)

The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established TSA, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). 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)). TSA in the past favored industry compliance with voluntary guidelines for pipeline physical security and cybersecurity.[86] Both TSA and the pipeline industry maintained that regulations were unnecessary because pipeline operators voluntarily implemented security programs.[87] For more information on the historical and current federal role in pipeline cybersecurity, see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran.

The May 2021 ransomware attack against the Colonial Pipeline Company spurred panic buying and fuel shortages along the Eastern Seaboard. Although the attack did not appear to target pipeline control systems, it forced the temporary suspension of fuel shipments via a major pipeline network, according to a company statement.[88] In the wake of this incident, the Biden Administration announced Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity," on May 12, 2021, which created cybersecurity and information-sharing

[84] Ibid, pp. 8104-8105. On November 15, 2021, PHMSA announced new regulations. See footnote 31 for details.

[85] See PHMSA, "Fact Sheet: Gathering Pipelines," https://primis.phmsa.dot.gov/comm/factsheets/fsgatheringpipelines.htm. On November 15, 2021, PHMSA announced it was issuing a final rule, effective May 16, 2022, to increase regulations on gathering pipelines. See footnote 31 for details.

[86] Transportation Security Administration (TSA), *Pipeline Security Guidelines*, March 2018, p. 1, https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

[87] See CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran, for more info.

[88] See, Colonial Pipeline Company, "Media Statement Update: Colonial Pipeline System Disruption," press release, May 17, 2021, https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption. An earlier statement released on May 7, 2021, announcing the disruption is no longer on the company website.

requirements applicable to federal agencies and government contractors. Administration officials voiced hopes that the E.O. 14028 would compel private-sector owner-operators of pipelines and other infrastructure to improve risk-management and information-sharing practices in these areas as a condition of doing business with the federal government.[89]

Additionally, TSA issued an emergency security directive—which has the effect of a regulation—for pipeline cybersecurity in May 2021 following the Colonial Pipeline ransomware attack. TSA Security Directive Pipeline-2021-01, issued under authorities provided by 49 C.F.R. §114, required regulated pipeline operators to report cybersecurity incidents, provide a cybersecurity coordinator to liaise with TSA and CISA as needed "to coordinate cybersecurity practices and address any incidents that arise," and to review current activities against TSA voluntary guidelines and to implement mitigation measures, and report results to TSA and CISA.[90] A second directive in July 2021 elaborated on requirements in the first directive.[91] Although existing authorities also cover physical security, TSA has not similarly exercised those authorities to date.

Voluntary Consensus Standards, Public-Private Partnerships, and Information Sharing

In recent decades, a variety of public-private partnerships for risk management and information sharing have developed in the oil and gas subsector. These programs and activities include development of voluntary consensus standards, public-private partnerships for policy or operational coordination, and information-sharing programs. These programs and activities may encompass one or more risk categories covered in this report (i.e., process safety; physical security; cybersecurity; supply-chain security and resilience), and may likewise apply to a specific critical functional area of the oil and gas subsector, the oil and gas subsector as a whole, or critical infrastructure in general.

[89] The White House, "Background Press Call by Senior Administration Officials on Executive Order Charting a New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," press release, May 12, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/12/background-press-call-by-senior-administration-officials-on-executive-order-charting-a-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/; also CRS Insight IN11683, *Critical Infrastructure Policy: Information Sharing and Disclosure Requirements After the Colonial Pipeline Attack*, by Brian E. Humphreys.

[90] Transportation Security Administration, *Security Directive Pipeline 2021-01*, Enhancing Pipeline Security, Springfield, VA, May 28, 2021, p. 1.

[91] See Transportation Security Administration, *Security Directive Pipeline 2021-02*, Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing, Springfield, VA, May 28, 2021. The directive is not officially available to the public. For a summary, see U.S. Government Accountability Office, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, GAO-21-105263, July 27, 2021, p. 1, https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2021/08/gao-critical-infrastructure-protection-july-2021.pdf.

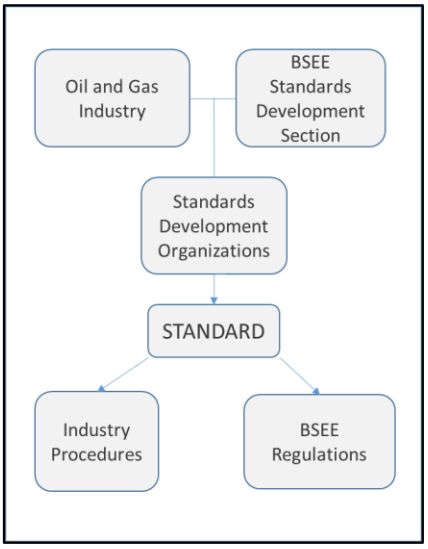
Voluntary Consensus Standards and Recommended Practices in the Oil and Gas Subsector

Voluntary consensus standards and recommended practices for infrastructure risk management in the oil and gas subsector have developed unevenly across industry segments over time, focusing primarily on those segments with a history of federal regulatory oversight or interest, such as offshore production facilities, refineries, and pipeline networks. Federal regulatory regimes, public-private coordination programs and activities, and voluntary consensus standards within the subsector often develop in conjunction with each other, via both formal and informal processes.

In some cases, industry standards and recommended practices are developed with participation of regulatory agencies in accordance with standing federal policy guidance promulgated under authority of the National Technology Transfer and Advancement Act (NTTAA) of 1995 (P.L. 104-113), and may either be incorporated into the C.F.R. by reference, or else left for private-sector entities to adopt on a voluntary basis.[92]

Figure 3. BSEE Standards Development Process

Agency and Private-Sector Collaboration



Source: Adapted from BSEE Standards Development Section, https://www.bsee.gov/what-we-do/offshore-regulatory-programs/the-standards-development-section-sds.

For example, BSEE maintains an office for joint standards development with private-sector stakeholders, known as the Standards Development Section (SDS). According to an agency website, "BSEE has a long history of using industry standards to supplement and enhance its regulatory program." Further, "As of December 2020, BSEE has incorporated by reference 125 industry standards in its regulations"[93] **Figure 3** (above) illustrates the BSEE standards development process.[94]

[92] According to OMB Circular 119, "Agencies must consult with voluntary consensus standards bodies, both domestic and international, and must participate with such bodies in the development of voluntary consensus standards when consultation and participation is in the public interest and is compatible with their missions, authorities, priorities, and budget resources," Office of Management and Budget, Executive Office of the President, *OMB-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, Washington, DC, January 2016, p. 27, https://www.nist.gov/system/files/revised_circular_a-119_as_of_01-22-2016.pdf. See **Appendix B** in this report for further detail.

[93] BSEE Standards Development Section, "Standards, Safety, and Industry Cooperation," https://www.bsee.gov/what-we-do/offshore-regulatory-programs/the-standards-development-section-sds.

[94] Other relevant agencies similarly report participation in standards development. See USCG, http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Commercial-Regulations-standards-CG-5PS/; DOT, "Standards Incorporated by Reference," https://www.phmsa.dot.gov/standards-rulemaking/pipeline/standards-incorporated-reference.

In other cases, voluntary consensus standards and recommended practices are not formally incorporated into a regulatory framework. For example, a 2021 revised edition of API Standard 1164,"Pipeline Control Systems Cybersecurity," intended for regulated pipeline operators, was based on nonmandatory guidance from TSA Pipeline Security Guidelines (March 2018) and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[95] Even though TSA has long had the authority to regulate pipeline physical security and cybersecurity, it relied on voluntary industry adoption of its cybersecurity guidelines through the consensus process as the preferred means to advance CISR goals until 2021.[96] Industry groups have argued that incorporation of federal voluntary guidelines into voluntary consensus standards is preferable to regulation.[97] However, the Colonial Pipeline ransomware attack appeared to contradict this argument, prompting TSA to revise its stance on regulatory restraint and issue its mandatory cybersecurity directives.[98]

API standards and recommended practices for risk management across national critical functions in the oil and gas industry largely align with existing regulatory oversight programs.[99] A CRS review of relevant API documents illustrates the general pattern of alignment between industry-led standards development and regulatory requirements for risk management. **Table 3** summarizes voluntary consensus standards and recommended practices for risk management developed by API.[100]

[95] See API Publications Store, *Pipeline Control Systems Cybersecurity*; Third Edition, August 2021, https://www.apiwebstore.org/publications/item.cgi?49847b7d-0a43-4d96-b0e2-b56d9acb6f2e.

[96] CRS Insight IN11060, *Pipeline Security: Homeland Security Issues in the 116th Congress*, by Paul W. Parfomak.

[97] For example, see Interstate National Gas Association of America, *Pipeline Cyber & Physical Security*, 2021, https://www.ingaa.org/File.aspx?id=34999&v=5c0904b.

[98] Some Senate Members have since expressed concerns that TSA may have exercised its authorities improperly by not fully engaging in established consultative and collaborative processes with pipeline industry stakeholders. See Letter from Hon. Rob Portman, Ranking Member, Committee on Homeland Security and Government Affairs, Hon. James Lankford, Ranking Member, Subcommittee on Government Operations and Border Management, Committee on Homeland Security and Governmental Affairs, and Hon. M. Michael Rounds, U.S. Senator, to Hon. Joseph V. Cufari, Inspector General, Department of Homeland Security, October 28, 2021, https://www.hsgac.senate.gov/imo/media/doc/2021-10-28%20RP%20Lankford%20Rounds%20to%20Cuffari%20re%20TSA%20Security%20Directives.pdf.

[99] In its investigation of a 2018 oil rig explosion in Oklahoma, CSB noted that the well operator did not use API Bulletin 97, *Well Construction Interface Guidelines*, a potentially applicable process safety document, because, "API Bulletin 97 implies it applies solely to the offshore drilling industry, not the onshore drilling industry. Application and implementation of API Bulletin 97 guidance could have helped to prevent the incident. There is also no regulatory requirement for developing a Well Construction Interface Document for land drilling operations. Such a requirement could improve the safety of U.S. land drilling operations." See CSB, *Investigation Report*, Gas Well Blowout and Fire at Pryor Trust Well 1H-9, Washington, D.C., June 12, 2019, p. 100, https://www.csb.gov/pryor-trust-fatal-gas-well-blowout-and-fire/.

[100] Analysis of performance-based risk-management standards and recommended practices from API standards catalog. CRS reviewed the following catalog sections: "Exploration and Production"; "Marketing"; "Transportation"; "Refining"; and "Safety and Fire Protection." See API, "Purchase API Standards and Software," https://www.api.org/products-and-services/standards/purchase?.

Table 3. API Standards Documents by Risk Type and Critical Function

Voluntary Consensus Standards for Risk Management in the Oil and Gas Subsector

	Process Safety	Physical Security	Cybersecurity	Supply Chain
Exploration and Extraction of Fuels (Offshore)	API RP 14J, Recommended Practice for Design and Hazards Analysis for Offshore Production Facilities (30 C.F.R. §250)[a]	RP 70, Security for Offshore Oil and Natural Gas Operations (33 C.F.R. §105)[a]		
	RP 75, Safety and Environmental Management System (SEMS) for Offshore Operations and Assets (30 C.F.R. §250)[a]	RP 70I, Security for Worldwide Offshore Oil and Natural Gas Operations		
	Bull 97, Well Construction Interface Document Guidelines			
Exploration and Extraction of Fuels (Onshore)	Bull 75L Guidance Document for SEMS for Onshore ONG Production			
Fuel Refining and Processing of Fuels	RP 580, Risk-Based Inspection (Refineries)			
	RP 752, Management of Hazards Associated with Location of Process Plant			
	RP 754, Process Safety Performance Indicators for Refining and Petrochemical Industries			
Fuel Storage and Reserves	Std 2350, Overfill Protection for Storage Tanks in Petroleum Facilities			
	RP 1170, Design and Operation of Solution-Mined Salt Caverns Used for Natural Gas Storage (49 C.F.R. §60141)[a]			

	Process Safety	Physical Security	Cybersecurity	Supply Chain
Pipeline Transport	RP 1171, Functional Integrity of Natural Gas Storage in Depleted Hydrocarbon Reservoirs and Aquifer Reservoirs (49 C.F.R. § 60141)[a] RP 1173, Pipeline Safety Management Systems RP 1160, Managing System Integrity for Hazardous Liquid Pipelines		Std 1164, Pipeline Control Systems Cybersecurity	

Source: CRS analysis of performance-based risk-management standards and recommended practices from API standards catalog. See API, "Purchase API Standards and Software," https://www.api.org/products-and-services/standards/purchase?. CRS reviewed the following catalog sections: "Exploration and Production," "Marketing," "Transportation," "Refining," and "Safety and Fire Protection."

Notes: Does not include ANSI/API Standard 780, "Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries," a generic security risk assessment methodology applicable to physical and cyber systems and assets. The document focuses on threats and hazards to maritime-facing distribution facilities, oil refineries, pipelines, and truck and rail transportation. Abbreviations: Std=standard; RP=recommended practice, Bull=bulletin.

a. C.F.R. references in parentheses denote incorporation of voluntary consensus standard by reference.

This general relationship between regulatory regimes and development of recommended practices and voluntary consensus standards depicted above is reflected across the risk categories covered in this report:

- 12 of 15 standards or recommended practices focus on process safety, the most heavily regulated risk category across industry segments.
- API recommended practices for management of physical security risks apply to offshore production and maritime-facing facilities—which are subject to USCG regulatory oversight under MTSA—but not to other oil and gas industry segments where physical security is not regulated.
- The API generic standard for security risk assessments focuses on regulated maritime facilities, refineries, and pipeline networks.
- General API recommended practices for risk management in the industry focus on process safety in regulated offshore facilities, refineries, storage facilities, and pipeline networks.
- The API cybersecurity standard applies exclusively to pipelines, which are increasingly subject to regulatory oversight from PHMSA and TSA in the wake of the Colonial Pipeline incident.[101]

[101] See CRS Insight IN11683, *Critical Infrastructure Policy: Information Sharing and Disclosure Requirements After the Colonial Pipeline Attack*, by Brian E. Humphreys. Also see footnote 31 for description of expanded PHMSA oversight.

Other nonindustry-specific SDOs have produced relevant standards and recommended practices that have been widely adopted across the oil and gas subsector, according to industry sources.[102] The International Electrotechnical Commission (IEC) publishes generic standards for industrial control systems security, which draw upon risk-based approaches.[103] Additionally, the International Standards Organization (ISO) has jointly published generic standards with IEC for information security management systems, as well as standards for SCRM specific to the oil and gas industry.[104]

Organization of Public-Private Partnerships for Coordination and Information Sharing in the Oil and Gas Subsector

DHS is the lead federal agency for coordinating CISR partnerships with the private-sector (see the "Federal Nonregulatory Authorities" section). Several coordination and information-sharing bodies organized under the PPD-21 framework provide a nexus for public-private collaboration for CISR in the oil and gas, and transportation systems (pipelines) critical infrastructure subsectors.

Sector Coordinating Councils

SCCs in the oil and natural gas subsector and pipeline subsector are self-organized by nongovernmental stakeholders as the counterpart to GCCs (see "Federal Nonregulatory Authorities"). The Energy GCC—co-chaired by the DOE and DHS—is the government counterpart to both recognized energy subsectors' coordinating councils. The Oil and Gas Subsector Coordinating Council (ONG SCC), organized under the NIPP framework and CIPAC charter, the government counterpart to ONG SCC. According to its charter, ONG SCC provides "a private forum for effective coordination of oil and natural gas security strategies and activities, policy, and communication across the sector to support the nation's homeland security mission."[105]

The ONG SCC also includes the Pipeline Working Group (PLWG), which serves as the subject matter advisory group to the ONG SCC for security matters and information sharing, including intelligence. (As the Pipeline Sector Coordinating Council (PSCC), the same group serves as the industry counterpart to the Transportation Systems—Pipeline Modal GCC, which is organized under Transportation Systems GCC auspices.)[106] Additionally, the ONG SCC maintains working groups for cybersecurity, information sharing, cross-sector coordination, regulatory engagement, and emergency management.[107] Membership of the ONG SCC and PLWG is comprised primarily of industry trade groups for policy advocacy and standards setting, as well as other industry representatives from major oil and gas companies.

---

[102] ONG SCC, *Defense-in-Depth*, op. cit., p. 16.

[103] International Electrotechnical Commission IEC 62433. See IEC, "IEC Webstore", https://webstore.iec.ch/.

[104] For example, ISO 29001-2020 and ISO/IEC 27000 family.

[105] ONG SCC, *Governance Principles and Operating Procedures*, August 2020, p. 1, http://ongsubsector.com/documents/ONG-SCC-Charter-082020a.pdf.

[106] Pipeline Working Group, Pipeline Sector Coordinating Council, *Charter*, November 2014, https://www.cisa.gov/sites/default/files/publications/Pipeline-SCC-Charter-508.pdf; and ONG SCC *Governance Principles*, op. cit., p. 6, which reads "Due to the dual coverage of pipelines under the NIPP within both the Energy and Transportation Sectors, a standing Pipeline Working Group has been established as a working group under the ONG SCC. The Pipeline Working Group under the ONG SCC also serves as the Pipeline SCC for the Transportation Sector."

[107] See ONG SCC, "About the ONG SCC: Working Groups," http://ongsubsector.com/.

Information Sharing and Analysis Centers

The Oil and Natural Gas (ONG) ISAC is an industry owned and operated nonprofit, which serves as "a central point of coordination and communication" across industry segments for sharing cyber threat information among member organizations and government partners.[108] A membership committee adjudicates applications according to organizational bylaws governing eligibility. Eligible entities include public and private oil and natural gas companies; certain ICT service providers, technology integrators, control systems service providers, and security providers; and certain trade or industry associations, other ISACs and information-sharing organizations, academic institutions, and research organizations.

Access to shared information is restricted by membership category using the Traffic Light Protocol (TLP).[109] Information labeled "red," the most restricted category, is shared only "in the room" with small defined groups—apparently representatives of large oil and gas firms with upper-tier memberships. "Amber," or confidential information, is available on a limited basis to other members at lower tiers, such as ICT service providers and nonprofit groups, but is not shared outside the ISAC membership. "Green" information may be shared with members, relevant government entities, and "strategic partners." "White" information may be shared with the general public subject to copyright rules.[110]

Membership dues vary by service tier and member type. Large for-profit firms with annual revenue greater than $15 billion pay $50,000 annually for the "platinum" package, while nonprofits pay $2,000 for the "nonprofit plus" package or $0 for a basic package.[111] Platinum members have full access to shared information. Information sharing with nongovernmental entities at lower membership tiers and government agencies is restricted to varying degrees. This tiered membership structure based on pricing and organization type potentially creates information asymmetries among ISAC members in favor of large for-profit firms.

The Cybersecurity Information Sharing Act of 2015 (P.L. 114-113) contains several relevant provisions that govern exchange of information on cyber threats between private-sector organizations—such as the ONG SCC—and government agencies at the federal, state, and local levels.[112] The legislation requires federal agencies to provide classified cyber threat information to private-sector partners with appropriate security clearances. Additionally, it exempts any information provided by private-sector entities under the statute from disclosure under the Freedom of Information Act (FOIA; P.L. 89-487) and other statutes governing public access to government records, as well as from any use in litigation, antitrust actions, or regulatory enforcement.

---

[108] See Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC), "Protecting Critical Infrastructure: ONG-ISAC Mission," https://ongisac.org/.

[109] For information on TLP, see CISA, "Traffic Light Protocol (TLP) Definitions and Usage," https://www.cisa.gov/tlp.

[110] See ONG-ISAC, "Protecting Critical Infrastructure: Traffic Light Protocol," https://ongisac.org/.

[111] See ONG-ISAC, "Industry Membership," https://ongisac.org/membership/industry-membership/#.

[112] ONG SCC states, "In 2015, the natural gas and oil industry was a leading supporter of the first-ever legal framework to govern cybersecurity information sharing. The Cybersecurity Act of 2015 enabled cybersecurity threat indicators to be shared between and among companies and the U.S. Government, established the legal requirements and protections for such sharing, and established DHS as the hub for government and private-sector cybersecurity information sharing." See ONG SCC and Natural Gas Council, *Defense-in-Depth: Cybersecurity in the Natural Gas & Oil Industry*, 2018, p. 18, http://naturalgascouncil.org/wp-content/uploads/2018/10/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

The Critical Infrastructure Information Act of 2002 (P.L. 107-296) provides similar protections for confidentiality, as well as limitations on use of protected information in legal or regulatory proceedings. Information may relate to systems, assets, and networks in any designated infrastructure sector. Under this authority, DHS created the Protected Critical Infrastructure Information (PCII) program, which is currently administered by CISA.

In addition to the ONG ISAC, the Downstream Natural Gas (DNG) ISAC serves natural gas utility (distribution) companies in coordination with the Electricity ISAC, "facilitating communications between participants, the federal government and other critical infrastructures."[113] For more information on federal agency pipeline cybersecurity activities, see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran. For more information on E-ISAC and federal agency electric grid cybersecurity activities, see CRS Report R45312, *Electric Grid Cybersecurity*, by Richard J. Campbell.

Federal Advisory Committees

As of December 2021, DOE—the SRMA for the energy sector—manages 22 federal advisory committees in accordance with FACA provisions. Advisory committee members typically represent a variety of stakeholder groups, consisting of "the users, industries, and organizations in the public and private sectors that could be directly affected by the work of the committee."[114] The National Petroleum Council (NPC) is the Oil and Natural Gas Advisory Committee to the Secretary of Energy. According to NPC, "The sole purpose of the Council is, at the Secretary of Energy's request, to advise, inform, and make recommendations to the Secretary, and through the Secretary, to the Executive Branch, on matters pertaining to oil and natural gas or to the oil and gas industries."[115]

DHS manages the National Offshore Safety Advisory Committee (NOSAC). According to its charter, NOSAC provides "advice to the Secretary of the Department of Homeland Security on matters relating to activities directly involved with, or in support of, the exploration of offshore mineral and energy resources, to the extent that such matters are within the jurisdiction of the Coast Guard."[116] The Coast Guard regulates offshore exploration and extraction safety and security under MTSA (see the "Regulation of Exploration and Production of Oil and Natural Gas" section).

Coordination and Information-Sharing Activities

Standards development, public-private coordination, and information-sharing activities take place under the federal CISR voluntary framework, both across the oil and gas subsector and with relevant government agencies. Some are specific to the oil and gas subsector, while others apply generally across critical infrastructure sectors, but have been adopted by some oil and gas subsector stakeholders.

[113] See "Downstream Natural Gas ISAC," https://www.isao.org/information-sharing-group/sector/downstream-natural-gas-isac/.

[114] See DOE, "Federal Advisory Committee Management," https://www.energy.gov/management/office-management/operational-management/federal-advisory-committee-management.

[115] National Petroleum Council, "Department of Energy Calls Industry Pandemic Performance Invaluable," press release, December 15, 2020, https://www.npc.org/NPC-postmtg-121520.pdf.

[116] DHS and USCG, *National Offshore Safety Advisory Committee Charter*, July 1, 2021, p. 1, https://www.dhs.gov/sites/default/files/publications/2021_nosac_charter.pdf.

Examples of Public-Private Coordination

In 2011, API and other industry stakeholders founded the Center for Offshore Safety (COS) to provide "tools, peer learning opportunities, good practices, and support for companies on the U.S. Outer Continental Shelf" and to help industry "meet its safety and sustainability objectives" under the SEMS process.[117] In May 13, 2021, testimony to the Senate Committee on Energy and Natural Resources, the COS Director—a former USCG officer and lead regulator for offshore oil and gas safety, security, and environmental compliance—described integration of COS information-sharing initiatives with regulatory requirements, saying: "The COS is playing a central role in both advancing a culture of safety in offshore operations and providing an important interface with government regulators,"[118] Activities include collection and analysis of SEMS third-party audit data, incident data, and safety performance data, which in turn have been posted on the COS public website and shared with regulators.[119]

In the onshore segment, API works with other SDOs and maintains an active membership in the National Service, Transmission, Explorations and Production Safety (nSTEPS) Network, "founded in 2003 in South Texas by OSHA and industry to reduce injuries and fatalities." According to API, it meets regularly with other stakeholders to share information and best practices related to workplace safety.[120] Additionally, API has sponsored the OSHA Oil and Gas Safety Conference.[121]

In 2014, NIST published a widely-referenced cybersecurity framework ("the NIST framework") for critical infrastructure in fulfilment of White House Executive Order (E.O.) 13636, "Improving Critical Infrastructure Cybersecurity."[122] The NIST framework calls for development of industry-specific profiles, which it describes as "an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core." Further, "Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a 'Current' Profile with a 'Target' Profile."[123] As described below, the NIST framework has been widely used to inform development of cyber risk-

---

[117] See Center for Offshore Safety (COS), "Who We Are," https://www.centerforoffshoresafety.org/About-COS/Who-We-Are; also API, "API: Board of Directors Approves Industry Center for Offshore Safety," press release, March 17, 2011, https://www.prnewswire.com/news-releases/api-board-of-directors-approves-industry-center-for-offshore-safety-118198374.html.

[118] U.S. Congress, Senate Committee on Energy and Natural Resources, *Testimony of Russell Holmes, Director, Center for Offshore Safety*, Full Committee Hearing to Examine Offshore Energy Development, 117th Cong., 1st sess., May 13, 2021, pp. 4-5, https://www.energy.senate.gov/services/files/16817187-8CDB-4806-BC57-28062DF95AF5.

[119] Ibid, p.4.

[120] API, *API Commitment to Safety: Onshore Oil and Gas Extraction*, 2016, pp. 1-2, https://www.api.org/-/media/Files/Policy/Safety/14-Industry-commitment-to-onshore-safety.pdf.

[121] API is listed as the "Pinnacle Sponsor" of the 2021 Oil and Gas Safety and Health Conference. According to the event website, the conference "will *focus on two regulated segments* in the oil and gas industry: safety and health and environmental. As always, the conference will provide a platform to exchange new ideas and concepts related to the oil and gas industry, all with the overriding goal of achieving better safety and environmental operations and *regulatory compliance* [emphases added]." See University of Texas, Arlington, "Oil & Gas Safety and Health Conference 2021 OSHA Exploration & Production," https://web.cvent.com/event/026fff5e-30a0-47af-bed6-32487a092a4a/summary?rt=NR4KMwTQrEC83OCoRg_TJA.

[122] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Public Papers of the Presidents of the United States: Barack H. Obama* (Washington: GPO, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[123] See NIST, "Cybersecurity Framework: An Introduction to the Components of the Network," https://www.nist.gov/cyberframework/online-learning/components-framework.

management guidance for the critical infrastructure enterprise generally, and the oil and gas subsector specifically.

USCG—consulting with ONG SCC and other industry partners—used the NIST framework to develop a profile for the Maritime Bulk Liquids Transfer (MBLT) and Offshore Facilities mission areas regulated under MTSA authorities.[124] The profile was intended as "nonmandatory guidance" for industry partners to aid compliance with 33 C.F.R. 154-156, which regulates a range of MBLT and offshore facilities' systems and operations related to handling of oil and other hazardous materials.[125] The profiles identified potential cybersecurity vulnerabilities relating to regulated systems and operations, and provided users with guidance on making risk assessments and implementing cybersecurity plans.

Since 2012, DOE has developed the Cybersecurity Capability Maturity Model (C2M2) for industry partners in the energy critical infrastructure sector, including the oil and gas subsector. C2M2 is developed in reference to the NIST Framework. The 2021 update to C2M2 lists ONG SCC and the Electricity SCC as the primary private-sector sponsors of the document, and lists dozens of oil and gas industry representatives from all segments as contributors.[126] Unlike the USCG cybersecurity profiles described above, C2M2 does not refer to a regulatory framework and is not intended to facilitate regulatory compliance.[127] DOE and its private-sector partners designed C2M2 to be used by relevant industries in conjunction with an online self-evaluation tool to benchmark current capabilities or "maturity" of cybersecurity programs and practices, and plan for future improvements.[128] It covers several related domains, such as risk management, third-party (or supply-chain) risk management, and threat and vulnerability management.[129]

As noted above (see "Voluntary Consensus Standards and Recommended Practices"), TSA has issued a series of voluntary Pipeline Security Guidelines ("the guidelines"), most recently in 2018. TSA developed the guidelines in collaboration with industry representatives and the Pipeline GCC and SCC.[130] These guidelines were developed to inform voluntary TSA consultations with pipeline sector stakeholders, and were intended to be advisory rather than regulatory in nature.[131] The guidelines recommend that pipeline operators should "consider the approach outlined in the NIST Framework and the guidance issued by DHS and the Department of Energy along with industry-specific or other established methodologies, standards, and best practices."[132]

Members of the Interstate Natural Gas Association of America, which represent the majority of interstate natural gas pipeline operators in the United States, have committed to following the

[124] USCG, *Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Profiles*, Version 3, Washington, D.C., December 2017, https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Cyber%20Profiles%20Overview.docx.

[125] Ibid, p. vi.

[126] DOE, *Cybersecurity Capability Maturity Model (C2M2)*, Version 2.0, Washington, DC, July 2021, p. iii, https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf.

[127] Ibid, p. vi.

[128] Ibid, p. 5.

[129] See DOE, Office of Cybersecurity, Energy Security, and Emergency Response, "Components of the C2M2," https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[130] Transportation Security Administration (TSA), *Pipeline Security Guidelines*, March 2018, p. 1, https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

[131] Ibid.

[132] Ibid, p. 22.

guidelines and the NIST Framework.[133] Voluntary commitments have since been superseded in part by the first of two TSA security directives issued in the wake of the Colonial Pipeline incident. The May 2021 directive requires covered pipeline operators to:[134]

- review Section 7 of the guidelines;
- assess whether current practices and activities to address cyber risks to Owner/Operators Information and Operational Technology systems align with the guidelines;
- identify any gaps; and
- identify remediation measures that will be taken to fill those gaps and a timeline for implementing these remediation measures.

Examples of Information Sharing

A table in a 2018 report, titled "Defense in Depth: Cybersecurity in the Natural Gas & Oil Industry," ONG SCC lists several examples of "information sharing with industry partners"—two of which were facilitated by ONG-ISAC.[135] In the first case, an oil and natural gas company shared information via the ONG-ISAC about a phishing campaign. The ONG-ISAC used the information to identify and notify other companies being targeted. In the second case, an oil and natural gas company analyst researched "known personalities, their associates and supporters involved in illegal activities during global natural gas and oil protests"—apparently a reference to anti-industry protestors that target oil and gas infrastructure with disruptive and potentially illegal tactics. The company shared a "threat information package" via DNG-ISAC, which included examples of "successful legal mitigations used by Federal, State, Local, Tribal and Territorial partners."[136]

The overall nature and scope of information sharing between ONG-ISAC and its governmental and private-sector partners is unclear from these two examples. However, the report states:

> Industry works closely with the government agencies responsible for cybersecurity throughout each of these segments—from Coast Guard regulatory oversight in maritime and maritime-facing facilities to Transportation Security Administration (TSA) regulatory oversight of pipelines, as well as bi-directional sharing with the U.S. intelligence community via the Department of Homeland Security (DHS)/NIST's National Cybersecurity & Communications Integration Center (NCCIC), DOE, FBI and others—ensuring collaboration and communication at every point.[137]

Broader federal efforts to increase sharing of cyber threat indicators and defensive measures between the private sector and federal agencies on a larger scale via automated means have produced modest results, according to a 2019 interagency report to Congress in compliance with the Cybersecurity Information Sharing Act of 2015.[138] According to the report, "as of June 2019,

[133] ONG SCC, *Defense in Depth*, op. cit., p. 23; and Interstate Natural Gas Association of America, "Commitments to Pipeline Security," https://www.ingaa.org/File.aspx?id=34310&v=836b69e4.

[134] See Transportation Security Administration, *Security Directive Pipeline 2021-01*, Enhancing Pipeline Security, Springfield, VA, May 28, 2021, p. 4.

[135] Ibid, p. 21. The report lists a total of five examples. Two involve ONG ISAC, two involve other peer-to-peer sharing, and one involves E-ISAC. It is unclear from the examples in the ONG SCC report what additional information may have been shared by ONG-ISAC with private-sector or public-sector partners.

[136] Ibid.

[137] Ibid, p. 7.

[138] See Office of the Inspector General of the Intelligence Community (OIGIC), *Unclassified Joint Report on the*

only four Federal and six non-Federal entities used AIS to share cyber threat information." (AIS refers to the Automated Indicator System—the automated capability mandated by the act, which is provided by CISA.)[139] The report identified several obstacles to greater information sharing, including restrictive classification processes; limited interoperability of relevant ICT systems; industry liability concerns; and perceived quality and relevance of information shared via automated means.[140] In response to these concerns, CISA began adding context to AIS data and has developed an industry engagement plan, according to the report.[141]

The PCII program (see the "Information Sharing and Analysis Centers" section) has also faced obstacles to widespread adoption by private-sector stakeholders, according to a 2006 Government Accountability Office (GAO) report.[142] More recently, DHS initiated a rulemaking process in 2016 to update PCII program regulations codified under 6 C.F.R. Part 29. (An updated rule has not been published as of December 2021.) DHS received a total of 11 responses during the comment period from corporate entities and individuals.[143] The response from Berkshire Hathaway Energy—the only energy company to submit comments—offered both praise and criticism for the PCII program.[144]

> Berkshire Hathaway Energy organizations have used the PCII protections as key confidence-building measure in engagements involving numerous Department of Homeland Security offices as well as other related partners including the Federal Energy Regulatory Commission, Department of Energy, Department of Defense, Federal Bureau of Investigation and numerous state law enforcement agencies. PCII provides a common framework across multiple political and administrative boundaries for establishing a key baseline set of reasonable protections.

Berkshire Hathaway Energy stated that it had participated "in more than a dozen" PCII engagements. However, the company also expressed concerns about persistent obstacles to information sharing.

> The most significant concern is that regulatory discretion by the Department of Homeland Security PCII authorities could expose sensitive information that was offered in good faith and with the expectation of PCII protections submitted in the future.... The U.S. government's track record of protecting both classified and non-classified information leaves room for improvement.

Implementation of the Cybersecurity Information Sharing Act of 2015, AUD-2019-005-U, Washington, DC, December 19, 2019, p. 11, https://www.oversight.gov/report/icig/unclassified-joint-report-implementation-cybersecurity-information-sharing-act-2015.

[139] See CISA, "Automated Indicator Sharing," https://www.cisa.gov/ais.

[140] OIGIC, op. cit., pp. 3 and 11.

[141] Ibid, p. 11.

[142] U.S. Government Accountability Office, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383, April 2006, https://www.gao.gov/assets/gao-06-383.pdf.

[143] See Regulations.gov, "Proposed Rule: Updates to Protected Critical Infrastructure Program," https://www.regulations.gov/document/DHS-2016-0032-0001, posted by DHS on April 21, 2016; and Regulations.gov, "Proposed Rule: Updates to Protected Critical Infrastructure Program," https://www.regulations.gov/document/DHS-2016-0032-0003, posted by DHS on May 13, 2016.

[144] Berkshire Hathaway Energy, *Comments on Proposed Updates to Protected Critical Infrastructure Program*, July 18, 2016, pp. 1-2.

Discussion and Analysis

The federal CISR policy framework affords significant autonomy to the private sector, which owns and operates much of the nation's critical infrastructure. In many instances relevant federal agencies rely upon private-sector partners to develop and implement voluntary consensus standards and recommended practices to manage risk across each of the 16 officially recognized critical infrastructure sectors, and to engage in voluntary public-private partnerships.

In public communications, oil and gas subsector stakeholders frequently present the compulsory and voluntary aspects of the federal CISR enterprise in binary terms, wherein more of one necessarily means less of the other. For example, the ONG SCC states in its 2018 cybersecurity report, "The reliance upon voluntary mechanisms, including … proven frameworks and public-private collaboration, rather than compulsory standards or regulations, is the most effective and robust way to bolster the cybersecurity of industry companies and the critical infrastructure they operate."[145]

Such statements echo those made by successive presidential administrations since the creation of the modern CISR enterprise in the late 1990s. These have generally advocated for voluntary public-private collaboration and coordination as the preferred and most efficient means to leverage industry expertise in highly complex and dynamic critical infrastructure sectors (see the "Balancing Coordination and Regulatory Authorities" section). Relevant executive orders, strategy documents, and agency programs in recent decades have therefore generally sought to preempt potential regulatory burdens through collaborative development of risk-based standards, best practices, and information sharing with private-sector partners.

The apparent alignment of voluntary public-private partnerships with emerging or evolving regulatory regimes in the oil and gas subsector as described in this report suggests that—in actual practice—private-sector participation in voluntary CISR programs and activities is significantly conditioned by the structure of federal regulatory authorities and oversight. Voluntary best practices and information-sharing initiatives and regulatory regimes are frequently co-constituted as elements of a common enterprise, and coexist within specific functional areas of the oil and gas subsector (see the "Coordination and Information-Sharing Activities" section).[146]

Federal participation in the voluntary consensus standards development process in the oil and gas subsector occurs most among agencies such as PHSMA, USCG, and BSEE that have significant regulatory roles (see "Voluntary Consensus Standards and Recommended Practices" section).[147] For example, USCG—the DHS agency that enforces security regulations under MTSA—states in the 2018 annual DHS agency report to NIST required under NTTAA that participation in voluntary consensus standards processes "helps the Coast Guard fulfill its regulatory functions more efficiently, develop the Government/industry partnerships crucial to stewardship, and gain valuable public feedback necessary for effective policy development."[148] CISA and TSA—DHS

[145] ONG SCC, Defense-in-Depth, op. cit., p. 26.

[146] For a theoretical discussion of this process, see Rebecca Slayton and Aaron Clark-Ginsberg, "Beyond Regulatory Capture: Coproducing Expertise for Critical Infrastructure Protection," *Regulation & Governance*, vol. 12, no. 1 (March 2018).

[147] See NIST, "NTTAA Reports," https://standards.gov/NTTAA/Report/viewAgencyReport.aspx, for access to congressionally-mandated annual federal agency reports to NIST.

[148] See "Department of Homeland Security Fiscal Year 2018 Agency Report," https://standards.gov/NTTAA/Report/viewAgencyReport.aspx. By contrast, the report indicates that other DHS agencies (CISA and TSA) focus on IT/ICT cybersecurity standards and aviation security technology respectively.

agencies with lesser regulatory footprints in the oil and gas subsector—used the report to highlight activities in other critical infrastructure sectors.

Major industry SDOs have generally developed risk-management standards in critical functional areas and risk categories where regulatory concerns exist (see the "Voluntary Consensus Standards and Recommended Practices" section), either to pursue incorporation of voluntary consensus standards documents by reference into existing regulatory regimes or preemption of regulation in the first place. There may be less impetus for voluntary consensus standards development in unregulated or lightly regulated areas of the subsector.

The record indicates that API and other industry organizations have been most active in developing risk-management standards and investing in voluntary public-private partnerships in heavily regulated industry segments, such as offshore fuel exploration and extraction. For example, the Center for Offshore Safety (COS) industry safety group provides aggregated incident data to industry regulators. BSEE claims to have used this data to inform regulatory oversight, and many regulatory filings cite examples of public-private coordination and collaboration under COS auspices.[149] By contrast, safety programs for the onshore exploration and extraction segment, such as the nSTEPS Network described in the "Examples of Public-Private Coordination" section, do not appear to have produced comparable public-private partnerships, or publicly available safety and security data.

Private-sector stakeholders in the oil and gas subsector often claim that—regardless of regulatory requirements—applicable standards for process safety, security (both physical and cyber), and SCRM enjoy wide adoption throughout the industry. For example, in its 2018 cybersecurity report, ONG SCC states that, "Cybersecurity in the natural gas and oil industry applies throughout the value chain, extending from wellheads to pipelines and through to the supply of natural gas to an electric power generation facility or gas utility, or the supply of oil to a refinery and through to a gasoline station."[150]

Assessing the accuracy of such statements is beyond the scope of this report. However, the limited availability of relevant information that could potentially be used for an assessment of cybersecurity or other CISR risk profiles in the oil and gas subsector is a source of concern for some observers. For example, the LLNL report states:

> Strict cybersecurity regulations govern power, chemical and nuclear facilities, but no federal laws impose such standards in the ONG industry.[151] When ONG companies have been compromised, they aren't required to report the cyber incident. Even when they turn to federal authorities for help, the specifics are typically kept secret because companies disclose information in exchange for anonymity and discretion. The Department of Homeland Security (DHS) publishes aggregated data on cyber-attacks within the ONG sector, but with no mandatory reporting requirements for asset owners, the data may be representative of only a small share of the cyberattacks against the energy industry.[152]

Information sharing among competing entities within the private sector, and between private-sector owner-operators of critical infrastructure and federal security agencies, were among the

[149] See BSEE, "Oil and Gas and Sulphur Operations in the Outer Continental Shelf: Safety and Environmental Management Systems Revisions," 78 *Federal Register* 20427, April 5, 2013.

[150] ONG SCC, *Defense in Depth*, op. cit., p. 17.

[151] For overview of electric grid cybersecurity enforceable standards, see CRS Report R45312, *Electric Grid Cybersecurity*, by Richard J. Campbell; CRS In Focus IF10853, *Chemical Facility Anti-Terrorism Standards*, by Frank Gottron; and CRS Report R42853, *Nuclear Energy: Overview of Congressional Issues*, by Mark Holt.

[152] LLNL Report, op. cit. p. 13.

core policy concerns that gave impetus to the CISR enterprise from its earliest days. Key legislation, such as the Critical Infrastructure Information Act of 2002 and the Cybersecurity Information Act of 2015, have sought to elicit sharing of sensitive information by limiting federal oversight authorities and providing assurances of confidentiality and certain immunities to owner-operators of critical infrastructure. However, results appear to be modest (see "Information Sharing and Analysis Centers"). As seen in the 2016 plant explosion in Pascagoula, MS, information secrecy can have catastrophic consequences (see text box, "Unmanaged Risk and Disruption of Critical Supply Functions").[153]

Information and data gaps may affect risk-management activities in several ways, according to experts. First, such gaps may hinder public and private-sector stakeholders from developing a consensus understanding of relevant risks based on accurate assessments of hazards and vulnerabilities affecting critical systems, assets, and networks. Second, such gaps may obscure understanding of both the technical content of risk-management programs, and the manner and extent of their implementation across the oil and gas subsector. This in turn may hinder assessment of the appropriateness and effectiveness of voluntary consensus standards, recommended practices, and guidelines as applied in practice, especially when multiple standards may be applicable and stakeholder consensus is weak (see the "Voluntary Consensus Standards and Recommended Practices" section).[154]

The structure of voluntary guidance, and its relationship to relevant regulatory frameworks, may affect information sharing. Again, comparison of offshore and onshore exploration and extraction segments may be illustrative. The offshore segment, regulated under OCSLA and MTSA authorities, provides a notable contrast with other segments. For example, the USCG cybersecurity profiles for operators of offshore and MBLT facilities are intended as nonmandatory guidance to aid compliance with 33 C.F.R. 154-156, which covers safety standards for maritime oil and gas transfer facilities. However, they are structured in such a way that private-sector entities using them would necessarily provide information about cybersecurity vulnerabilities and mitigations to USCG regulators under the reporting requirements of 33 C.F.R. 105-106. Additionally, SEMS requirements have apparently led to industry development of a robust community of interest for information sharing and analysis under COS auspices (see "Examples of Information Sharing").

By contrast, the DOE C2M2 model is designed primarily to facilitate information sharing *within* organizations using the self-assessment tool (see "Examples of Information Sharing"). Although the model applies to all critical infrastructure within the energy sector with cyber-interfaces—including the various critical functional areas of the oil and gas subsector—it specifically excludes integration with regulatory compliance regimes that would facilitate sharing information about cybersecurity vulnerabilities or mitigations with external entities, including federal agencies.

The appropriate purpose, scope, extent, and content of regulation in the oil and gas subsector, and its implications for development of CISR communities of interest, remain salient concerns for oil and gas subsector stakeholders. Many subsector stakeholders view increased regulatory burdens as its own category of risk.[155] For such stakeholders, ensuring that critical infrastructure risk-management continues to be largely based on voluntary public-private collaboration, rather than regulation, is likely to be a priority. Advocates for this approach frequently claim that owner-

[153] CSB, *Case Study: Loss of Containment, Fires, and Explosions at Enterprise Products Midstream Gas Plant*, No. 2016-02-I-MS, February 13, 2019, p. 38. https://www.csb.gov/assets/1/6/final_case_study_-_enterprise.pdf.

[154] Ibid, pp. 31, 38-39.

[155] BDO 2017, op. cit., p.6.

operators are best positioned to assess and manage risks to their critical systems, assets, and networks. Overly prescriptive approaches, they say, may make risk management less efficient—i.e., expending more resources for less overall risk mitigation.

Others question whether the existing emphasis on voluntary industry participation and consensus is achieving necessary levels of risk reduction or mitigation in a high-risk critical infrastructure subsector. Among federal agencies, CSB in particular has often exercised its advisory authorities to highlight regulatory gaps and to advocate setting and enforcing specific risk reduction goals for oil and gas infrastructure operators.[156] The 2021 incidents affecting electricity supply in Texas and fuel supplies on the East Coast, described above, focused congressional attention on perceived failures of the voluntary CISR framework. Numerous hearings and legislative proposals raised the issue of new regulatory authorities and functions to protect critical infrastructure.[157] However, significant congressional support still exists for the voluntary public-private partnership model.[158]

117th Congress Legislation

Congress enacted a number of provisions to improve cybersecurity of the bulk power system under Subtitle B, "Cybersecurity," of the Infrastructure Investment and Jobs Act (P.L. 117-58), focusing on voluntary assessments, information sharing, investment incentives, grants, and technical assistance from DOE, DHS, and other federal agencies. One provision specifically includes elements of the oil and gas subsector. "Modeling and Assessing Energy Infrastructure Risk," directs the Secretary of Energy, in coordination with other federal agencies, to develop a $50 million program to improve vulnerability assessments and modeling capabilities, research infrastructure and hardening solutions, conduct exercises, and update the DOE C2M2 model to include physical security (see "Examples of Public-Private Coordination"). The purpose of the program is to secure electric, natural gas, and oil exploration, transmission, and delivery networks "in the face of natural and human-made threats and hazards, including electric magnetic pulse and geomagnetic disturbances."

The Ransom Disclosure Act (S. 2943) would require certain entities to disclose ransom payments to DHS. Specifically, within 48 hours of paying a ransom, disclosure must be made to DHS by any entity that (1) is engaged in interstate commerce, (2) is engaged in an activity affecting interstate commerce, or (3) receives federal funds. DHS must annually publish information disclosed, including the total dollar amount paid, without revealing identifying information. Although not specific to the oil and gas subsector, this legislation would affect Colonial Pipeline Company and other subsector companies subjected to ransomware attacks.

The Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440) would establish a new CISA Cyber Incident Review Office responsible for collecting and reviewing incident data from covered critical infrastructure entities, as well as facilitating bidirectional information sharing between relevant private-sector stakeholders and government intelligence agencies.

---

[156] For example, U.S. Chemical Safety and Hazard Investigation Board, *Drilling Rig Explosion and Fire at the Macondo Well*, vol. 4, Washington, DC, April 20, 2017.

[157] For example, U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems*, 117th Cong., 1st sess., September 23, 2021, and U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, 117th Cong., 1st sess., September 1, 2021.

[158] See Portman et al., op. cit., p. 1. The letter to the DHS Inspector General in response to TSA directives for pipeline security in 2021 reads in part, "Our critical infrastructure must be secured and protected against cyberattacks. However, securing critical infrastructure requires a collaborative approach with the experts in these industries—the people who operate this critical infrastructure and who are charged with implementing these directives."

Covered critical infrastructure entities would be subject to certain requirements (subject to agency rulemaking) for reporting cybersecurity incidents to the Cyber Incident Review Office.

The Defense of United States Infrastructure Act of 2021 (S. 2491) would establish a National Cyber Resilience Assistance Fund, "to improve the ability of the Federal Government to assist in enhancing critical infrastructure cyber resilience, to improve security in the national cyber ecosystem, to address Systemically Important Critical Infrastructure, and for other purposes." The proposed grant program would allow DHS to award cybersecurity resilience improvement grants to eligible private-sector entities under three conditions:

- presence of "clearly defined cybersecurity risk" affecting critical infrastructure
- insufficient private-sector incentives to mitigate risk
- clear need for federal responsibility to mitigate identified risks

The proposed legislation also contains provisions for cloud based information sharing across federal agencies, a product certification program for designated "critical information and communications technology" based on to-be-developed consensus standards, and establishment of a Bureau of Cybersecurity Statistics with DHS to track and analyze cyber incident data.

Several bills in the 117th Congress would affect federal pipeline cybersecurity programs, including the Pipeline Security Act (H.R. 3243), the Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 3078), the Promoting Interagency Coordination for Review of Natural Gas Pipelines Act (H.R. 1616), and the Energy Product Reliability Act (H.R. 6084). These bills primarily deal with federal agency roles and responsibilities in the pipeline sector, and interagency coordination. For discussion of these bills and related issues, see the "Issues for Congress" section in this report.[159]

116th Congress Legislation

The Consolidated Appropriations Act, 2021 (P.L. 116-260), enacted under the 116th Congress, contains the Leonel Rondon Pipeline Safety Act (the Act), named after a Massachusetts resident killed in a residential natural gas explosion. The Act directed the Secretary of Transportation to promulgate regulations to require new standards for downstream gas distribution operators' integrity management plans for low-pressure pipelines. Among other provisions, it required operators to assess hazards of cast iron pipes and mains (if present) and system pressure anomalies, and to consider factors other than past anomalies when making assessments. Additionally, it specifically prohibited operators from determining that there are no consequences associated with low-probability events without appropriate engineering or other justification.

Issues for Congress

With respect to critical infrastructure risk management in the oil and gas sector, Congress may consider several specific issues of potential interest: the role of federal agencies in industry-led standards development processes and reliance on industry associations to provide standards used for regulatory purposes; information sharing and incident disclosure requirements and the structure and governance of information-sharing bodies; and optimization of regulatory, nonregulatory, or hybrid frameworks that combine voluntary guidance and public-private coordination with risk-management mandates.

[159] For additional information (except H.R. 6084), see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*, by Paul W. Parfomak and Chris Jaikaran.

Legislation introduced or enacted in the 116th and 117th Congresses may have implications for all of these issues, both within the oil and gas subsector (including pipelines) and among other critical infrastructure sectors and subsectors. Taken together, this legislation indicates congressional focus on several key areas:

- directly supporting private-sector risk mitigation investments, particularly in cybersecurity;
- closing data gaps through creation of new agency functions and regulatory requirements for cybersecurity incident reporting;
- revised agency roles and responsibilities for critical infrastructure security and resilience; and
- expanded scope of mandatory physical and cybersecurity standards.

The Voluntary Critical Infrastructure Security and Resilience Framework

Some legislation suggests a fundamentally altered approach to critical infrastructure security and resilience risk management as a national enterprise. For example, the current framework places primary responsibility for risk management for privately owned systems, assets, and networks on owner-operators—including the costs of risk mitigation. S. 2491 identifies market failures as having potential to discourage necessary infrastructure security and resilience investments by the private sector, and proposes a government funding mechanism—i.e., a new series of homeland security grants—to address identified gaps. It is perhaps a tacit acknowledgement that private-sector business imperatives may not necessarily align with national risk-management goals in all or most cases—a key assumption of the existing framework. In any case, federal funding for private-sector risk mitigation would represent a new direction for the critical infrastructure enterprise, placing increased responsibility on the federal government to support private-sector investment in critical infrastructure security and resilience.

H.R. 3078 would elevate the role of DOE in voluntary risk-management programs "through councils or other entities in sharing, analysis, or sector coordinating, to ensure the security, resiliency, and survivability of natural gas pipelines (including natural gas transmission and distribution pipelines), hazardous liquid pipelines, and liquefied natural gas facilities." Similar functions are currently carried out by TSA and DOT in the Transportation Systems Sector, which includes the Pipeline Modal Subsector. The bill contains a savings clause which preserves existing agency authorities while modifying DOE authorities and mandates in the subsector. In the FY2020 NDAA, Congress mandated DHS updates to critical infrastructure sectors and SRMAs. As of this writing, no updates have been publicly released that would indicate revised roles and responsibilities of SRMAs.

Information Sharing, Data Gaps, and Incident Reporting Requirements

Congress continues to show interest in information sharing as a key component of efforts to make relevant data for risk management more widely available to critical infrastructure sector stakeholders. Existing programs described in this report are predicated upon industry willingness to share critical information if the federal government eliminates or mitigates certain barriers to information sharing by providing assurances of anonymity and discretion. The comparatively modest results of these programs have increased congressional interest in mandates to compel disclosure of critical infrastructure vulnerabilities or incidents, such as those proposed in S. 2943 and H.R. 5440, described above.

In recent years, Congress has enacted a number of strategy development and risk assessment requirements for federal agencies entrusted with critical infrastructure security and resilience. Congress has likewise created agencies and offices to exercise necessary analytical functions to fulfil these requirements—the Cybersecurity and Infrastructure Security Agency Act of 2018 that created CISA is one such example. The Bureau of Cybersecurity Statistics proposed under S. 2491 would further centralize federal functions for critical infrastructure risk analyses and assessments, while also creating a new demand signal for critical infrastructure data.

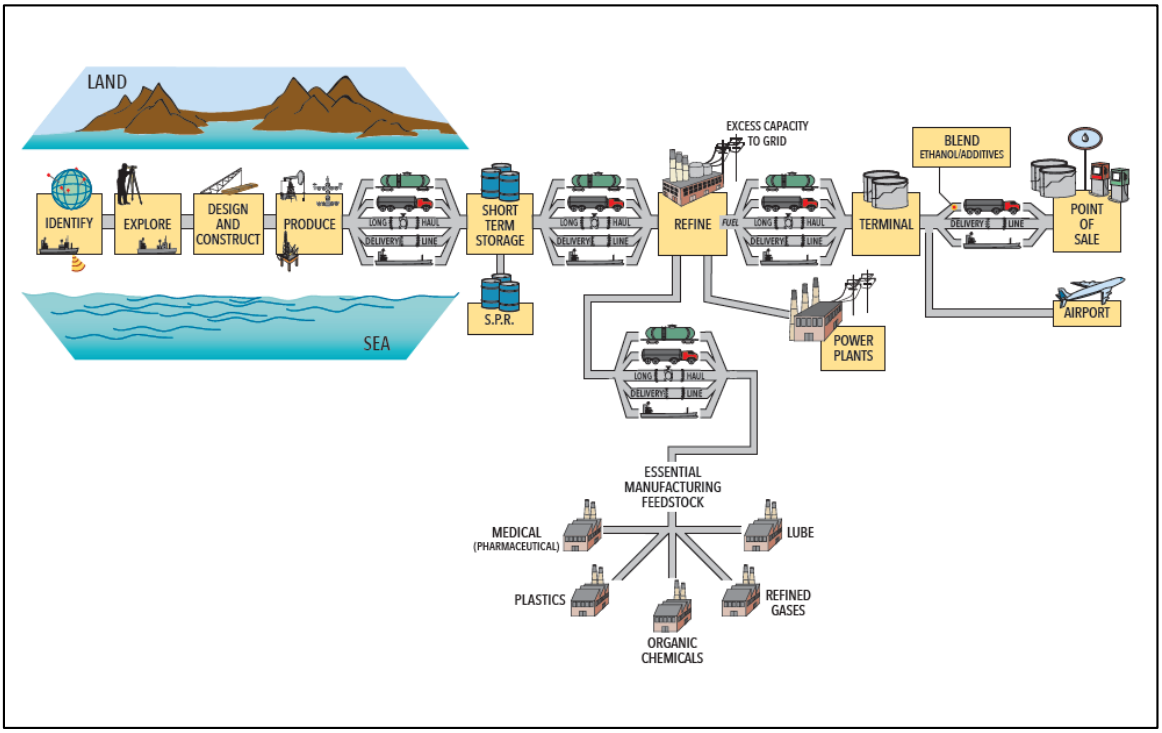
Regulatory Authorities and Oversight of Pipeline Security

Pipeline security continues to elicit congressional attention, particularly in the wake of the 2021 Colonial Pipeline Company ransomware attack and other widely publicized failures. Issues of agency jurisdiction, mission, and coordination with other agencies were raised in legislation introduced in the 117th Congress. H.R. 3243 revises TSA duties, requiring it to enhance pipeline security operations in coordination with CISA, and creating a pipeline security section with TSA. This mandate presupposes a more assertive regulatory role and capability for TSA. Prior to the Colonial Pipeline incident, TSA generally focused on cultivating public-private partnerships with pipeline operators and promulgating voluntary guidelines.

H.R. 6084 would fundamentally restructure the regulatory framework for pipeline infrastructure security and resilience, proposing a framework that closely parallels the one currently in force in the electricity subsector. It would give the Federal Energy Regulatory Commission (FERC), an independent agency within DOE, authority to create an independent industry reliability organization (the "Energy Product Reliability Organization") responsible for developing and implementing mandatory pipeline reliability standards for cybersecurity, physical security, and supply coordination (for electricity generation facilities), under agency regulatory oversight. FERC's current regulatory role in the pipeline subsector focuses on siting and rate-setting issues. However, FERC already oversees an industry reliability organization (the "Electricity Reliability Organization") in the electricity subsector which performs a function similar to that proposed in H.R. 6084.

Appendix A. Oil and Gas Subsector Supply-Chain Diagrams

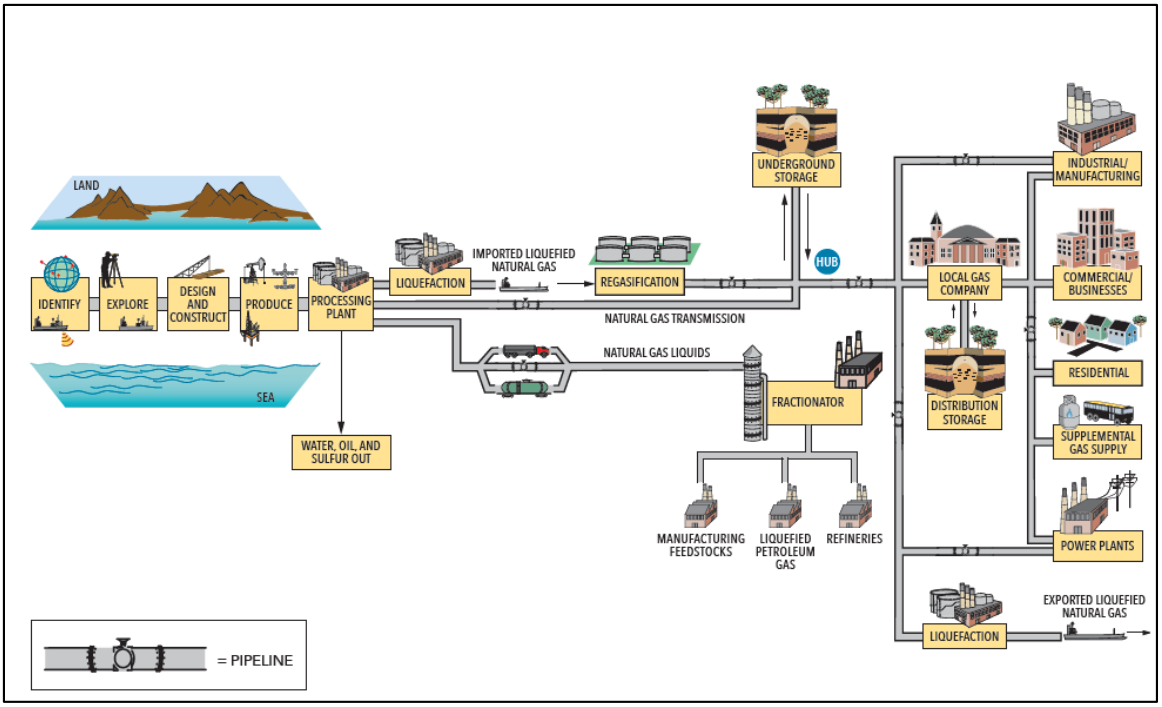
Figure A-1. Hydrocarbon Liquids (Oil) Supply Chain



Source: National Petroleum Council

Notes: See National Petroleum Council, *Enhancing Emergency Preparedness: Government and Oil & Natural Gas Industry Actions to Prepare, Respond, and Recover*, p. H-2, Washington, DC, 2014.

Figure A-2. The Natural Gas and Natural Gas Liquids Supply Chain



Source: National Petroleum Council.

Notes: See National Petroleum Council, *Enhancing Emergency Preparedness: Government and Oil and Natural Gas Industry Actions to Prepare, Respond, and Recover*, p. G-2, Washington, DC, 2014.

Appendix B. The National Standards System: Federal Roles, Authorities, and Policies

The origins of the national standards development process date back more than a century. Public and private-sector stakeholders developed the system to facilitate increased industrial efficiency and expansion of domestic and global markets for U.S. goods.[160] Stakeholder categories include individual enterprises; industry groups; accredited standards developing organizations (SDOs); public-private coordinating bodies; and regulatory agencies.

The federal government supports, but does not directly administer, the national standards system. The American National Standards Institute (ANSI), a private nonprofit organization, coordinates private-sector standards development through its accreditation process. Industry participation is voluntary. However, only ANSI-accredited SDOs may seek recognition of proposals as American National Standards. Private-sector entities may use the ANSI process to develop American National Standards to facilitate recognition and acceptance by federal and international regulatory bodies. According to ANSI, American National Standards are based on several factors, including industry consensus; an open and transparent development process; balance among stakeholders; and due process. (SDOs may also publish recommended practices that may meet some, but not all, requirements for ANSI standards.) The national standards system is both decentralized and competitive—i.e., private-sector SDOs seek wide recognition and acceptance for proprietary voluntary consensus standards offered for sale to interested stakeholders.

The National Institute of Standards and Technology (NIST), a Department of Commerce agency, provides technical support to private-sector accreditation bodies and domestic SDOs, but does not set voluntary consensus standards in most cases, except for cybersecurity. Under the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), Congress directed NIST to "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure … to coordinate closely and regularly with relevant private-sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations, including *Sector Coordinating Councils and Information Sharing and Analysis Centers*, and incorporate industry expertise." [emphasis added]

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (P.L. 104-113) and OMB Circular A-119 together provide legislative and national standards policy guidance to federal agencies. Specifically, federal agencies are required to participate in the deliberations of standards-setting bodies and to use voluntary consensus standards developed under the national system "whenever practicable and appropriate." The OMB circular does not directly reference critical infrastructure security and resilience. It focuses on reducing burdens to private-sector contractors caused by competing federal agency and private-sector standards. Nonetheless, relevant regulatory agencies have cited it when developing risk-based performance standards in partnership with regulated entities. Many of the largest oil and gas industry associations that exercise both standards development and policy advocacy functions are members of relevant PPD-21 coordination bodies.

[160] Maureen A. Breitenberg, *The ABC's of Standards Activities*, National Institute of Standards and Technology (NIST), NISTIR 7614, Gaithersburg, MD, August 2009.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer