United States Government Accountability Office

Report to Congressional Requesters

October 2022

OFFSHORE OIL AND GAS

Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure

GAO-23-105789

GAO Highlights

Highlights of GAO-23-105789, a report to congressional requesters

October 2022

OFFSHORE OIL AND GAS

Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure

Why GAO Did This Study

A network of more than 1,600 offshore oil and gas facilities produce a significant amount of domestic oil and gas. To promote safety and protect the environment, BSEE regulates offshore oil and gas infrastructure. This includes drill ships, production facilities, pipelines, and related equipment.

GAO was asked to review the cybersecurity of offshore oil and gas infrastructure. This report examines (1) the cybersecurity risks facing offshore oil and gas infrastructure and (2) the extent to which BSEE has addressed them.

GAO reviewed relevant federal and industry reports on offshore oil and gas cybersecurity risks and analyzed relevant BSEE documentation. This documentation included a draft strategic framework, a potential regulatory framework, safety alerts, and budget justifications.

GAO interviewed officials from agencies with offshore and cybersecurity responsibilities. It also obtained the perspectives of nonfederal stakeholders representing the offshore oil and gas industry.

What GAO Recommends

GAO is making one recommendation: BSEE should immediately develop and implement a strategy to address offshore infrastructure risks. Such a strategy should include an assessment and mitigation of risks; and identify objectives, roles, responsibilities, resources, and performance measures, among other things. In an email, we were informed that Interior generally concurred with our findings and recommendation.

View GAO-23-105789. For more information, contact Frank Rusco at (202) 512-3841 or ruscof@gao.gov or Marisol Cruz Cain at (202) 512-9342 or cruzcainm@gao.gov.

What GAO Found

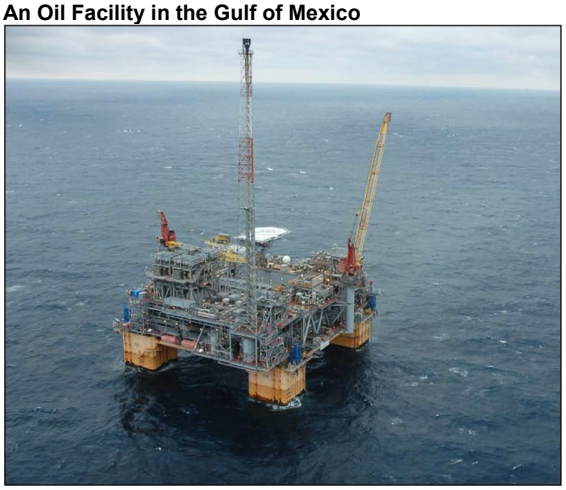
Offshore oil and gas infrastructure faces significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts.

Threat actors. State actors, cybercriminals, and others could potentially conduct cyberattacks against offshore oil and gas infrastructure. The federal government has identified the oil and gas sector as a target of malicious state actors.

Vulnerabilities. Modern exploration and production methods are increasingly reliant on remotely connected operational technology—often critical to safety—that is vulnerable to cyberattack. Older infrastructure is also vulnerable because its operational technology can have fewer cybersecurity protection measures.

Potential impacts. A successful cyberattack on offshore oil and gas infrastructure could cause physical, environmental, and economic harm, according federal officials. For example, officials said that the effects of a cyberattack could resemble those that occurred in the 2010 *Deepwater Horizon* disaster. Disruptions to oil and gas production or transmission could also affect energy supplies and markets.

An Oil Facility in the Gulf of Mexico



Source: GAO. | GAO-23-105789

The Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) has long recognized the need to address cybersecurity risks but has taken few actions to do so. In 2015 and 2020 BSEE initiated efforts to address cybersecurity risks, but neither resulted in substantial action. Earlier this year, BSEE again started another such initiative and hired a cybersecurity specialist to lead it. However, bureau officials said the initiative will be paused until the specialist is adequately versed in the relevant issues. Absent the immediate development and implementation of an appropriate strategy, offshore oil and gas infrastructure will continue to remain at significant risk. Such a strategy would call for, among other things, an assessment of cybersecurity risks and mitigating actions; and the identification of objectives, roles, responsibilities, resources, and performance measures.

Contents

Tables

Figures

Abbreviations

BSEE	Bureau of Safety and Environmental Enforcement
CISA	Cybersecurity and Infrastructure Security Agency
DOE	Department of Energy
DHS	Department of Homeland Security
NIST	National Institute of Standards and Technology
OT	operational technology
OCS	outer continental shelf
PHMSA	Pipeline and Hazardous Materials Safety Administration
USCG	United States Coast Guard

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

October 26, 2022

The Honorable Raúl M. Grijalva
Chair
Committee on Natural Resources
House of Representatives

The Honorable Alan Lowenthal
Chair
Subcommittee on Energy and Mineral Resources
Committee on Natural Resources
House of Representatives

A network of more than 1,600 structures on the outer continental shelf (OCS) is responsible for a significant portion of U.S. domestic oil and gas production.[1] In calendar year 2021, OCS leases in the Gulf of Mexico and off the coasts of California and Alaska produced approximately 628 million barrels of oil and 824 trillion cubic feet of natural gas.[2] This accounted for approximately 62 percent of the oil and 20 percent of the natural gas produced on federal property.

Offshore oil and gas infrastructure—including mobile offshore drilling units, fixed and floating production facilities, and pipelines and related equipment—is reliant on operational technology (OT) to monitor and control physical equipment. Although this technology offers many advantages to oil and gas owners and operators, the OT systems are also vulnerable to cyberattacks. In addition, cyberattacks can cause significant and potentially catastrophic damage to oil and gas infrastructure, which can result in physical, environmental, and economic harm.

[1]The outer continental shelf (OCS) refers to the submerged lands outside the territorial jurisdiction of all 50 states, but within U.S. jurisdiction and control. The portion of the North American continental edge that is federally designated as the OCS generally extends seaward 3 geographical miles off the coastline to at least 200 nautical miles. This figure reflects information from the Department of the Interior's Bureau of Safety and Environmental Enforcement's Offshore Infrastructure Dashboard as of September 7, 2022.

[2]These figures are derived from data published by the Department of the Interior's Office of Natural Resources Revenue. The vast majority of offshore oil and gas production occurs in the Gulf of Mexico.

The federal government has a significant role in addressing cybersecurity risks facing offshore oil and gas infrastructure, even though the infrastructure is owned and operated by private industry. For example:

- In 2013, the President directed federal agencies to work with owners and operators of critical infrastructure, including offshore oil and gas infrastructure, to take proactive steps to manage risk and strengthen the security of critical infrastructure from all hazards, including cyberattacks.[3] In 2015, the Department of Homeland Security (DHS) issued the *National Infrastructure Protection Plan* to further integrate critical infrastructure protection efforts between government and private sectors.[4] The plan recognizes that some sectors are overseen by federal regulators that bring key capabilities to the critical infrastructure partnership, including ensuring sector resilience through oversight.
- The Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) regulates offshore oil and gas infrastructure from permitting design and installation through decommissioning on the OCS and is responsible for the oversight of exploration, development, and production activities.[5] BSEE's regulations do not explicitly mention cybersecurity, but the bureau has determined that addressing cybersecurity risks to offshore oil and gas infrastructure aligns with its mission to promote safety and protect the environment.

Managing federal oil and gas resources and ensuring the cybersecurity security of the nation represents a nexus of two long-standing areas of concern to GAO.[6] We added the management of federal oil and gas resources to our High Risk List in 2011, on the basis of challenges that we identified with Interior's management of oil and gas on leased federal lands and waters. We found that Interior (1) experienced problems hiring, training, and retaining sufficient staff to provide oversight and management of oil and gas operations on federal lands and waters; and

[3]The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[4]Department of Homeland Security, *NIPP* [*National Infrastructure Protection Plan*] *2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.).

[5]30 C.F.R. Part 250.

[6]In 1990, GAO began a program to report on government operations that we identified as "high risk." Since then, generally coinciding with the start of each new Congress, we have reported on the status of progress in addressing high-risk areas and updated the High Risk List.

(2) was undertaking a significant and challenging reorganization of the department's oversight of its offshore oil and gas management functions.[7]

Likewise, information security has been on our High Risk List since 1997, and we expanded this area to include the protection of critical cyber infrastructure, including offshore oil and gas infrastructure, in 2003. In September 2018, we issued an update to the High Risk List that identified actions needed to address cybersecurity challenges facing the nation.[8] We later identified ensuring the nation's cybersecurity as one of nine high-risk areas that need especially focused executive and congressional attention.[9] We continue to identify the protection of critical cyber infrastructure as component of a high-risk area, as reflected in our March 2021 high-risk update on major cybersecurity challenges.[10]

You asked us to review issues related to the cybersecurity of offshore oil and gas infrastructure. This report examines (1) the cybersecurity risks to offshore oil and gas infrastructure and (2) the extent to which BSEE has addressed them.

To address our objectives, we interviewed officials and analyzed documentation from five key federal agencies and obtained the perspectives of three nonfederal organizations representing various aspects of the offshore oil and gas industry:

Federal agencies. We interviewed officials from five federal agencies with responsibilities related to oversight of the OCS or critical infrastructure protection: BSEE, the Office of Cybersecurity, Energy Security, and Emergency Response within the Department of Energy

[7]In 2021, we removed the Restructuring of Offshore Oil and Gas Oversight segment from the High Risk List because of BSEE's progress in addressing long-standing deficiencies in the bureau's investigative, environmental compliance, and enforcement capabilities and its implementation of strategic initiatives to improve offshore oversight and internal management. GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[8]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[9]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[10]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

(DOE),[11] the U.S. Coast Guard (USCG)[12] and the Cybersecurity and Infrastructure Agency (CISA)[13] within DHS; and the Pipeline and Hazardous Materials Safety Administration (PHMSA)[14] within the Department of Transportation.

Industry organizations. We contacted six nonfederal industry organizations to obtain their perspectives on the cybersecurity risks facing offshore oil and gas infrastructure.[15] Of these, three—the American Petroleum Institute,[16] the Center for Offshore Safety,[17] and the Offshore Operators Committee[18]—provided written responses to our questions. The other three—the Oil and Natural Gas Subsector Coordinating Council,[19] the Oil and Natural Gas Information Sharing and Analysis

[11]DOE's Office of Cybersecurity, Energy Security, and Emergency Response is responsible for implementing the energy sector portion of the national cybersecurity strategy for critical infrastructure, including developing and coordinating a plan for addressing oil and gas infrastructure cybersecurity.

[12]USCG has broad legal authorities associated with maritime transportation, hazardous materials shipping, oil spill response, pilotage, and vessel construction and operation.

[13]CISA is the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts.

[14]On the OCS, PHMSA is generally responsible for regulating oil and gas transportation pipelines.

[15]We selected these associations because of their relevant knowledge of the cybersecurity of offshore oil and gas infrastructure, and we identified these offshore oil and gas associations from previous GAO reports and stakeholder recommendations.

[16]The American Petroleum Institute is a national trade association that represents the U.S. oil and natural gas industry. Its corporate members—producers, refiners, suppliers, pipeline operators, and marine transporters, as well as service and supply companies—represent all segments of the industry.

[17]The Center for Offshore Safety is an industry-sponsored organization focused exclusively on safety on the OCS. The center serves the U.S. offshore oil and gas industry, with the purpose of adopting standards to ensure continuous improvement in safety and offshore operational integrity.

[18]The Offshore Operators Committee is committed to being the primary technical advocate for the offshore energy industry on issues such as safety, regulation, exploration, development, and production on the OCS.

[19]The Oil and Natural Gas Subsector Coordinating Council represents the private sector interests of the oil and natural gas industry in its public-private partnership with the federal government. It does so by providing a forum to coordinate oil and natural gas security strategies, activities, policy, and communication across the sector to support the nation's homeland security mission.

Center,[20] and the National Ocean Industries Association[21]—declined to participate in our review.

To identify the cybersecurity risks facing offshore oil and gas infrastructure, we developed a list of threat actors that could pose a threat to such infrastructure and potential vulnerabilities in the infrastructure and reviewed the potential impacts of cyberattacks on offshore infrastructure. To develop the list of cyber threat actors, we reviewed our prior work on cyber-based threats facing other energy sectors, as well as the threats identified by the *2022 Annual Threat Assessment of the U.S. Intelligence Community*.[22] In addition, we interviewed officials from key federal agencies and obtained the perspectives of relevant industry stakeholders to confirm, add, or remove cyber threat actors from our list.

To identify cybersecurity vulnerabilities to offshore oil and gas infrastructure, we reviewed reports developed by key federal and industry stakeholders, as well as our previous work on cybersecurity risks to critical infrastructure.[23] We also interviewed key federal agencies and obtained the perspectives of industry organizations to identify potential vulnerabilities and any related reports or assessments. To understand the potential impacts of a successful cyberattack on offshore oil and gas infrastructure, we reviewed reports describing the results of previous OT failures associated with offshore oil and gas infrastructure and discussed with federal officials the extent to which they would be similar, if caused

[20]The Oil and Natural Gas Information Sharing and Analysis Center serves as a central point of coordination and communication to aid in the protection of exploration and production, transportation, refining, and delivery systems of the oil and gas industry, through the analysis and sharing of trusted and timely cyber threat information, including vulnerability and threat activity specific to OT systems and supervisory control and data acquisition systems.

[21]The National Ocean Industries Association represents and advances the offshore energy industry, providing solutions to support communities and protect workers, the public, and the environment.

[22]GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, GAO-22-104256 (Washington, D.C.: June 21, 2022); *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021); *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019); and Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (February 2022).

[23]GAO-22-104256; GAO-21-81; and GAO-19-332.

by a threat actor.[24] In addition, we interviewed the key agencies and obtained the perspectives of industry organizations listed previously to identify any reported incidents and potential impacts of an attack on offshore oil and gas infrastructure.

To assess the extent to which BSEE has addressed cybersecurity risks to offshore oil and gas infrastructure, we reviewed documentation regarding actions that BSEE has taken and plans to take to identify and respond to cybersecurity threats to offshore oil and gas infrastructure. These documents included a draft strategic framework, a potential regulatory framework, budget justifications, bureau statements and press releases, and safety alerts. We also interviewed officials from BSEE and other key federal agencies regarding past and planned bureau actions to address cybersecurity risks. We then compared BSEE's actions to address cybersecurity risks against National Institute of Standards and Technology (NIST) cybersecurity guidance and GAO criteria for developing and implementing effective program strategies.[25]

We conducted this performance audit from February 2022 to October 2022, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

[24]National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling: Report to the President* (January 2011); U.S. Department of the Interior Outer Continental Shelf Safety Oversight Board, *Report to Secretary of the Interior Ken Salazar* (Sept. 1, 2010); and Office of Inspector General, *A New Horizon: Looking to the Future of the Bureau of Ocean Energy Management, Regulation and Enforcement* (December 2010). We also reviewed reports documenting the results of BSEE panel investigations, which the bureau conducts in response to severe or technically complex incidents, such as a fatality, serious injury, or significant pollution event.

[25]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Apr. 16, 2018); *Guide to Operational Technology (OT) Security*, Special Publication 800-82- Rev. 3 Initial Public Draft (Gaithersburg, MD: April 2022); GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, GAO-05-372 (Washington, D.C.: Sept. 8, 2005); *Managing for Results: Practices for Effective Agency Strategic Reviews*, GAO-15-602 (Washington, D.C.: July 29, 2015); and *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, GAO-17-300 (Washington, D.C: Apr. 6, 2017).

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Offshore Oil and Gas Operations and Supporting Technology

Oil and gas infrastructure are divided among the following three categories: upstream (e.g., exploration and drilling); midstream (e.g., transportation); and downstream (e.g., processing, refining, and delivery to customers). Offshore oil and gas operations comprise components of the nation's upstream and midstream infrastructure. The life cycle of offshore operations includes activities to explore for potentially viable oil and gas sources, examine potentially viable sites, develop infrastructure needed to drill for and extract oil and gas, extract and transport oil and gas, and decommission relevant platforms.

Modern offshore oil and gas operations heavily rely on OT systems to support activities across the life cycle of offshore operations, including processes to extract and separate fluids (e.g., water, oil, and natural gas), and the monitoring of temperature and pressure during those processes. In addition, remote access capabilities in the OT systems allow system operators to monitor and control operations from onshore control centers. Of note, although most offshore oil and gas platforms have personnel onsite, unmanned oil and gas production is becoming increasingly common.

Energy Critical Infrastructure Sector Roles and Responsibilities

The nation's critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the U. S., that the incapacity or destruction of them would have a debilitating impact on U.S. security, economic stability, public health or safety, or any combination of these factors.[26] Presidential Policy Directive 21 identified the energy sector, which includes offshore oil and gas, as one of the 16 critical infrastructure sectors.

In addition, Presidential Policy Directive 21 and federal law made DOE the sector risk management agency for the energy sector, which includes

[26]42 U.S.C. § 5195c(e).

offshore oil and gas operations.[27] Specifically, DOE is responsible for leading, facilitating, and supporting the security and resilience programs and associated activities of the energy sector in an all-hazards environment (including cyber threats) in coordination with DHS, among other duties.[28]

The directive also called for DHS to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA as an operational component agency within DHS.[29] As the lead federal agency responsible for coordinating the national effort to understand and manage risk to critical infrastructure, CISA has a critical

[27]Presidential Policy Directive 21 refers to these agencies as "sector-specific agencies." The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: February 2013). See also Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003(c)(2), 129 Stat. 1312, 1779 (2016) (codified at 6 U.S.C. § 121 note). After enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Sector-Specific Agencies became known as Sector Risk Management Agencies. Pub. L. No. 116-283, § 9002(a)(7), (c)(2), 134 Stat. 3388, 4768–73 (2021) (codified as amended at 6 U.S.C. §§ 651(5), 652a).

[28]We have previously reported on DOE's efforts to address cybersecurity risks facing the energy sector. For example, in February 2018, we found that DOE had taken action to facilitate adopting NIST's voluntary cybersecurity framework within the energy sector. See GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018). However, we reported that DOE had not developed qualitative or quantitative measures of framework adoption. As a result, we recommended that DOE develop methods for determining the level and type of framework adoption by entities across their respective sectors. DOE neither agreed nor disagreed with this recommendation. As of August 2022, DOE has not implemented this recommendation.

[29]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168–74 (codified as amended at 6 U.S.C. § 652). Since its establishment, CISA has been reorganizing offices and functions previously organized under the department's National Protection and Programs Directorate and aligning its new organizational structure with its mission. See GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236 (Washington, D.C.: Mar. 10, 2021).

responsibility to effectively coordinate and consult with its federal, state, local, territorial, tribal, and private sector partners.[30]

The *National Infrastructure Protection Plan* further integrates critical infrastructure protection efforts between government and the private sectors.[31] The plan recognizes that some sectors are regulated by federal or state regulatory agencies that are not the designated sector risk management agency for the sector. In these cases, regulators possess unique insight into the functioning of the critical infrastructure they oversee and bring key capabilities to the critical infrastructure partnership,[32] including

- ensuring sector resilience through the policymaking and oversight process,
- encouraging critical infrastructure owners and operators to participate in public-private partnerships (e.g., sharing with information sharing and analysis centers), and
- coordinating with other agencies on critical infrastructure security and resilience initiatives.

[30]We have previously reported on DHS's efforts to address cybersecurity challenges facing the energy sector. For example, in March 2021, we reported that CISA had developed a new catalog of its products and services to inform the agency's stakeholders (including energy sector owners and operators) of available services, encourage information sharing, and promote the protection of digital systems. See GAO-21-236. However, we also reported that selected government and private-sector stakeholders from the 16 critical infrastructure sectors, including the energy sector, had noted a number of challenges in coordinating with CISA. Because CISA had not developed strategies to address all of these challenges, we made three recommendations to DHS to do so. DHS concurred with our recommendations. As of September 2022, DHS had not implemented our recommendations.

[31]Department of Homeland Security, *NIPP* [*National Infrastructure Protection Plan*] *2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[32]We have previously reported on federal regulatory agencies' efforts to address cybersecurity risks—including those facing OT systems in the energy sector. For example, in August 2019, we reported that the electric grid—particularly its OT systems—faced various cybersecurity risks. In addition, we reported that the Federal Energy Regulatory Commission had approved mandatory grid cybersecurity standards. See GAO-19-332. However, the commission had not ensured that those standards address federal guidance, specifically NIST's voluntary cybersecurity framework. To address these issues, we made two recommendations to the Federal Energy Regulatory Commission. DOE and the Federal Energy Regulatory Commission agreed with our recommendations; however, as of September 2022, these recommendations had not been implemented.

BSEE's Role on the Outer Continental Shelf

BSEE is responsible for overseeing offshore oil and gas operations. The bureau's mission is to promote safety, protect the environment, and conserve resources offshore through regulatory oversight and enforcement. It is responsible for overseeing offshore operations, which includes the authority to investigate incidents that occur on the OCS, monitor operator compliance with environmental stipulations, and take enforcement actions against operators that violate safety or environmental standards.

BSEE's regulatory programs advise a wide range of offshore activities and facilities, including drilling, well completion, production, pipeline, and decommissioning operations. The bureau implements advancements in technology and conducts onsite inspections to assure compliance with regulations, lease terms, and approved plans. To date, BSEE's regulations do not explicitly mention cybersecurity, but the bureau has determined that addressing cybersecurity risks to offshore oil and gas infrastructure aligns with its mission to promote safety and protect the environment.

BSEE's headquarters is responsible for setting national program policy to meet the bureau's mission. BSEE's three regional offices—the Gulf of Mexico regional office in New Orleans, Louisiana; the Pacific regional office in Camarillo, California; and the Alaska regional office in Anchorage, Alaska—are responsible for executing oversight of oil and gas activities, such as conducting inspections of all facilities on the OCS.

Offshore Oil and Gas Infrastructure Faces Significant and Increasing Cybersecurity Risks

Offshore oil and gas infrastructure faces significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts. Threat actors are becoming increasingly capable of carrying out attacks on critical infrastructure, including offshore oil and gas infrastructure. At the same time, the infrastructure is becoming more vulnerable to attacks. More specifically, the OT in oil and gas infrastructure is increasingly vulnerable to being exploited in cyberattacks that could result in serious harm to human safety, the environment, and the economy.

Various Threat Actors Are Increasingly Capable of Carrying Out Cyberattacks Against Offshore Oil and Gas Infrastructure

According to the *2022 Annual Threat Assessment of the U.S. Intelligence Community*, China, Iran, North Korea, and Russia pose the greatest cyber threats. Of particular concern, these countries possess the ability to launch cyberattacks that could have disruptive effects on critical

infrastructure.[33] Further, the assessment stated that transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide.[34] In addition, hackers and hacktivists,[35] as well as insiders, pose significant cyber threats to offshore oil and gas infrastructure, according to federal agency officials and representatives of nonfederal entities whom we interviewed. Table 1 describes potential threat actors to offshore oil and gas infrastructure.

[33]Office of the Director of National Intelligence*, Annual Threat Assessment of the U.S. Intelligence Community* (February 2022).

[34]Ransomware is a type of malware (i.e., malicious software) used to deny access to IT systems or data and to hold systems or data hostage until a ransom is paid.

[35]Hackers break into networks for reasons that include the challenge, revenge, stalking, or monetary gain. By contrast, hacktivists are ideologically motivated actors who use cyberattack tools to further political goals.

Table 1: Threat Actors That May Pose Significant Threats to Offshore Oil and Gas Infrastructure

Threat actors	Description and potential motivation	Examples of past cyberattacks
Nations	Nations, including nation-states, state-sponsored, and state-sanctioned groups or programs, use cyber tools as part of their efforts to further economic, military, and political goals. Chinese and Russian cyber threat actors have previously targeted the U.S. energy sector, including oil and gas companies. In addition, Iran has previously targeted foreign oil and gas companies, using cyberattack techniques.	According to the Cybersecurity and Infrastructure Agency (CISA) and the Federal Bureau of Investigation, from December 2011 to 2013, state-sponsored Chinese actors conducted a spearphishing and intrusion campaign targeting U.S. oil and gas pipeline companies.[a] Of the 23 targeted pipeline operators, 13 were confirmed compromises. In August 2012, malicious cyber actors attacked Saudi Aramco, the world's largest oil producer, and deleted information on about 30,000 workstations in the company's network. The attackers likely used the Shamoon malware, which the U.S. government has attributed to Iranian cyber actors.[b] In 2015, Russian cyber actors conducted a cyberattack on the Ukrainian power grid that systematically disconnected substations, resulting in a power outage for about 225,000 customers.[c]
Transnational criminal groups	Transnational criminal groups,[d] including organized crime organizations, seek to use cyberattacks for monetary gain. Further, cyber criminals are increasing the number, scale, and sophistication of ransomware[e] attacks that threaten to cause greater disruptions of critical services.	In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyberattack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. According to a joint advisory released by the Department of Homeland Security and the Federal Bureau of Investigation, the company proactively disconnected certain systems that monitor and control physical pipeline functions to ensure the safety of the pipeline.[f] Disconnecting these systems resulted in a temporary halt to all pipeline operations, which led to gasoline shortages throughout the southeast U.S.
Hackers and hacktivists[g]	Hackers break into networks for reasons including the challenge, revenge, stalking, or monetary gain. In contrast, hacktivists are ideologically motivated actors who use cyberattack tools to further political goals. According to U.S. Coast Guard officials, the agency considers environmental groups opposed to petroleum development to be a threat actor that could potentially target offshore oil and gas infrastructure.	The hacker activist group Anonymous threatened to target the oil and gas sector in a June 20, 2013, operation. Specifically, the group said that it would target several countries, including the U.S., China, and Russia. Press reporting indicated that the threats did not result in significant disruptions.
Insiders	Insiders are individuals (such as employees, contractors, or vendors) with authorized access to an information system or enterprise and who have the potential to cause harm, wittingly or unwittingly, through the destruction, disclosure, or modification of data, or through denial of service. Bureau of Safety and Environmental Enforcement officials indicated that insiders, such as a disgruntled employee, could cause issues on an offshore oil and gas facility.	In 2009, a federal grand jury indicted a disgruntled employee on allegations of intentionally disabling a computer system that monitored for leaks on three platforms off the shore of Huntington Beach, California.

Sources: Prior GAO work and summary of relevant documentation. | GAO-23-105789

[a]Cybersecurity and Infrastructure Security Agency, Joint Cybersecurity Advisory, "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013" (Alert AA21-201A), accessed Aug. 12, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa21-201a.

[b]Cybersecurity and Infrastructure Security Agency, ICS Joint Security Awareness Report (JSAR-12-241-01B), last accessed by Aug. 12, 2022, https://www.cisa.gov/uscert/ics/jsar/JSAR-12-241-01B.

[c]Cybersecurity and Infrastructure Security Agency, ICS Alert: Cyber-Attack Against Ukrainian Critical Infrastructure (IR-ALERT-H-16-056-01), last accessed Aug. 12, 2022, https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[d]Transnational criminal groups have used ransomware to target IT systems and subsequently disrupt vulnerable operational technology systems.

[e]The National Institute of Standards and Technology defines ransomware as a type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

[f]Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks, Alert (AA21-131A) (May 11, 2021).

[g]Hackers and hacktivists no longer need a great amount of skill to compromise IT systems because they can download commonly available cyberattack tools. Hackers and hacktivists may have less capability to do harm than nations, but their intent to inflict harm or to damage operations is typically more immediate than nations with longer-term goals.

Threat actors are becoming increasingly capable of conducting damaging cyberattacks. For example, hackers and hacktivists no longer need a great amount of skill to compromise business IT systems because of the growing availability of public and commercial cyberattack tools. Additionally, in 2022, the Federal Bureau of Investigation observed that several ransomware groups had developed code designed to stop critical infrastructure or industrial processes. Furthermore, threat actors may become even more capable—particularly with advances in artificial intelligence.[36]

Offshore Oil and Gas Infrastructure Are Increasingly Vulnerable to Cyberattacks

According to agency officials and industry representatives, OT in offshore oil and gas infrastructure is becoming increasingly vulnerable to cyberattacks. Most notably, OT systems were once largely isolated from internet and business IT systems but are now frequently connected with those systems both within a company and accessible by internet systems

[36]According to the National Security Commission on Artificial Intelligence, the expanding application of existing artificial intelligence capabilities will make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale. The National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

globally. As a result, cyberattacks are now more likely to originate in business IT systems and migrate to OT.[37]

According to MITRE's widely accepted framework for classifying cyberattacks, threat actors can use multiple techniques to gain initial access to OT used to control offshore oil and gas infrastructure.[38] Table 2 describes publicly reported examples of such techniques.[39]

[37]More specifically, USCG officials stated that since the *Deepwater Horizon* incident, companies have incorporated more tools and services to enable remote access and monitoring of offshore oil and gas infrastructure. For example, large companies can control drilling processes from onshore, according to BSEE officials.

[38]MITRE Corporation, Main Page, "ATT&CK® for Industrial Control Systems," last modified on June 3, 2020, https://collaborate.mitre.org/attackics/index.php/Main_Page. The MITRE ATT&CK® Framework for Industrial Control Systems is an overview of the tactics and techniques, including corresponding examples that could be used to attack industrial control systems. This framework defines a technique as the way in which a threat actor achieves their goal by performing an action.

[39]Some of the examples included in table 2 do not directly relate to offshore oil and gas infrastructure but reflect examples of attacks on OT generally that may be relevant to OT used on the offshore oil and gas infrastructure.

Table 2: Techniques Employed to Exploit Cybersecurity Vulnerabilities

Description	Examples
Attackers may exploit internet-accessible devices in operational technology (OT) systems.	In 2012, attackers used automated tools to discover General Electric industrial control systems devices connected to the internet.[a] The attackers then exploited this connection to infect the devices with malware.[b]
Attackers may compromise the supply chain[c] of OT systems by manipulating products (such as hardware or software) or delivery mechanisms before receipt by the end consumer.	In 2018, Schneider Electric issued an alert regarding certain solar system monitoring devices that were packaged with universal serial bus (USB) removable media that one of its suppliers contaminated with malware during manufacturing.[d] According to a Finnish cybersecurity company, in 2014, a group of attackers used malware to compromise the software installers for industrial control systems devices available on the websites of three vendors based in Europe. According to the cybersecurity company's research, this malware infected multiple organizations in Europe and at least one company in California. The malware reportedly gathered information about other industrial control systems' devices connected to the infected devices and sent this information to servers that the malicious actors controlled.
Attackers may send a specific individual, company, or industry a "spearphishing" email with links or attachments that include malicious code to gain access to a corporate network.	According to a report from the Electricity Information Sharing and Analysis Center and the SANS Institute, in 2015, malicious actors sent spearphishing emails with malware embedded in Microsoft Word attachments to users on three Ukrainian electricity utilities' business IT networks.[e] When users opened the Microsoft Word attachments, the malware was installed on the users' systems.
Attackers may exploit services that allow users to connect to network resources from a remote location (e.g., virtual private network[f]). The attackers then use these services to access and attack OT networks.	After gaining initial access to the business IT networks of the three regional Ukrainian electricity distribution utilities in 2015, attackers compromised the virtual private networks that the utilities used to connect business IT networks to OT networks.[g] This compromise was enabled by the attacker's harvesting of legitimate credentials from the business IT network and then using them to access the virtual private network, which likely did not require multifactor authentication.[h]

Sources: GAO analysis and summary of relevant documents, prior GAO work, and summary of relevant information from the MITRE ATT&CK® Matrix for Enterprise and Matrix for Industrial Control Systems. | GAO-23-105789

[a]National Institute of Standards and Technology guidance on industrial control systems security strongly encourages organizations not to directly expose industrial control systems devices to the internet. National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security, NIST 800-82 Rev. 2 (Gaithersburg, MD: May 2015). Yet search engines that catalog industrial control systems (e.g., Shodan) suggest that industrial control systems remain directly exposed to the internet.

[b]Cybersecurity and Infrastructure Security Agency, ICS Alert: Ongoing Sophisticated Malware Campaign Compromising ICS (ICS-ALERT-14-281-01E), accessed Aug. 5, 2022, https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-281-01B.

[c]The supply chain is a linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of products and services and extends through development, sourcing, manufacturing, handling, and delivery of products and services to the acquirer.

[d]Schneider Electric, Security Notification – USB Removable Media Provided with Conext Combox and Conext Battery Monitor (Andover, MA: Aug, 24, 2018).

[e]Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid (Washington, D.C.: Mar. 18, 2016).

[f]A virtual private network is a logical network connection that overlays existing physical networks to provide secure transmission of data.

[g]Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid (Washington, D.C.: Mar. 18, 2016).

[h]Multifactor authentication uses two or more different factors to achieve authentication. Factors may include (i) something the user knows (e.g., password/PIN); (ii) something the user has (e.g., cryptographic identification device, token); or (iii) something the user is (e.g., biometric factor).

According to the MITRE cyberattack framework, after gaining initial access to OT, attackers may use other tactics—such as execution (i.e., running malicious code), evasion (i.e., avoiding detection), and lateral movement (i.e., moving through the OT environment)—to position themselves to achieve their ultimate goals of manipulation or interruption of OT systems. According to relevant federal guidance,[40] OT systems—including those used by offshore oil and gas operators—may be vulnerable to these tactics because of poor cybersecurity practices related to, for example, encryption,[41] authentication,[42] patch management,[43] and configuration management.[44]

As we have previously reported,[45] these and other vulnerabilities in offshore oil and gas OT systems may also stem from factors such as the following:

[40]National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, Special Publication 800-82- Rev. 3.

[41]NIST defines "encryption" as the translation of data into a form that is unintelligible without a deciphering mechanism. National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, NIST SP 800-47 (Gaithersburg, MD: August 2002).

[42]NIST defines "authentication" as the verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Gaithersburg, MD: January 2015).

[43]NIST defines "patch management" as the systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as "patches," "hot fixes," and "service packs." National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST SP 800-137 (Gaithersburg, MD: September 2011).

[44]NIST defines "configuration management" as a collection of activities focused on establishing and maintaining the integrity of industrial control systems through control of processes for initializing, changing, and monitoring the configurations of those products. National Institute of Standards and Technology, *Security and Privacy Controls*.

[45]GAO-21-81; GAO-19-332.

- Older legacy systems were not designed with cybersecurity protections because they were not intended to connect to networks such as the internet. For example, many legacy devices are not able to authenticate commands to ensure that they have been sent from a valid user and may not be capable of running modern encryption protocols. In addition, some legacy devices do not have the capability to log commands sent to the devices, making it more difficult to detect malicious activity. Further, older legacy systems often rely on unsupported operating systems that no longer receive modern software security patches to address vulnerabilities.
- Systems components often have to be taken offline so that owners and operators can apply security patches to address known cybersecurity vulnerabilities. However, this may not happen in a timely manner because the devices must remain highly available to support the reliable operation of offshore oil and gas infrastructure.

Successful Cyberattacks Could Result in Severe Impacts

The extent of past cyberattacks on offshore oil and gas infrastructure is unclear. Specifically, no federal officials or industry representatives we contacted were aware of any cyberattacks against offshore oil and gas infrastructure or specific requirements to report them if they occur.[46] However, successful cyberattacks against offshore oil and gas infrastructure could have potentially severe effects on safety, the environment, and the economy.

We identified reports of two cybersecurity incidents involving offshore oil and gas infrastructure in the course of our review.[47] Specifically:

[46]The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires CISA to promulgate rules requiring "covered entities" to report "covered cyber incidents" and ransom payments. Pub. L. No. 117-103, § 103(a)(2), 136 Stat. 49, 1042–48. The Cyber Incident Reporting for Critical Infrastructure Act requires a Notice of Proposed Rulemaking to be published within 24 months of the statute's enactment (i.e., by March 2024) and a final rule to be issued within 18 months of the Notice of Proposed Rulemaking's publication (i.e., no later than September 2025). It is unclear whether the "covered entities" will include owners and operators within the offshore oil and gas subsector.

[47]These examples were not identified via a formal literature review and therefore, might not represent a comprehensive listing of publicly reported cybersecurity incidents involving offshore oil and gas infrastructure. In addition, we identified two other cybersecurity incidents based on press reporting, but we were unable to corroborate those reports. Specifically, in 2010, an offshore rig traveling from South Korea suffered a cybersecurity incident involving malware that took the blowout preventer system offline, according to press reporting. It reportedly took engineers 19 days to fix the issue and make the offshore rig operational. Further, in 2015, hackers caused an offshore oil rig off the coast of Africa to tilt to one side, according to press reporting. Operations and production were reportedly shut down for a week while technicians worked to resolve the issue.

- In 2009, a grand jury indicted a former employee of an offshore oil and gas entity on allegations of temporarily disabling a computer system for detecting pipeline leaks for three oil derricks off the southern California coast.
- In 2015, a USCG official made statements regarding a cybersecurity incident where malware was unintentionally introduced onto a mobile offshore drilling unit. According to the USCG, the malware affected the dynamic positioning system, which resulted in the need to maneuver to avoid an accident.

Future successful cyberattacks against offshore oil and gas infrastructure could have severe consequences. For example, significant disruptions and other harms that resulted from successful cyberattacks in other industrial sectors can serve as proxies for potential impacts to offshore oil and gas infrastructure. Table 3 describes five publicly reported examples of impacts from cyberattacks on OT in other industrial sectors that could be similar to the effects of attacks on offshore oil and gas infrastructure.

Table 3: Potential Impacts of Cyberattacks on Operational Technology (OT) Systems in the Offshore Oil and Gas Subsector

Impact	Description[a]	Example
Damage to property	Malicious actors may damage or destroy infrastructure, equipment, and the surrounding environment when attacking control systems. This may result in device and operational equipment breakdown or represent tangential damage from other techniques used in an attack.	In December 2014, a cyberattack resulted in the misoperation of an OT system, including the improper shutdown of a furnace and physical damage to a German steel mill's facilities.[b]
Loss of productivity and revenue	Attackers may cause loss of productivity and revenue by damaging or disrupting the availability or integrity of industrial control systems operations, devices, and related processes.	In December 2019, a form of ransomware named EKANS infected various OT devices, reportedly in the U.S., Europe, and Japan, by encrypting files and displaying a ransom note, which impaired operations.[c]
Loss of safety	Attackers may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.	In 2017, Russian cyber actors manipulated a foreign oil refinery's safety devices, which resulted in the refinery shutting down for several days.[d]
Loss or denial of control	Malicious actors may seek to prevent operators and engineers from interacting with process controls.	In the 2015, Russian attackers uploaded malicious software to certain devices in Ukraine, with the intent of ensuring that utility operators could not issue remote commands to bring electricity substations back online.[e]
Manipulation of control	Command messages are used in OT networks to give direct instructions to devices. Attackers may send unauthorized command messages to instruct industrial control systems devices to perform actions outside their desired functionality for process control.	In the 2015 Ukrainian attacks, Russian attackers issued unauthorized commands to open the breakers at substations that three regional electricity utilities managed, causing a loss of power to about 225,000 customers.[e]

Sources: Prior GAO work and summary of relevant information from the MITRE ATT&CK® Matrix for Enterprise and Matrix for Industrial Control Systems. | GAO-23-105789

[a]These tactics to affect OT are not mutually exclusive. Some tactics may be used in conjunction with one another.

[b]SANS Industrial Control Systems, ICS CP/PE (Cyber-to-Physical or Process Effects) (case study paper): German Steel Mill Cyber Attack (Rockville, MD: Dec. 30, 2014).

[c]Dragos, EKANS Ransomware and ICS Operations, accessed November 25, 2020, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[d]Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Energy, Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector, Alert (AA22-083A) (Mar. 24, 2022).

[e]Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid (Washington, D.C.: Mar. 18, 2016).

BSEE and USCG officials indicated that the effects of a successful cyberattack would likely resemble that of other incidents related to OT systems that have occurred on the OCS. According to BSEE incident investigation documentation, these can include deaths and injuries, damaged or destroyed equipment, and pollution to the marine environment. However, in a worst-case OT failure scenario, all these impacts can occur simultaneously at a catastrophic scale. For example, the failure of the mobile offshore drilling unit Deepwater Horizon's blowout preventer—an OT system—contributed to its explosion and sinking (see fig. 2), as well as 11 deaths, serious injuries, and the largest marine oil spill in the history of the U.S. (approximately 4.9 million barrels). Additionally, according to PHMSA officials, cyberattacks against pipeline OT—such as valves controlling oil and gas flow—could disrupt production and transmission and, thereby, negatively affect energy supplies, markets, and the economy.[48]

[48]For example, in May 2021, the Colonial Pipeline Company announced that it was the victim of a ransomware attack that led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast U.S.

Figure 1: Deepwater Horizon on Fire, with Supply Boats Responding

Source: United States Coast Guard. | GAO-23-105789

According to BSEE officials, the severity of these impacts could be mitigated by on-site manual controls that can override automated systems. Specifically, these officials stated that operators have the ability to manually shut down operations, in the event of an emergency, to prevent the worst outcomes. However, these statements were generally based on the professional experience of the BSEE officials we interviewed, and they were not aware of any assessments confirming that manual controls could mitigate the impacts of cyberattacks. For example, the *Deepwater Horizon's* blowout preventer was designed to be activated by crew members, a remotely operated vehicle,[49] or an automated emergency system. However, these mechanisms did not prevent the blowout that contributed to the *Deepwater Horizon* disaster, indicating that such OT systems are not foolproof.

[49]Remotely operated vehicles are unoccupied, highly maneuverable underwater machines operated by a controller at the water surface.

BSEE Has Taken Few Actions to Address Cybersecurity Risks to Offshore Oil and Gas Infrastructure

BSEE has recognized the need to address cybersecurity risks to offshore oil and gas infrastructure since at least 2015 but has made little progress in doing so. Specifically, we identified at least two prior efforts in which BSEE started an initiative, but no resulting actions were taken to address cybersecurity issues.

- In August 2015, BSEE determined that it needed to address quick-developing and constantly changing cybersecurity risks to offshore oil and gas infrastructure.[50] According to its statement at the time, the bureau sought to better understand and develop cybersecurity risk management practices and work with other entities, such as USCG, to address this quickly emerging offshore risk. BSEE indicated that it was researching the subject in order to inform future decision-making. However, BSEE officials we interviewed told us that they are unaware of any results from this effort.
- In October 2020, recognizing a growing urgency to address cybersecurity risks, BSEE developed a draft strategic framework for overseeing the cybersecurity of oil and gas infrastructure on the OCS.[51] Specifically, the draft framework described (1) the relevance of cybersecurity risks to BSEE's mission; (2) the authorities of BSEE and other federal agencies—including CISA, DOE, PHMSA, and USCG—with relevant critical infrastructure or other OCS oversight roles;[52] (3) BSEE interaction with stakeholders, such as industry organizations and the Oil and Natural Gas Subsector Coordinating Council;[53] and (4) steps that the bureau could take to establish a

[50]Bureau of Safety and Environmental Enforcement, *BSEE & Coast Guard Confront Offshore Cyber Attack Issues* (Aug. 4, 2015). https://www.bsee.gov/blog-post/8042015

[51]Bureau of Safety and Environmental Enforcement, *Draft Framework for BSEE Cybersecurity Activities: Cybersecurity Risks, Responsibilities, and Regulations, and a Proposed Cybersecurity Oversight Role for the Bureau of Safety and Environmental Enforcement* (Oct. 29, 2020).

[52]BSEE's draft strategic framework identified an immediate need to establish and formalize working relationships with its primary federal partners.

[53]According to BSEE's draft strategic framework, industry participation on the Oil and Natural Gas Subsector Coordinating Council has been, and will likely remain, inconsistent until the cybersecurity risks to OCS operations and solutions to address them are clearer.

cybersecurity program.[54] The draft framework also recommended that BSEE coordinate with other federal agencies to assess and promote more effective management of cybersecurity risks to the OT of industry on the OCS. However, BSEE officials we interviewed described the draft framework as an internal white paper to inform the bureau of the importance of addressing cybersecurity risks. These officials told us that BSEE never formally adopted or implemented the framework.

Since 2020, BSEE has issued two safety alerts to industry recommending that operators follow CISA guidance.[55] Specifically, in September 2020, BSEE warned that CISA was aware of multiple vulnerabilities that could allow a highly skilled attacker to remotely take control of various OT, such as those that open and close valves or control system flow rates and pressures.[56] Subsequently, in March 2022, because of the potential for increased threats to U.S. infrastructure associated with the war in Ukraine,[57] BSEE encouraged OCS operators to strengthen and

[54]BSEE identified the need to engage in risk assessment activities, hire a cybersecurity specialist, support the development and application of cybersecurity-related standards, and formalize relationships with other federal agencies, including drafting a cybersecurity-specific memorandum of understanding with USCG. BSEE proposed that, subsequent to assessment, the bureau should work with industry to detect cybersecurity compromises, advise it of available resources to protect OT, and move it from a reactive to a proactive paradigm. Activities would likely involve clarifying incident reporting rules, expanding BSEE investigative skillsets, and possible modifications or clarifications to BSEE regulations. BSEE officials told us that they currently believe that the incorporation of cybersecurity standards into a future iteration of the bureau's Safety and Environmental Management System regulations is a viable pathway toward addressing cybersecurity risk.

[55]A safety alert is a tool used by BSEE to inform the offshore oil and gas industry of the circumstances surrounding a potential safety issue. An alert may also include recommendations that could assist in avoiding potential incidents on the OCS.

[56]Bureau of Safety and Environmental Enforcement, *Recently Discovered Cybersecurity Vulnerabilities May Impact Energy Company Industrial Control Systems*, Safety Alert No. 394 (Sept. 25, 2020).

[57]According to CISA, Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks.

systematize their cybersecurity defenses and regularly monitor the guidance issued by CISA.[58]

Earlier this year, in its fiscal year 2023 budget justification, BSEE proposed developing a foundational cybersecurity capability in the form of an offshore cybersecurity safety threats program to work with industry on decreasing cybersecurity risks to OT and infrastructure on the OCS. Similar to its draft 2020 strategic framework, BSEE identified immediate goals of initiating cybersecurity staffing, developing programmatic documentation and policy, and engaging with federal agencies and industry stakeholders to address cybersecurity risks on the OCS.[59]

More than 7 years have elapsed since BSEE explicitly identified the need to address cybersecurity risks to offshore oil and gas infrastructure, but the bureau remains in the early stages of establishing a program to do so. Our past work has shown that having a strategy is a starting point and basic underpinning for better managing federal programs and activities.[60] For example, a strategy can enhance the ability of agency officials and congressional decision makers to ensure accountability and provide oversight. Our prior work has highlighted the importance of following key characteristics for effective strategies—including those pertaining to critical infrastructure cybersecurity programs:

- **Risk assessment.** Assess the risks to critical assets and operations. We have also previously highlighted the importance of performing a cybersecurity risk assessment to help inform the steps that agencies

[58]Bureau of Safety and Environmental Enforcement, *Check Your Cybersecurity Readiness*, Safety Alert No. 434 (Mar. 21, 2022).

[59]This proposal also described BSEE intentions to work with CISA and others to program voluntary validated architecture design reviews to (1) reduce risk to critical infrastructure components; (2) analyze related energy systems based on standards, guidelines, and best practices; (3) promote effective defense-in-depth strategies; and (4) provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture. A validated architecture design review is a cybersecurity infrastructure assessment based on federal and industry standards, guidelines, and best practices of current regulated industry cybersecurity practices. CISA officials told us that offshore operators have not used the cybersecurity services that it currently offers.

[60]GAO-04-408T; GAO-05-372; GAO-15-602; and GAO-17-300.

should take when developing a critical infrastructure cybersecurity program.[61]

- **Objectives, activities, and performance measures.** Addresses what the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability. When defining the steps to achieve results, we have previously highlighted the importance of agencies determining whether they should act in a regulatory or advisory role.[62] We have also previously highlighted the importance of relying on NIST cybersecurity guidance to identify practices that critical infrastructure owners and operators should follow.[63]
- **Roles, responsibilities, and coordination.** Addresses who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts.
- **Identification of needed resources and investments.** Addresses what the strategy will cost and the types of resources and investments needed.

However, BSEE has not developed a strategy to guide the development of its cybersecurity program. In May 2022, BSEE hired a cybersecurity specialist to serve as the senior principal bureau contact for assignments and projects related to cybersecurity matters. BSEE officials told us that this specialist is responsible for developing the cybersecurity program and will spend the remainder of fiscal year 2022 learning about the bureau, establishing contacts with other government agencies and industry, and coordinating with other BSEE program personnel. However, BSEE officials also told us that until the specialist is adequately versed in the relevant issues and entities, formal program development and implementation will be paused. The officials stated that the program is in

[61]See, e.g., GAO-19-332; and GAO, *Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning*, GAO-18-62 (Washington, D.C.: Oct. 30, 2017).

[62]See, e.g., GAO, *Regulatory Guidance Processes: Selected Departments Could Strengthen Internal Control and Dissemination Practices*, GAO-15-368 (Washington, D.C.: Apr. 16, 2015).

[63]See, e.g., GAO-19-332; and GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018); and National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Apr. 16, 2018); *Guide to Operational Technology (OT) Security*, Special Publication 800-82- Rev. 3.

the very early stages of development and that BSEE does not expect to begin making key programmatic decisions or drafting programmatic documents and policies until sometime in fiscal year 2023.

BSEE's commitment of minimal resources and lack of urgency in addressing cybersecurity risks reflect cybersecurity's relatively low priority within the bureau. Until such time as BSEE top management decides to make it a priority by establishing and implementing a strategy for its cybersecurity program that addresses the above characteristics, offshore oil and gas infrastructure will continue to be at risk.

Conclusions

BSEE has taken few actions to address cybersecurity risks to the more than 1,600 oil and gas facilities and structures on the OCS. This creates significant liability, given that a successful cyberattack on such infrastructure could have potentially catastrophic effects. Since recognizing the need to take action in 2015, the scale and scope of cybersecurity risks have continued to increase, creating even greater urgency for the bureau to respond. However, BSEE has struggled to address cybersecurity risks to offshore oil and gas infrastructure and only recently has taken steps to start a new initiative.[64] This effort remains in the earliest stages of development. Accordingly, it is not guided by an overarching strategy that identifies cybersecurity risks; relevant practices to address those risks; the bureau's role in addressing them; milestones for activities such as formalizing relationships with other federal agencies and industry organizations; resource needs, such as appropriate staffing levels; and performance measures to assess results. Without a strategy to guide the development and implementation of its new cybersecurity program that incorporates these key features, the effectiveness of any cybersecurity program that BSEE ultimately establishes could be constrained. This, in turn, would jeopardize the bureau's ability to address the significant and increasing cybersecurity risks facing offshore oil and gas infrastructure on the OCS.

[64]BSEE's limited progress in addressing cybersecurity risks to offshore oil and gas infrastructure is consistent with its recent difficulties in implementing other key internal efforts—including a restructuring of its oversight capabilities, several strategic and management initiatives, and updating its pipeline regulations—on which we have previously reported. See GAO, *Oil and Gas Management: Interior's Bureau of Safety and Environmental Enforcement Restructuring Has Not Addressed Long-Standing Oversight Deficiencies*, GAO-16-245 (Washington, D.C.: Feb. 10, 2016); *Oil and Gas Management: Stronger Leadership Commitment Needed at Interior to Improve Offshore Oversight and Internal Management*, GAO-17-293 (Washington, D.C.: Mar. 21, 2017); and *Offshore Oil and Gas: Updated Regulations Needed to Improve Pipeline Oversight and Decommissioning*, GAO-21-293 (Washington, D.C.: Mar. 19, 2021).

Recommendation for Executive Action

The BSEE Director should immediately develop and implement a strategy to guide the development of its most recent cybersecurity initiative; such a strategy should include (1) a risk assessment; (2) objectives, activities, and performance measures; (3) roles, responsibilities, and coordination; and (4) identification of needed resources and investments. (Recommendation 1)

Agency Comments

We provided a draft copy of this report to the Departments of the Interior, Energy, Homeland Security, and Transportation. In an email, we were informed that Interior generally concurred with our findings and recommendation. The Departments of Energy and Homeland Security provided technical comments, which we incorporated as appropriate. The Department of Transportation told us they had no comments on the draft report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretaries of the Interior, Energy, Homeland Security, and Transportation; and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact us at (202) 512-3841 or ruscof@gao.gov or (202) 512-9342 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix I.

Frank Rusco
Director, Natural Resources and Environment

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

Frank Rusco, (202) 512-3841 or ruscof@gao.gov

Marisol Cruz Cain, (202) 512-9342 or cruzcainm@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Kaelin Kuhn (Assistant Director), David Marroni (Assistant Director), Matthew Tabbert (Analyst-in-Charge), Mark Braza, John Delicath, Wil Gerard, Darren Grant, Ceara Lance, David Matcham, and Dan Royer made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548