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

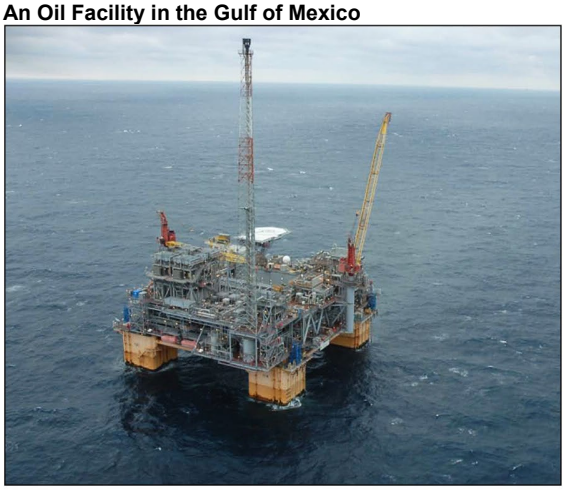
Offshore oil and gas infrastructure faces significant and increasing cybersecurity risks in the form of threat actors, vulnerabilities, and potential impacts.

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.