United States Senate
WASHINGTON, DC 20510

May 7, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Deb Haaland
Secretary
Department of the Interior

Dear Secretary Haaland:

An offshore network of nearly 1,400 facilities produces a significant portion of U.S. domestic oil and gas.[1] These facilities, relying on remote technology, face growing risks of cyberattacks.[2] Cyberattacks on these facilities threaten to disrupt oil and gas production, affecting the economic and national security of the United States. The Bureau of Safety and Environmental Enforcement (BSEE), located within the Department of Interior (DOI), is the lead agency tasked with ensuring the safety related to the offshore energy industry, primarily oil and natural gas, on the U.S. Outer Continental Shelf (OCS).[3]

The Government Accountability Office (GAO) published a report in October 2022 regarding the cybersecurity of offshore oil and gas facilities entitled, "*Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*."[4] This report outlined the need for an appropriate cybersecurity strategy, and noted that without an appropriate strategy, "offshore oil and gas infrastructure will continue to remain at significant risk."[5]

According to GAO, in 2015 and 2020, BSEE initiated efforts to address cybersecurity risks, but neither resulted in substantial action.[6] Specifically, the report notes that in 2015, BSEE recognized the need "to address cybersecurity risks for offshore oil and gas infrastructure."[7] But,

---

[1] Bureau of Safety and Environmental Enforcement, *OCS Facility Infrastructure*, https://bobson.maps.arcgis.com/apps/dashboards/400bba386d3d4ec58396dbaa559c422c.
[2] GAO, GAO-23-105789, *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risk to Infrastructure* (October 26, 2022) at 12-14, https://www.gao.gov/assets/d23105789.pdf. The report listed some examples of past cyberattacks: 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. Of the 23 targeted pipeline operators, 13 were confirmed compromises; 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. *See also* https://www.gao.gov/products/gao-23-105789 (Updates as to the status of the GAO recommendations).
[3] U.S. Dept. of the Interior, Bureau of Safety and Environmental Enforcement, *About BSEE*, https://www.bsee.gov/who-we-are/about-bsee.
[4] GAO Report at 1.
[5] *Id*. at 1-6.
[6] *Id*. at 21-23.
[7] *Id*. at 21.

according to GAO, "BSEE officials we interviewed told us that they were unaware of any results from this effort."[8] GAO's report also noted that in 2020, BSEE "developed a draft strategic framework for overseeing the cybersecurity of oil and gas infrastructure on the OCS."[9] Among other items, the draft recommended "BSEE coordinate with other federal agencies to develop the framework and cybersecurity strategies."[10] But, GAO found that BSEE didn't implement the framework.

As a result of the October 2022 report, GAO made one priority recommendation.[11] This recommendation states, in part, that "[t]he BSEE Director should immediately develop and implement a strategy to guide the development of its most recent cybersecurity initiative."[12] According to GAO, as of April 2024, BSEE "completed a cybersecurity strategy and began initial actions to implement it."[13]

It is imperative that BSEE and DOI continue to develop and implement plans to protect the oil and gas facilities it regulates. Additionally, is vitally important that BSEE ensure a strong U.S. cybersecurity defense of these facilities.

Accordingly, please answer the following questions no later than May 21, 2024:

1. What steps has DOI and BSEE taken to close the open priority recommendation from the October 2022 report? Provide all records.[14]

2. What does DOI consider to be the number one priority in the cybersecurity of the oil and gas facilities it regulates? How does DOI prioritize cybersecurity threats to these facilities? Provide all records.

3. While implementing BSEE's cybersecurity strategy, has it engaged private stakeholders in developing cybersecurity initiatives to protect oil and gas facilities? Please explain. If not, why not?

---

[8] *Id.*
[9] *Id*. at 21-22. The GAO report noted, "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. 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; (3) BSEE interaction with stakeholders, such as industry organizations and the Oil and Natural Gas Subsector Coordinating Council; and (4) steps that the bureau could take to establish a cybersecurity program. 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."
[10] *Id*.
[11] *Id*. at 26.
[12] *Id*.
[13] *Supra* note 2 (Updates as to the status of the GAO recommendations).
[14] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

4. What is DOI and BSEE's process to report and respond to cyberattacks in real time? Provide all records.

5. How many cyberattacks have occurred on the oil and gas facilities DOI and BSEE regulates? What is the process for DOI reporting cybersecurity threats and attacks to federal agencies, Congress, and private stakeholders? Provide all records.

In keeping with Executive Order 13526, please segregate all unclassified materials within the classified documents, and provide all unclassified information directly to the committee, and provide a classified addendum to the Office of Senate Security. Although the committee complies with all laws and regulations governing the handling of classified information, it is not bound, absent its prior agreement, by any handling restrictions.

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,

Charles E. Grassley
Ranking Member
Committee on the Budget