United States Department of the Interior
BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT
WASHINGTON, DC 20240-0001

LETTER TO LESSEES, OPERATORS, AND CONTRACTORS ENGAGED IN AUTHORIZED ACTIVITIES ON THE OUTER CONTINENTAL SHELF

Protection: Cybersecurity Threats on the Outer Continental Shelf

As critical infrastructure, offshore energy facilities are essential to the prosperity and wellbeing of our national economy. More than one thousand oil and gas facilities fall under the purview of the Bureau of Safety and Environmental Enforcement (BSEE), as well as a growing number of renewable energy facilities.

Offshore critical infrastructure faces significant challenges, threat actors, vulnerabilities, and potential impacts because of cyberattacks and intrusions. Various statutes, including the Outer Continental Shelf (OCS) Lands Act, the Maritime Transportation Security Act of 2002, and the Homeland Security Act provide Federal agencies with authorities related to cybersecurity, including the regulation of OCS activities. BSEE, the U.S. Coast Guard (USCG), and other Federal agencies work in partnership to support these regulatory mandates to mitigate cybersecurity vulnerabilities on the OCS.

The Government Accountability Office (GAO) issued a November 2022 report on "Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure."[1] This report outlines and highlights cybersecurity as a critical component of offshore infrastructure and operational safety. In response to the GAO report, BSEE developed a comprehensive cybersecurity strategy titled, "BSEE's Operational Technology (OT) Cybersecurity Strategy for the Outer Continental Shelf." BSEE's cybersecurity program focuses on reducing the offshore energy industry's vulnerabilities to threats and on strengthening cybersecurity through continuous coordination and communication among key federal agencies, including the USCG, the White House Office of the National Cyber Director, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA), and the Department of Energy. As a part of its strategy, BSEE is encouraging lessees to review their cybersecurity plans and ensure they address, in detail, both informational technology and OT systems. For more information, review BSEE's cybersecurity webpage, which includes BSEE's Cybersecurity Strategy Executive Summary. In addition, please review this fact sheet from DHS CISA regarding People's Republic of China state-sponsored cyber activity for more specific and recent cybersecurity concerns that could affect OCS facilities and actions you can take to reduce disruptions to critical systems.

BSEE, along with the USCG and other federal partners, remains committed to ensuring cybersecurity risks on the OCS are minimized. OCS lessees, operators, and contractors are reminded to report cybersecurity incidents in accordance with current law and regulations. Currently, all reporting for any cybersecurity related incidents should be made directly to the USCG's National Response Center (NRC) at 1-800-424-8802 or the NRC Watch Email at NRC@uscg.mil, and to the DHS CISA reporting number and email listed in the fact sheet.

If you have any questions about this letter to lessees, please contact Stacey Noem, BSEE's Office Chief of Offshore Regulatory Programs at Stacey.Noem@bsee.gov.

Kevin M. Sligh, Sr.
Director

[1] Government Accountability Office, Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure (2022). Retrieved from https://www.gao.gov/products/gao-23-105789.