BSEE

JANUARY 11, 2024

Operational Technology Cybersecurity Strategy For the U.S. Outer Continental Shelf

UNITED STATES DEPARTMENT OF THE INTERIOR (DOI)
BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT (BSEE)

Executive Summary

The President's 2023 National Cybersecurity Strategy describes the whole-of-government approach necessary to protect the critical infrastructure of the United States from potential cyberattacks by malicious threat actors. It states, "Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility and delivers a foundational level of security and resilience for our digital ecosystem."

In alignment with the President's policy guidance, this Operational Technology Cybersecurity Strategy describes how the Bureau of Safety and Environmental Enforcement (BSEE) will contribute to the safety and security of critical energy infrastructure on the Outer Continental Shelf (OCS), where the Bureau shares oversight responsibilities for the safe and secure operation of offshore oil, gas, and renewable energy facilities.

In the past, Industrial Control Systems (ICS) or Operational Technology (OT) systems on offshore energy facilities operated in isolation, without bridging over Information Technology (IT) infrastructures. However, modern integrated control technologies now enable remote access to those OT systems via an IT bridge.

Such access in turn introduces new vulnerabilities, which must be addressed to avoid potential harm to people or the environment. Unless addressed, these vulnerabilities may lead to an increase in the number and frequency of cyberattacks against offshore energy facilities. Malicious threat actors could exploit vulnerable devices or use malware attacks on networked services to gain access to critical operating systems and machinery, with the intent to cause equipment failure, mischief, or further disruption.

Given the importance of the offshore energy industry to the national interests of the United States, BSEE commissioned the development of this Strategy to help mitigate the risk of OT cybersecurity attacks on OCS facilities. Although BSEE does not have regulatory authority to direct cybersecurity practices for the offshore energy industry, BSEE supports the national effort to protect critical infrastructure, and thus prevent potential harm to the safety of people and the environment on the OCS. This Strategy is a key component of that effort.

This Strategy will serve BSEE as a cornerstone for future program implementation, conservation of natural resources, and operational planning. This Strategy will also help federal and industry partners understand and participate in the Bureau's long-term planning and regulatory priorities.

This Strategy consists of four parts:

1. Potential risks, threats, and vulnerabilities to the offshore energy sector and practical mitigation measures.
2. Objectives, activities, and performance goals necessary to develop effective mitigation measures.
3. Roles, responsibilities, and coordination of various Bureau offices involved in achieving the objectives and goals.
4. Added resources and investment needed to execute the overall Strategy.

This Strategy calls for four primary objectives:

1. Build out a staff with appropriate cybersecurity expertise to help assess growing threats and vulnerabilities, and to train Bureau personnel to recognize them.
2. Be a resource for industry operators and contractors in identifying threats and vulnerabilities, so they can take appropriate action to address them.
3. Consider revising existing regulations to reframe cybersecurity as risk mitigation relative to the safety of offshore personnel and facilities.
4. Continue to participate more broadly with other federal partners to improve regulatory frameworks, where necessary, to harmonize cybersecurity practices and requirements throughout the offshore energy sector.