ARMEXA

Case Study:

Achieving Compliance with TSA Pipeline Security Directive

With the growing emphasis on securing Operational Technology (OT) systems in pipeline operations, our client sought to ensure compliance with the evolving TSA Pipeline Security Directives. Initially, the 2021 directives focused on fundamental cybersecurity practices, but the proposed 2024 TSA rules introduced stricter requirements specifically targeting OT systems. Our role was to analyze and evaluate the client's existing OT Cybersecurity Program and author new compliance documentation to meet TSA's enhanced requirements.

We performed a comprehensive and detailed gap analysis comparing their existing Program to the Directive. In the analysis, we identified areas where the existing Program was deficient, complied with, or exceeded the requirements in the TSA Directive.

Then, we ensured that the existing Program addressed any gaps and developed and documented new compliance programs, including Cybersecurity Implementation Plans (CIP) and Cybersecurity Audit Programs (CAP).

Industry:
Pipeline

Location:
United States

Current OT Enviroment:

- Operational Technology (OT)
- Regulatory Compliance

Services:

- Cybersecurity Governance
- TSA Directive Compliance

Challenge: Evolving TSA guidance required a proactive approach to develop effective CIP and CAPs

One of the key challenges faced during the engagement was the incomplete and evolving guidance from the TSA regarding the expectations for compliance documentation. This lack of clarity made it difficult to develop effective Cybersecurity Implementation Plans (CIP) and Cybersecurity Assessment Plan (CAP).

This lack of clarity made it difficult to develop effective Cybersecurity Implementation Plans (CIP) and Cybersecurity Assessment Plan (CAP) . While the TSA has since addressed these gaps, at the time, our client needed a structured and forward-thinking approach to meet regulatory expectations proactively.

Solution: Leveraging our deep OT cybersecurity expertise, knowledge of standards, and significant experience supporting pipeline operators

We assisted the client in:

- **Assessing OT Cybersecurity Readiness:** Conducted a thorough evaluation of the client's existing cybersecurity program against TSA directives, focusing on areas such as risk management, access control, and continuous monitoring
- **Developing a Comprehensive Cybersecurity Implementation Plan (CIP):** Structured a detailed plan aligning with TSA's pipeline security directives, including the 2024 proposed rules , ensuring a robust Cybersecurity Risk Management Program (CRMP) for OT systems
- **Creating a Cybersecurity Assessment Plan (CAP):** Established a framework to continuously assess compliance, incorporating best practices from industry standards like ISA/IEC 62443 and NIST 800-82
- **Enhancing Supply Chain Security:** Addressed third-party risks by recommending security measures for vendor and supply chain relationships
- **Institutionalizing Cybersecurity Best Practices:** Promoted a culture of security by embedding best practices into operational procedures and employee training programs to ensure long-term sustainability and compliance

Impact:

- The TSA recognized our client's CIP as the best submission they received—well-organized, thorough, and setting a high standard for others
- The CIP and CAP became integral to the client's OT Cybersecurity Program, enhancing resilience against evolving cyber threats
- The organization improved collaboration between OT and IT teams, ensuring continuous monitoring, incident response, and regulatory compliance.

This case study highlights the importance of proactive cybersecurity measures in the pipeline industry, especially with the heightened focus on OT security in the TSA's 2024 proposed rules. By providing clear, structured compliance documentation, we enabled our client not only to meet but exceed regulatory expectations and position them as a leader in cybersecurity preparedness.

In this instance, the client had a well-established program, but Armexa is equipped to assist organizations in meeting the Directive at any level of program maturity.

ARMEXA