TSA Security Directive Pipeline-2021-02F

EFFECTIVE MAY 3, 2025

Cancels and supersedes Security Directive Pipeline-2021-02E. Its goal is to protect the national security, economy, and public health and safety of the United States from the impact of malicious cyber intrusions affecting the nation's most critical gas and liquid pipelines.

WHO IS THIS FOR?

Owners / operators of TSA-designated critical pipeline systems or facilities notified before July 26, 2022

WHAT CAPABILITIES DO YOU NEED TO EFFECTIVELY SECURE OT ENVIRONMENTS?

- ✓ **Asset Visibility and Inventory**
- ✓ **OT Network Monitoring and Deep Packet Inspection**
- ✓ **Risk-Based Vulnerability Management**
- ✓ **Intelligence-Driven Threat Detection**
- ✓ **Investigation and Response**
- ✓ **Secure Remote Access**
- ✓ **Segmentation Policy Validation**

WHAT ARE THE REQUIREMENTS?

Create a Cybersecurity Implementation Plan that includes the following measures:

III.A Identify **Critical Cyber Systems**

III.B Implement **network segmentation** policies and controls

III.C Implement **access control** measures to secure and prevent unauthorized access

III.D Implement **continuous monitoring**, and detection policies and procedures to **prevent, detect, and respond to cybersecurity threats** and anomalies affecting Critical Cyber Systems

III.E Apply security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the owner/operator's documented **risk-based methodology**

Develop and maintain a **Cybersecurity Incident Response Plan**

Develop a **Cybersecurity Assessment Plan** for proactively assessing and auditing cybersecurity measures

DRAGOS®