USING ARMIS TO ENABLE TSA PIPELINE CYBER SECURITY ASSET GUIDELINES

PIPELINE SECURITY GUIDELINES MARCH 2018 (WITH CHANGE 1 (APRIL 2021)

SECURITY DIRECTIVE PIPELINE-2021-01

In early 2018, the TSA put forth updated guidelines to aid and assist US Pipeline operators in their efforts to address the ever-changing threat environment in both the physical and cyber security realms they are faced with. The Pipeline Security Guideline, as published in March of 2018, supersedes the 2011 version of the Pipeline Security Guidelines. These updated security measures provide new guidance for the basis of TSA's Pipeline Security Program Corporate Security Reviews and Critical Facility Security Reviews.

Further, In May of 2021, the TSA released Security Directive Pipeline-2021-01which focuses on 3 critical actions:

First, it requires TSA-specified Owner/Operators to report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Second, it requires Owner/Operators to designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise.

TSA Pipeline Security Guidelines

Table 3: Cyber Security Measures for Pipeline Cyber Assets

IDENTIFY	• Employ mechanisms to maintain accurate inventory and to detect unauthorized components • Develop a detailed inventory of every endpoint. • Review Network Connections, including remote and 3rd party connections. • Monitor remote user access to critical pipeline assets. • Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months. • Develop an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks. • Establish a process to identify and evaluate vulnerabilities and compensating security controls.

Third, it requires Owner/Operators to review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and repo1t the results to TSA and CISA.

These guidelines and directives are applicable to operational natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility operators. Securing these OT systems and components, including pipeline assets, is critical in helping organizations prevent cyber- attacks and strengthen their defenses against hackers. These guidelines protect critical infrastructure against emerging attack vectors and stiffens network security against issues like human error, natural disasters, and cyber threats.

However, the growth of the Industrial Internet of Things (IIoT) and Industry 4.0 are creating greater security threats for pipeline assets. Industrial environments face the greater risk of increasingly sophisticated cyber-attacks that could damage their equipment, cause downtime, and result in data leaks.

All-encompassing TSA Guideline capabilities

Armis is an agentless and passive solution that is perfectly positioned to help pipeline operators implement and abide by the TSA Guidelines and Directives as published. Armis covers more TSA requirements and subsequent directives across more components and systems than any other OT Security vendor.

Armis takes into consideration all enterprise assets, including Building Management System, Building Automation Systems, Internet Technology (IT), IoT devices, in addition to OT pipeline requirements. Whereas niche point solutions only cover OT devices, which is only a portion of the entirety of the scope of TSA Guidelines and Directives.

PROTECT

- Ensure that user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company.
- Segregate and protect the pipeline cyber assets from enterprise networks and the internet using physical separation, firewalls, and other protections.
- Regularly validate those technical controls comply with the organization's cybersecurity policies, plans and procedures, and report results to senior management.
- Implement technical or procedural controls to restrict the use of pipeline cyber assets for only approved activities.

DETECT

- Implement processes to generate alerts and log cybersecurity events in response to anomalous activity.
- Monitor for the introduction of malicious code and activities.
- Perform regular testing of intrusion and malware detection processes and procedures.
- Utilize independent assessors to conduct pipeline cyber security assessments.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com
1.888.452.4011

20211018-1