FORTRA™

GUIDE (TRIPWIRE)

Staying Current With the TSA's Oil and Gas Security Directives

Pipeline Compliance Flows Smoothly With Tripwire

Escalating cyberthreats in the oil and gas industry underscore the need for collaboration between public and private sectors to mitigate this national security risk, and much of this responsibility falls on individual pipeline operators who need to comply with the Transportation Security Administration (TSA) Security Directive.

Despite being best known for its role in air travel security, the TSA also oversees safety standards for pipelines transporting natural gas, oil, and other hazardous liquids. This poses unique difficulties for operators, who need to stay informed of dynamic security threats while managing their pipeline networks and adapting to evolving regulatory demands.

About the Transportation Security Administration

Founded in 2001, the TSA is a U.S. government agency responsible for ensuring the security of transportation systems. The TSA was created with the Aviation and Transportation Security Act and is part of the larger Department of Homeland Security (DHS). Its overarching mission is to safeguard the nation's transportation systems and ensure the safety of travelers across all modes of transportation.

What Are TSA Security Directives?

Each July, the TSA releases an updated Security Directive for oil and natural gas pipeline operators. Its federal partners like the Department's Cybersecurity and Infrastructure Security Agency (CISA) and major stakeholders from the oil and gas industry work together to keep the nation's pipelines safe and resilient against cyberattacks with these frequent updates.

> *"The directive establishes a new model that accommodates variance in systems and operations to meet our security requirements. We recognize that every company is different, and we have developed an approach that accommodates that fact, supported by continuous monitoring and auditing to assess achievement of the needed cybersecurity outcomes."*
>
> **– TSA Administrator David Pekoske**[1]

The TSA can request the following documentation and inspect it to determine your organization's compliance alignment[2]:

- Hardware and software asset inventory, including supervisory control and data acquisition systems
- Firewall rules
- Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and virtual local area networks
- Policy, procedural, and other documents
- Data providing a "snapshot" of activity in and between informational and operational technology systems, such as log files

Pipeline owners are required to submit an updated cybersecurity assessment plan for review and approval each year. This plan must include the outcomes of previous year's assessments and outline a schedule for evaluating and auditing specific cybersecurity measures to verify their effectiveness.

Consequences of Non-Compliance

The biggest consequence of non-compliance is falling prey to a cyberattack. For example, the Colonial Pipeline Company had to completely halt operations in 2021, due to a ransomware attack. This incident caused a temporary disruption in the supply of gasoline across the East Coast.

Compliance mandates like the TSA's provide detailed instructions for cybersecurity measures like network segmentation, access control, and multi-factor authentication. There are other consequences in addition to cyberattacks; pipeline operators can be fined and penalized by the TSA and can even lose their business licenses. Penalties for non-compliance begin at $7,000 per day[3].

How Tripwire Helps With TSA Compliance

Fortra's Tripwire empowers pipeline operators to automate security control enforcement and change monitoring backed by audit-ready reporting. This mapping demonstrates Tripwire's coverage for each of the measures contained in the TSA Security Directive for pipeline owners/operators.

Security Directive Measure	Tripwire Coverage
Identify critical cyber systems	Tripwire IP360 discovers all critical cyber systems by their IP addresses and seamlessly integrates with other solutions that identify cyber asset systems in operational technology (OT) environments.
Network segmentation and controls	Tripwire Enterprise continuously monitors the configuration settings of network devices to ensure the integrity of your network segmentation.
Access control measures	Tripwire Enterprise tracks changes to Active Directory and group policy object (GPO) changes.
Continuous monitoring and detection	Tripwire Enterprise is the leader in continuous monitoring and detection, combining file integrity monitoring (FIM) and security configuration management (SCM) to detect suspicious changes and enforce cybersecurity policies like the TSA's.
Security patches and updates	Tripwire IP360 detects vulnerabilities and identifies where patches are needed, while Tripwire Enterprise Dynamic Software Reconciliation verifies the integrity of patches, ensuring that only authorized changes occur.
Cybersecurity incident response plan	As part of your incident response plan, Tripwire can compare drift in systems to see where malware may be installed and to ensure system integrity is maintained.
Cybersecurity assessment plan	Tripwire conducts industrial cybersecurity assessments and can evaluate your security posture by monitoring configuration states and identifying vulnerabilities, scoring them based on severity.

Tripwire® Enterprise: Tripwire Enterprise is the leading compliance monitoring solution, using file integrity monitoring (FIM) and security configuration management (SCM). Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions.

- Real-time change detection
- Automated compliance
- Extensive integrations

Tripwire IP360™: Tripwire IP360 proactively discovers, profiles, and assesses the vulnerability risk of your assets and can stand as the fundamental solution of your vulnerability management (VM) program. It enables fast detection of vulnerabilities, granular prioritization of risk, and remediation management.

- Prioritized risk scoring
- Discovers all network assets
- Continuous updates by Tripwire's vulnerability research team

Tripwire LogCenter®: Tripwire LogCenter provides secure and reliable log collection to add real-time intelligence to machine data, with security analytics and forensics for rapid incident detection and response. It readily integrates with your existing infrastructure and includes a growing library of available correlation rules.

- Automated compliance evidence
- Highlighted events of interest
- Reliable log data capture and reporting

Tripwire State Analyzer: Tripwire State Analyzer works in tandem with Tripwire Enterprise and Tripwire IP360 to offer an automated, flexible solution to this security challenge.

- Automate the validation of detected system configurations
- Generate detailed system configuration reports
- Improve the process of validating software and patches

Tripwire ExpertOps℠: Tripwire ExpertOps delivers a cloud-based managed services model of the industry's best security configuration and vulnerability management. A single subscription includes personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security.

- Cybersecurity and compliance as a managed service
- Customized service plan and progress reports
- Supplements your team with a dedicated expert

Ensure TSA compliance and audits are streamlined and efficient with Tripwire as your integrity management ally. Let us take you through a demo of Tripwire's security and vulnerability management products and services customized to your specific IT security and compliance needs. Visit www.tripwire.com/demo.

Sources:

1. https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners
2. https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf
3. https://www.csoonline.com/article/570803/tsa-s-pipeline-cybersecurity-directive-is-just-a-first-step-experts-say.html

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

