

# The Updated TSA Pipeline Security Directive: Overview and How to Comply

## Pipeline Security Background

Pipeline security and regulations have been assigned to the **Transportation Security Administration (TSA)** by Congress in 2001 through the Aviation and Transportation Security Act. For two decades, TSA advocated for [voluntary pipeline cybersecurity standards](#) under the rationale that it enabled greater flexibility to protect against rapidly evolving cyber threats.

In light of the [May 7, 2021 Colonial Pipeline incident](#), TSA administrators changed course by issuing Security Directive Pipeline-2021-01 on May 28, 2021, quickly followed by [Security Directive Pipeline-2021-02](#) on July 26, 2021. The first directive placed three **mandatory requirements on pipeline owners and operators**:

1. Report all cybersecurity incidents to CISA within 12 hours,
2. Designate a primary and alternative Cybersecurity Coordinator, at the corporate level, who is accessible 24/7 to TSA and CISA, and
3. Conduct a cybersecurity vulnerability assessment and provide a report of this assessment to TSA and CISA within 30 days.

The second directive added three mandatory requirements:

1. Implement immediate mitigation measures to protect against cyberattacks
2. Develop a cybersecurity contingency and recovery plan, and
3. Conduct a cybersecurity architecture design review.

Failure to comply can lead up to fines as high as **\$11,904 per day, per violation**, which is the maximum civil penalty for pipelines under the latest [TSA guidance](#).

The eminent nature of the threat led TSA to issue these security directives without going through a rulemaking or stakeholder feedback process. The industry reacted with concerns and perceived the requirements to be overly burdensome and not readily attainable for most pipeline owners and operators. In response, TSA engaged with cybersecurity experts and industry stakeholders over the past 12 months and decided to offer more flexibility to meet the intended security outcomes by **transitioning to a performance-based approach**. The new requirements have been issued through [Security Directive Pipeline-2021-02C](#) on July 27, 2022. The new approach supersedes previous directives and is presented below.

## TSA Security Directive Overview

The latest security directive includes the following three requirements:

1. Establish and implement a TSA-approved **Cybersecurity Implementation Plan** that describes the specific cybersecurity measures employed and the schedule for achieving the outcomes described in Section III.A. through III.E of the directive.
2. Develop and maintain an up-to-date **Cybersecurity Incident Response Plan** to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in the directive, should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident (Section III.F. of the directive).
3. Establish a **Cybersecurity Assessment Program** and submit an annual plan that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities (Section III.G. of the directive).

The following diagram provides a breakdown overview of the requirements and related cybersecurity objectives.

One important aspect of the revised Security Directive allows owners and operators to map their Cybersecurity Implementation Plan on a performance-based schedule. The directive also includes the following list of **documentation to establish compliance**:

- Hardware/software asset inventory that includes the SCADA environment
- Firewall rulesets and filtering policies
- Network diagram including switch and router configurations
- Documents that informed the development and implementation of the Cybersecurity Implementation Plan, the Cybersecurity Incident Response Plan, and the Cybersecurity Assessment Program
- Snapshot activity data including log files and up to 24 hours of network traffic capture

The next section describes how to best prepare for a TSA audit by leveraging a network modeling and verification solution such as NP-View.

## Preparing for a TSA Audit with NP-View

TSA relies upon existing [investigative and enforcement procedures](#) to ensure compliance with the security directive requirements. **The pipeline owners and operators must make records necessary to establish compliance with the requirements available to TSA upon request for inspection.** TSA already went through an information collection process in 2021 by visiting critical pipeline facilities and sending Critical Facility Security Review (CFSR) form to the [top 100 most critical pipelines](#).

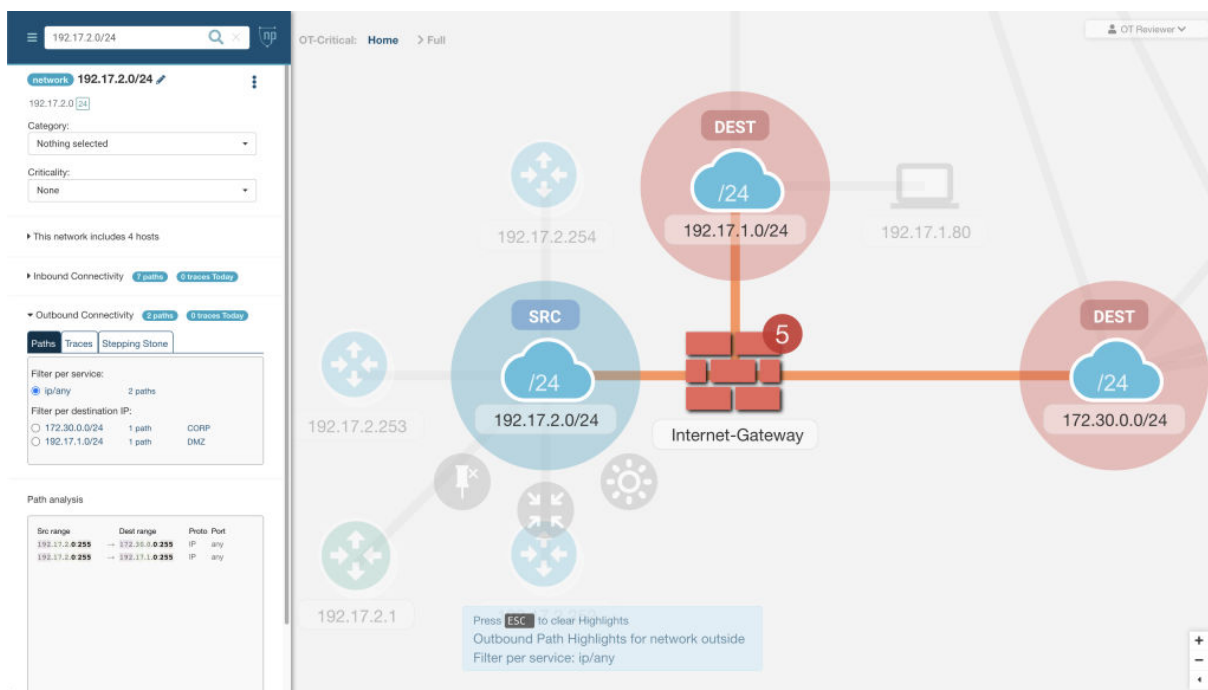
During critical facility visits, TSA documents and provides recommendations to pipeline operators to improve the security posture of the reviewed facility. TSA then follows up with pipeline operators via email on the status toward implementation of the recommendations made during the critical facility visits. The follow up is conducted at intervals of 6, 12 and 18 months after the facility visit.

To understand how an audit works, one should look at how the Federal Energy Regulatory Commission (FERC) has long required electric power systems to comply with mandatory [NERC CIP](#) cybersecurity regulations. [It is recommended](#) for pipeline owners and operators to make their **TSA policies and procedures consistent with NERC CIP cybersecurity standards** across their telecommunication infrastructure.

Network Perception knows the NERC CIP framework well. We developed our [NP-View software](#) specifically to support the network diagramming and firewall rule verification needs of both the NERC auditors and the compliance teams at electric utilities. NP-View works by ingesting firewall, router, and switch configuration files offline to automatically produce evidence to demonstrate compliance. The network modeling capabilities enables users to:

- **Verify the correct implementation of network segmentation (III.B)** and access control measures (III.C), including all external connections to the OT system.
- **Ensure clear understanding of communication paths between IT and OT (III.F.1.b and III.F.1.d).**
- **Generate automatically network architecture diagram (III.G.2.b)** with a representation of logical zone boundaries and their criticality.

NP-View runs on premise as a lightweight desktop application designed to save up to 80% of the time required to audit complex firewalls. Contact us to learn more and strengthen your TSA Cybersecurity Implementation Plan.



*Screenshot of NP-View representing a layer-3 network diagram with connectivity path analysis. Visit the [Knowledge Base](#) to learn more.*

Want to learn more?

Read the latest [article](#) written by Network Perception's CEO & Co-Founder, Robin Berthier, on how to prepare for a TSA Audit using NP-View.

or

**Talk to an OT/ICS Specialist TODAY**