SHIFT5 WHITEPAPER

TSA ENHANCED RAIL CYBERSECURITY DIRECTIVES

The TSA's Security Directive strengthens initial requirements and mandates that owners/operators of passenger and freight rail systems implement performance-based measures to "achieve critical cybersecurity outcomes," including onboard operational technology (OT) systems and components. This white paper describes these outcomes and Shift5's recommendations.

SHIFT5

1100 Wilson Blvd, Ste 2100 - Rosslyn, VA 22209 // shift5.io // 703-810-3320 //

Introduction

Ten months after releasing its initial requirements and a month after the White House held closed-door briefings for owners/operators on rail cybersecurity threats, the U.S. Transportation Security Administration (TSA) released an in-depth update to its Security Directives for freight and passenger railroad carriers in October 2022. The latest directive strengthens the initial requirements and mandates that owners/operators of passenger and freight rail systems implement performance-based measures to "achieve critical cybersecurity outcomes," including onboard operational technology (OT) systems and components.

These TSA directives come in the wake of focused attention by the U.S. government on our nation's critical infrastructure sectors following the cyberattack on Colonial Pipeline in 2021. Beginning with directives aimed at pipeline operators, the TSA then extended its scope to include rail owners/operators, helping to ensure the safety and security of our nation's rail infrastructure.

The rail cybersecurity directives followed high-profile attacks in 2021, including

» An attack on the New York Metropolitan Transit Authority's computer systems by hackers with suspected ties to China.

» A ransomware attack on the Santa Clara Valley Transportation Authority's computer systems, leaving them inoperable for several days.

» U.S. rail operator CSX suffered a data security incident where a ransomware gang posted internal company files to a leak site.

The growing frequency and severity of attacks on rail systems is a unique national security concern, as rail is a critical enabler for our nation's economy. It is the transportation backbone for the distribution of goods throughout North America, responsible for supporting billions of dollars in trade. Rail also supports our national defense through the Federal Railroad Administration's Strategic Rail Corridor Network (STRACNET), with 38,800 miles of rail lines that provide service to 193 defense installations.

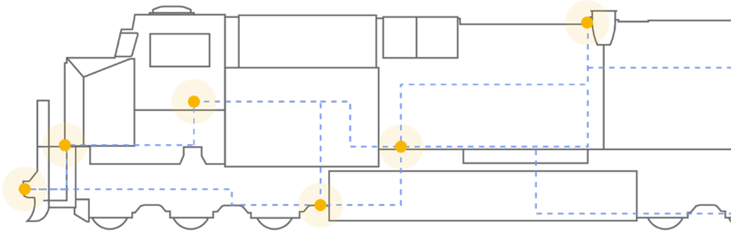
Read on for our recommendations to rail owners and operators navigating the requirements of these updated directives.

October 2022 Rail Cybersecurity Directive Requirements

According to the TSA, Security Directive 1580/82-2022-01 requires "TSA-specified passenger and freight railroad carriers take action to prevent disruption and degradation to their infrastructure to achieve the following critical security outcomes."

Network Segmentation

Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology (OT) system if the Information Technology (IT) system is compromised or vice-versa.



Our recommendation:

The directive released today requires implementing policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes. But while network segmentation is a foundational cybersecurity strategy, air gapping, segmenting, and firewalling critical networks as a silver bullet are myths in the converged IT/OT era.

As a result of locomotive modernization, IT and OT are interconnected — there is no air gap. The National Security Telecommunications Advisory Committee (NSTAC) recently acknowledged this, saying, "[OT] asset owners/operators should recognize that in most environments, the air gap is a myth. In fact, many members of the President's National Security Telecommunications Advisory Committee have 25 years-plus experience and have never seen a true air-gapped OT system."

Once discrete, today's operationally-critical onboard locomotive components– such as braking controls – now interface with IT, creating an extended attack surface for owners/operators to monitor and manage. With such interconnectivity, network segmentation policies, although foundational for IT, are insufficient for OT. We recommend rail owners/operators implement network segmentation policies and controls but that they also bolster them with additional tactics to safeguard their assets.

> "[OT] asset owners/operators should recognize that in most environments, the air gap is a myth. In fact, many members of the President's National Security Telecommunications Advisory Committee have 25 years-plus experience and have never seen a true air-gapped OT system."
>
> National Security Telecommunications Advisory Committee (NSTAC)

Access Control

Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.

Our recommendation:

The directive mandates that if an owner/operator does not apply multi-factor authentication for access to Operational Technology components or assets, the owner/operator must specify what compensating controls are used to manage access. Developing access control measures is a simple IT-oriented tactic to prevent malicious attackers from taking the easy route of gaining access to your locomotive or rail network. While applying multi-factor authentication (MFA) into IT systems is common today, owners/operators cannot apply MFA to OT systems with the same ease, given the realities of operations in the rail ecosystem.

We recommend that rail operators reexamine their access control measures to OT systems, particularly to keep bad actors out of critical operational technology. Owners/operators should invest efforts in applying the NIST Risk Management Framework principles when assessing segmentation and access controls. Shift5 also offers a Cyber Survivability Risk Assessment — an in-depth penetration test that helps companies and government agencies assess risk to their OT systems, identify the best risk mitigations, and prevent future malicious cyber activity.

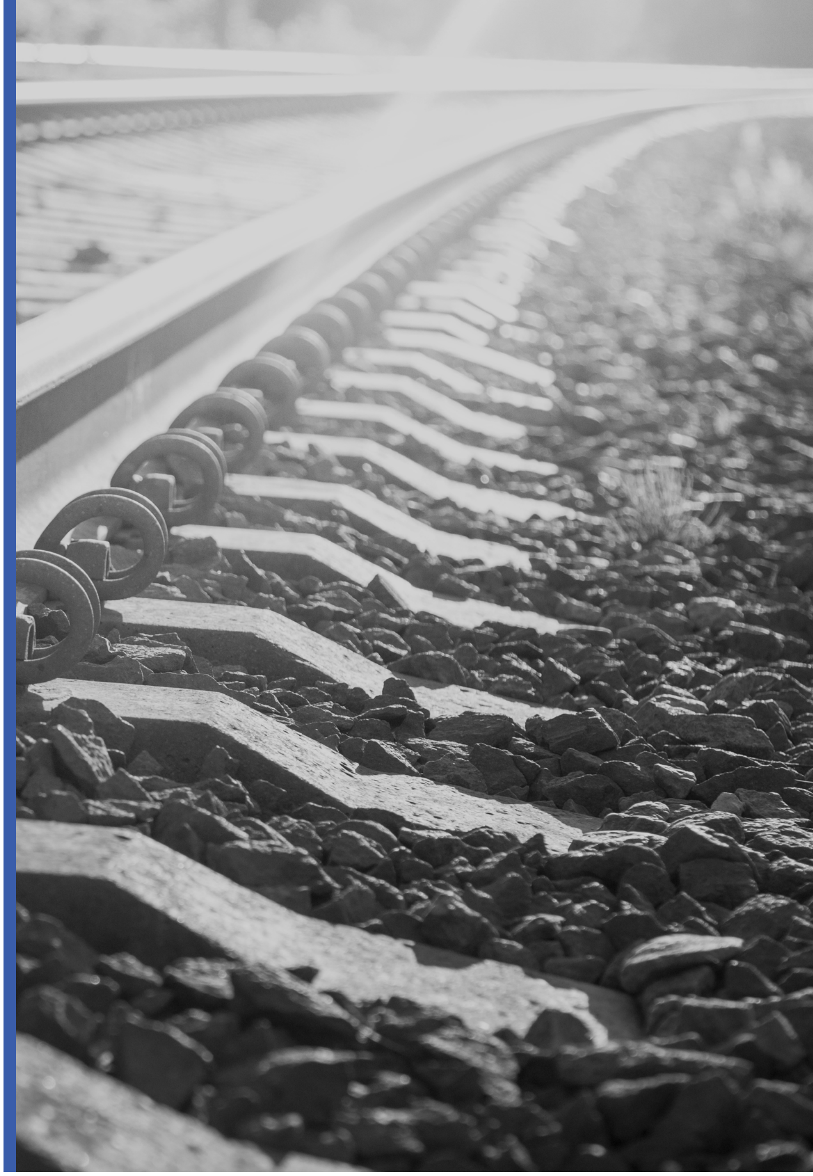
Continuous Monitoring

Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems.

Our recommendation:

An important clarification to this requirement is for owners/operators to continuously collect and analyze data for potential intrusions and anomalous behavior on critical cyber systems and other IT and OT systems that directly connect with them. Critical cyber systems include those responsible for safe, reliable operations, such as digitally-controlled braking and throttling systems. This data must also be maintained for sufficient periods to enable cybersecurity incident investigation. Data collected from onboard OT systems can also provide invaluable information about operational conditions that could affect the availability and safety of an operator's assets.

However, traditional, trusted IT security solutions cannot monitor traffic coming from onboard OT components. That means rail owners/operators face a blind spot in monitoring and detecting OT-level traffic to determine the resilience of their onboard systems. Detection and monitoring are cornerstones of a modern cybersecurity strategy. As such, we recommend owners/operators ensure they have visibility into all parts of their locomotives and rail networks and actively monitor and log activity for real-time alerting and future threat response and investigation.



Risk Reduction

Reduce the risk of exploitation of unpatched systems by applying security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology.

Our recommendation:

The TSA's directive says the strategy for patches must include:

- A risk methodology for categorizing and determining the criticality of patches and updates
- An implementation timeline based on categorization and criticality
- Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog

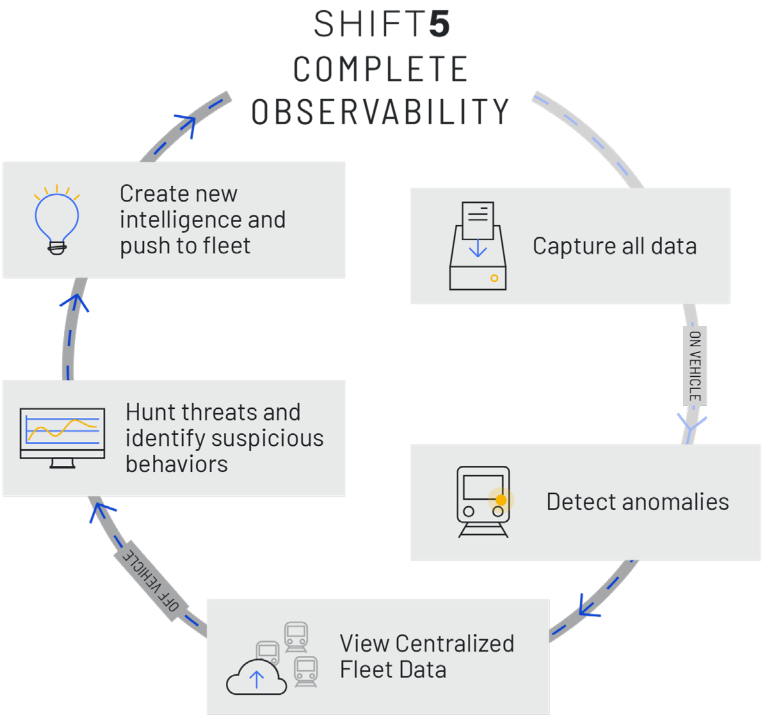
Patching software is critical in keeping all rail systems resilient against malicious actors. But while most IT system defenders have the IT patching process down to a science, **patching OT systems is a more complex challenge for rail owners/operators, given the potential impacts on rail operations uptime.**

In addition, the rail cybersecurity directive mandates that if the owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.

We recommend, at a minimum, that rail owners/operators develop a strategy and implement solutions that can safeguard onboard systems while keeping operations running safely and smoothly. They should also implement solutions that can mitigate risks effectively, whether or not software patches can or will ever get deployed on affected OT systems. And continuously educating staff responsible for securing critical systems and developing a culture of cybersecurity beyond IT to include OT can add tremendous value to an owner/operator's security strategies.

The Shift5 Platform

Trains are composed of thousands of digital components, each emitting valuable data that can be collected and transformed into useful intelligence. Shift5 provides modern observability into these assets so organizations can improve cybersecurity and increase operational efficiency.


SHIFT5
COMPLETE
OBSERVABILITY
Capture all data
ON VEHICLE
Detect anomalies
View Centralized Fleet Data
OFF VEHICLE
Hunt threats and identify suspicious behaviors
Create new intelligence and push to fleet

Capture all data

Onboard data traverses serial bus networks that often rely on embedded protocols. Shift5 captures all data crossing onboard serial bus networks and detects anomalies in real-time, directly on the vehicle.

Detect anomalies

Shift5 layers rules-based detection for known attacks with advanced machine learning and analytics-based methods to find anomalies that do not contain a specific fingerprint. This means the Shift5 technology can detect attacks that have never been seen before. Shift5 further increases detection rates by continually writing signatures and rules for observed attacks. The more data Shift5 collects, the better it defends operational technology platforms.

Centralize data

Data collected from vehicles across the fleet is centralized in a public, private, or government cloud for analysis. This analysis can support threat hunting, operational efficiency, or incident response use cases and provides crew and maintenance with essential situational awareness.

Hunt threats and identify suspicious behavior

Armed with large amounts of onboard network data collected over time, threat researchers can model, test, and proactively hunt for new threats before they do damage. Create new intelligence: Intelligence created through analysis of the aggregated fleet data is fed back to the vehicles so anomaly detection is continuously improved.

Next Steps

Gaining observability into the onboard OT networks that power your most important assets is a journey. To learn more about the possibilities, go to **shift5.io** to schedule a briefing. Classified briefings are available to organizations with the proper security clearance.

SHIFT**5**

Shift5 is the onboard OT data and cybersecurity company for planes, trains, and tanks. Created by founding members of the U.S. Army Cyber Command who pioneered modern weapons system cyber assessments, Shift5 defends military platforms and commercial transportation systems against malicious actors and operational failures. Customers rely on Shift5 to detect threats and maintain the readiness and availability of today's planes, trains, tanks, and weapons systems and tomorrow's next-generation vehicles.

shift5.io *"Shift5 TSA Rail Directives Whitepaper" Version 2.0 // Dec 2022*