

Security Plan

Security Plan Overview

The security plan must be based on and supported by the railroad carrier's vulnerability assessment. The security plan ensures that security processes and procedures are in place to effectively prevent and respond to threat incidents and terrorist attacks.

Freight Rail Security Plan Structure

The Plan should address the following elements, as applicable:

- Rail Carrier's Statement of Security Plan Objectives (what the plan sets out to do).
- Designation of "Rail Security Coordinator(s)"—Team responsible for developing, managing, and ensuring the security countermeasures are implemented during raised alert levels or response to a security threat/incident.
- Roles and Responsibilities of those designated with security responsibilities
- Procedures in place to communicate, disseminate, and respond to threat information.
- Procedures for updating information and ensuring security countermeasures are being implemented during raised alert levels (Process needs to be set up to get the latest information internally and to be able to externally communicate the status of their security response related to a terrorist attack or security incident).
- Security countermeasures to be implemented by your railroad in response to a terrorist attack or threat incident at each alert level (blue to red).
- Procedures in place for periodic audits, exercises and drills for security plans, and for its amendment in response to experience.
- Measures to prevent unauthorized access to designated or restricted areas.
- Measures to prevent the introduction of dangerous substances and devices to designated restricted areas and/or railroad property.
- Procedures and expected timeframes for responding to security threats or breaches of security, including provisions for maintaining security of infrastructure and operations on railroad property.
- Identifications of security processes to work with State and local law enforcement agencies, emergency responders, and Federal officials in response to a terrorist attack.
- Procedures for evacuating railroad facilities or conveyances in case of reliable security threats or breaches of security.
- Procedures in place for protection of railroad carrier designated critical infrastructures.

- Procedures for employee identification and background checks for employees and contractors.
- Identification of, and methods to communicate with railroad, system and facility security officers, company security officers, field operating and security officers and management personnel, public safety officers and emergency response personnel, crisis management organizational representatives in local areas, including 24 hour contact details.
- Security measures designed to ensure security of local communities, critical infrastructure, special events, railroad facilities, railroad conveyances/equipment, passengers and passenger trains operating on railroad tracks owned or operated by your railroad, cargo and cargo handling equipment owned by you or your customer and other railroad interdependencies covered by contractual agreements.
- Procedures to address secure handling and storage of toxic inhalation hazardous materials when threat conditions warrant.
- Plans to minimize the occasions when loaded tank cars carrying TIH materials are unattended in High Threat Urban Area (HTUA's).
- Plan for employee security awareness training to include timeline for conducting employee training
- Plans for a positive and secure handoff of SSM rail cars at points of interchange with shippers, receivers and other carriers.
- Plans and procedures to provide redundant and backup systems required to ensure continued railroad operations.
- Procedures to respond to and facilitate the recovery of the railroad operations after a transportation security incident.
- Procedures for cyber security.
- Appendix containing risk mitigation strategies for addressing vulnerabilities identified in the vulnerability assessment but not sufficiently addressed by the security plan. This should include:
 - o Outstanding vulnerabilities
 - o Mitigation options and associated costs of alternatives
 - o Preferred mitigation strategy
 - o Comprehensive funding plan and schedule for risk remediation