# Rail Carrier Security Criteria

Rail carriers must conduct a comprehensive assessment of their security practices based upon the following C-TPAT minimum-security criteria. Recognizing that rail carriers do not control their shippers and have a common carrier obligation to transport goods tendered to them, rail carriers shall work with their shippers on their security practices as set forth in these criteria.

These minimum security criteria are fundamentally designed to be the building blocks for rail carriers to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.

Rail carriers should periodically assess their degree of vulnerability to risk and should prescribe security measures to strengthen or adjust their security posture to prevent security breaches and internal conspiracies. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Security measures, as listed throughout this document, must be implemented and maintained as appropriate to the carrier's business model and risk understanding.

**Business Partner Requirements**
Rail carriers must have written and verifiable processes for the screening of new business partners, including carrier's agents, sub-contracted rail carriers, and service providers, as well as screening procedures for new customers, beyond financial soundness issues to include security indicators. These processes apply to business partners and service providers not eligible for C-TPAT membership.

***Security Procedures*[1]**

- Written procedures must exist to address specific factors or practices, the presence of which would trigger additional scrutiny by the rail carrier. U.S. Customs and Border Protection (CBP) will work in partnership with the rail carriers to identify specific information regarding what factors, practices or risks are relevant.
- For those business partners eligible for C-TPAT certification (importers, ports, terminals, brokers, consolidators, etc.) the Rail carrier must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified. Non-C-TPAT business partners may be subject to additional scrutiny by the Rail carrier. Rail carriers should institute appropriate security procedures for their contract service providers.

- Rail carriers have a common carrier responsibility for all cargo loaded aboard their rail cars, they must communicate the importance of security to their employees as a fundamental aspect of their security policies.
- Rail carriers should strongly encourage that contract service providers and shippers commit to C-TPAT security recommendations.

*Rolling Stock Security*
Rail carriers shall have procedures to protect against the introduction of unauthorized personnel and material.[2]

- It is recognized that even though a carrier may not "exercise control" over the loading of rail cars and the contents of the cargo, rail carriers must be vigilant to guard against stowaways, and the smuggling of implements of terrorism and contraband. The rail carrier shall have procedures in place to guard against the loading of contraband while trains are in transit to the border, even in regards to unforeseen train stops.
- Rail carriers must have procedures in place for reporting unauthorized entry into rail cars, and locomotives.
- Rail carriers must maintain inventory information and movement records on each rail car and use the physical rail car tracking technology that is inherent to the North American rail network system.

*Inspection Procedures*

- Rail personnel should be trained to inspect their rail cars and locomotives, for anomalies. Training in conveyance searches should be adopted as part of the company's on-the-job training program. Training that is held should be recorded or documented in a personnel file of the employee that attended the training.
- A systematic inspection must be made prior to reaching the U.S. border.
- During required on-ground safety inspections of rolling stock entering the U.S., conduct security inspections for any apparent signs of tampering, sabotage, attached explosives, contraband, stowaways, and other unusual or prohibited items. It is understood that railroads must comply with the Federal Railroad Safety Act and the Hazardous Materials Transportation Act.
- CBP will work in partnership with the rail carriers to identify specific information regarding what factors, practices or risks are relevant including the use of non-intrusive gamma ray technology or other inspections.

**Conveyance Tracking and Monitoring Procedures**

- Rail carriers must maintain, to the extent feasible and practicable, locomotive and rail car integrity while the train is en route to the U.S. border by maintaining inventory information and movement records for each rail car. Rail carriers must record unannounced or unforeseen train stops.
- Rail carriers must utilize existing tracking and monitoring processes to track conveyances while they are en route to the U.S. border. Unannounced or unforeseen train stops shall be documented.

- Railroad supervision must ensure that tracking and monitoring processes are being adhered to.

*Seals*

The sealing of rail cars, and intermodal maritime containers, along with continuous seal integrity are crucial elements of a secure supply chain, and remains a critical aspect of a rail carrier's commitment to C-TPAT. To the extent practical, a high security seal should be affixed to all loaded rail cars bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals. Rail carriers crossing the U.S. border must also fully comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

- Clearly defined written procedures must stipulate how seals in the rail carrier's possession are to be controlled during transit. These written procedures should be briefed to all rail crewmembers and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must include:
    - Verifying that the seal is intact, and if it exhibits evidence of tampering along the route.
    - Properly documenting the original and second seal numbers.
    - Verify that the seal number and location of the seal is the same as stated by the shipper on the shipping documents.
    - If the seal is removed in-transit to the border, even by government officials, a second seal must be placed on the trailer, and the seal change must be documented.
    - Rail crewmembers must immediately notify the dispatcher that a seal was broken; by whom, and the second seal number, which was placed on the rail car.
    - The rail carrier must make immediate notification to the shipper, the customs broker and the importer of the placement of the second seal.
- Written procedures must stipulate how unapplied seals in the rail carrier's possession are controlled. Rail carriers crossing the U.S. border must also fully comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

**Physical Access Controls**

To the extent practical, rail carriers should institute access controls to prevent unauthorized entry to rail property and rail cars and should maintain control of employees and visitors. Access controls should include the positive identification of employees, visitors, service providers, and vendors. Rail companies should also conduct spot inspections of motor vehicles on railroad property where international shipments are handled.

*Employees*

An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to high security areas such as dispatch centers if necessary for the performance of their duties. Railroad supervision or railroad police must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key

cards, etc.) must be documented. Establish employee identification measures for all employees. Conduct spot checks of identification as threat conditions warrant.

*Visitors, Vendors and Service Providers*
To the extent feasible and practicable, and as threat conditions warrant, restrict the access of contractors and visitors to non-public areas of company-designated critical infrastructure and monitor the activities of visitors in or around such infrastructure.

*Challenging and Removing Unauthorized Persons*
Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

*Unauthorized Persons*

- Implement measures to deter unauthorized entry and increase the probability of detection at company-designated critical infrastructure. Provide safety and security training for employees at facilities where international shipments are handled.
- Establish procedures to detect or deter unmanifested material and unauthorized personnel from gaining access to trains crossing into the United States.
- Reinforce the need for employees to immediately report to the proper authorities all suspicious persons, activities, or objects encountered.
- Focus proactive community safety and security outreach and trespasser abatement programs in areas adjacent to company-designated critical infrastructure to reduce the likelihood of unauthorized individuals on company property and to enhance public awareness of the importance for reporting suspicious activity.

**Personnel Security**
Written and verifiable processes must be in place to screen prospective rail employees and to periodically check current employees.

*Pre-Employment Verification / Background Checks / Investigations*
Application information, such as employment history and references must be verified prior to employment.

*Background checks / investigations*
Depending on the sensitivity of the position, background checks and investigations shall be conducted for current and prospective employees as appropriate and as required by foreign, federal, state and local regulations. Conduct background checks on all new railroad employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee’s position.

*Personnel Termination Procedures*
Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

**Procedural Security**
Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to rail cars and locomotives.

Security procedures should be implemented that restricts access to the rail car and locomotive and prevents the lading of contraband while en-route from facilities in international locations to the United States.

Procedures must be in place to record and immediately report all anomalies regarding train crew personnel to U.S. Customs and Border Protection. Likewise, rail companies should investigate all suspicious activity and report it to the proper authority.

*Bill of Lading/Manifesting Procedures*
Procedures must be in place to ensure that the information in the carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent, and is filed with CBP in a timely manner. Documentation control must include safeguarding computer access and information.

*Reporting Train Crew Personnel*
Identify all personnel on the train as required by CBP.

*Reporting Suspicious Cargo*
All instances of suspicious cargo shipments should be reported immediately to the nearest CBP port-of-entry or other nearest appropriate authority.

**Physical Security**
Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to conveyance, including concealment in rail cars. Rail carriers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

*Fencing*
Perimeter fencing should enclose areas deemed by the rail carrier to be a critical infrastructure.

*Parking*
Privately owned vehicles should be monitored when parked in close proximity to rolling stock that crosses the international border.

*Building Structure*
Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

*Lighting*
Adequate lighting must be provided where appropriate, for entrances and exits.

*Alarms Systems & Video Surveillance Cameras*
Where appropriate, alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to rail property

**Security Training and Threat Awareness**
A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists. Employees must be made aware of the procedures the rail carrier has in place to address a situation and how to report it.

Additionally, specific training should be offered to assist employees in maintaining rolling stock integrity, recognizing internal conspiracies, and protecting access controls.

Establish an employee security awareness-training program to include procedures to recognize suspicious activity and report security concerns.

During required on-ground safety inspections of international shipments inspect for any apparent signs of tampering, sabotage, attached explosives, and other suspicious items. Train employees to recognize suspicious activity and report security concerns found during inspections and in transit.

Implement a policy to preclude unnecessary disclosure of sensitive information.

**Information & Technology Security**

*Password Protection*
Measures should be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access. Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place.

*Accountability*
IT security policies, procedures, and standards must be in place to address the abuse of IT including improper access, sharing, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

[1]*C-TPAT recognizes that rail carriers are common carriers and are already subject to defined security mandates created under the Department of Transportation, such as the Federal Railroad Safety Act and the Hazardous Materials Transportation Act, as well as the Customs and Border Patrol (CBP) Trade Act of 2002, Maritime Transportation Security Act, FDA 2002 Bio-Terrorism Act, and other applicable federal requirements of the TSA. It is not the intention of C-TPAT to duplicate these security requirements rather C-TPAT seeks to build upon the government security measures and industry practices already in place.*

[2]*For purposes of this document, the term rolling stock is used to denote locomotives and rail-cars.*