



RECOMMENDED SECURITY ACTION ITEMS FOR THE RAIL TRANSPORTATION OF TOXIC INHALATION HAZARD MATERIALS

This document contains recommended security action items for the rail transportation of materials poisonous by inhalation, commonly referred to as Toxic Inhalation Hazard (TIH)¹ materials. Adoption of these measures is voluntary. Movement of large quantities of TIH materials by rail in proximity to population centers warrants special consideration and attention. These materials have the potential of causing significant numbers of fatalities and injuries if intentionally released in an urban environment.

The efficient operation of our critical interstate rail system requires a uniform nationwide approach to railroad security. The security action items listed in this document have been identified by the Department of Homeland Security (DHS) and the Department of Transportation (DOT) during risk assessments and security reviews and build upon existing DOT hazardous materials regulations. In particular the DOT regulations at 49 CFR Sections 172.704 and 172.800-804 require each transporter of hazardous materials, including TIH materials, to develop and implement security plans and to train appropriate employees in security measures. DHS and DOT are issuing these voluntary action items as measures that should be considered when security plans are developed, implemented, and revised. The action items are voluntary to allow the railroad carriers to adopt measures best suited to their particular circumstances, provided the measures are consistent with existing regulations. It is not our intent that these security action items be enacted into law by state and local governments. Existing federal regulations likely would preempt any such law.

The security action items have been divided into three categories 1) system security; 2) access control; and 3) en-route security. System security and access control refer to practices affecting the security of the railroad and its property. En-route security refers to the actual movement and handling of railcars containing TIH materials.

DHS and DOT recognize that no one solution fits all locations and circumstances. These security action items allow for flexibility in implementation based upon the assessed vulnerability of a particular process or operation. Where applicable, implementation of these action items to their fullest extent practicable should be the goal of the affected property owner and operator.

DHS and DOT reserve the right to update or modify these security action items as circumstances warrant.

¹ Under the Hazardous Materials Regulations (49 CFR 171-180), TIH materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans as to pose a hazard to health in the event of a release during transportation. See 49 CFR 171.8, 173.115, and 173.132.

**DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF TRANSPORTATION**

SYSTEM SECURITY PRACTICES AFFECTING THE TRANSPORTATION OF TIH MATERIALS

1. Designate an individual with overall responsibility for hazardous materials transportation security planning, training, and implementation. This individual should report directly to an executive officer of the company. Designate an individual with overall responsibility for security planning and countermeasure implementation for company-designated critical infrastructure.
2. Conduct exercises, at least annually, to verify the effectiveness of security plan(s).
3. Develop and conduct an internal or external company audit program to independently verify that the security plan is being effectively implemented. The audit process should include a policy for record keeping of the audit and a method for management review and performance measurement.
4. Identify and then annually review company-designated critical infrastructure. Ensure that changes or additions to the operating environment have been properly addressed.
5. Maintain a communications network to receive timely government notices of current threat conditions and available intelligence information. Adjust security measures as necessary to reflect current threats and vulnerabilities based on available information.
6. Make use of opportunities to establish liaison and regular communication with federal, state, and local law enforcement, emergency responders, security agencies, and industry partners. Strive to make local law enforcement aware of railroad security issues.
7. Establish liaison and collaboration with other railroad security offices to promote information sharing and security enhancements.
8. As with industry safety programs, regularly reinforce security awareness and operational security concepts to all employees at all levels of the organization.
9. Reinforce the need for employees to immediately report to the proper authorities all suspicious persons, activities, or objects encountered.
10. Have contingency plans in place to supplement company security personnel to protect company-designated critical infrastructure as threat conditions warrant such as contracts to engage private security guard providers or procedures to request supplemental physical security assistance of federal, state, local, and tribal authorities.
11. Restrict access to information controlled by the railroad that it determines to be sensitive, in particular information about hazardous materials shipments and security measures.
12. Make available emergency response planning materials, and when requested, work with local communities to facilitate their training and preparation to deploy and respond to an emergency or security incident.
13. Cooperatively work with the federal, state, local, and tribal governments to identify through risk assessments those locations where security risks are the highest. Cooperatively work with the federal, state, local, and tribal governments to identify and implement protective measures at these locations.

**DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF TRANSPORTATION**

ACCESS CONTROL SECURITY PRACTICES

14. 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 of reporting suspicious activity.
15. To the extent feasible and practicable, utilize photo identification procedures for company-designated critical infrastructure. Establish procedures for background checks and safety and security training for contractor employees with unmonitored access to company-designated critical infrastructure.
16. To the extent feasible and practicable, and as threat conditions warrant, restrict the access of contractors and visitors at non-public areas of company-designated critical infrastructure and monitor the activities of visitors in or around such infrastructure.
17. Establish employee identification measures for all employees. Conduct spot checks of identification as threat conditions warrant.
18. Implement measures to deter unauthorized entry and increase the probability of detection at company-designated critical infrastructure as threat conditions warrant. To the extent patrols are utilized, vary the pattern and schedule to avoid predictability.
19. Utilize interlocking signals and/or operating rules to prevent trains from occupying moveable bridges until they are locked in place.

EN-ROUTE SECURITY PRACTICES

20. Maintain systems to locate rail cars transporting TIH materials in a timely manner to enable the implementation of security measures when necessary and provide information on the location of rail cars carrying TIH materials to DHS and DOT, as requested, in case of events of national significance.
21. During required on-ground safety inspections of cars containing TIH materials, inspect for any apparent signs of tampering, sabotage, attached explosives, and other suggested items. Train employees to recognize suspicious activity and report security concerns found during inspections.
22. Provide local authorities with information on the hazardous materials transported through their communities consistent with AAR Circular OT-55.
23. Consider alternative routes when they are economically practicable and result in reduced overall safety and security risks. Work with the DHS and DOT in developing better software tools to analyze routes.
24. In rail yards, to the extent feasible, place cars containing TIH materials where the most practical protection can be provided against tampering and outside interference when appropriate for the threat level in the geographic area in accordance with the AAR Security Management Plan.