Freight Railroad Security

Railroads employ a multi-faceted, cooperative approach that unites private and public sector capabilities to prevent and respond to security threats. These security practices can be applied across modes of transportation and critical infrastructure sectors. Railroads are not resting on their laurels though — driven by initiative, innovation and investment, they are committed to further improvement in all matters related to security.

The rail industry maintains a comprehensive Security Management Plan.

In the immediate aftermath of the 9/11 terrorist attacks, railroads worked cooperatively to develop the rail industry's Security Management Plan. Put into effect in early 2002, the plan constitutes a comprehensive blueprint of security enhancement and risk mitigating actions. Railroads regularly review, evaluate and update the plan in consultation with government and private security and intelligence experts to ensure continued effectiveness in the face of evolving security threats.

The unified, intelligence-driven approach maintains four alert levels that call for increasing physical and cyber security measures based on intelligence assessments and analyses of developing threats. More than 130 North American railroads — including all freight railroads that transport security-sensitive materials through high-threat urban areas — have integrated the security plan into their respective networks and operations.

Key Takeaway

Railroads protect the rail network 24/7 through a multi-faceted, cooperative effort that taps the full range of capabilities in the private sector and government to ensure preparedness and to deter and respond to hostile acts. Preparedness and capabilities testing includes:

- Physical and cyber security drills and exercises conducted by railroads at their own facilities.
- Joint security and related preparedness exercises held with local police and emergency responders.
- Table-top exercises held within the industry and/or with local, state and government officials.
- Cross-sector exercises coordinated by federal agencies in the United States and Canada.

Each year, the rail industry and other critical infrastructure sectors participate in the North American Railroad Industry Joint Security Exercise to test the security plan, evaluate preparedness, and enhance capabilities or procedures using lessons learned. This exercise involves security, police and operations professionals from freight and passenger railroads in the United States and Canada; the security team and other functional staff from the Association of American Railroads (AAR); information technology leads from Railinc; and officials from government security and law enforcement agencies including the TSA, DHS and FBI.

In addition to the industry-level exercise, each year railroads engage in scores of individual company initiatives to evaluate and enhance employee awareness efforts and support emergency responders in the jurisdictions in which they operate, This collective effort reflects the sustained commitment across the industry to implement and sustain measures and actions to prevent and respond to physical and cyber threats.

Timely and consistent information sharing is essential to effective security measures.

The rail industry's commitment to information sharing is most directly demonstrated in the daily efforts of the **Railway Alert Network (RAN)**. Since the implementation of the security plan in early 2002, the rail industry has maintained the RAN, managed by AAR, to serve as the security information center for North American railroads. By analyzing evolving intelligence, the RAN supports security awareness through timely advisories and information briefs on potential terrorist tactics, malicious cyber activity, rail-related threats and incidents, and other suspicious activity. Railroads regularly use these materials in their employee security training and awareness programs. The RAN also shares security awareness products with counterparts in other transportation modes and with government security officials in the United States and Canada.

Two dedicated industry committees serve as the main channels of communication and coordination with government agencies on security issues.

- **Rail Security Working Committee (RSWC)**: The RSWC is a standing committee that coordinates the rail industry's overall security effort, focusing principally on physical security and emergency preparedness. Supported by AAR security staff, this committee is comprised of senior executives, security staff and police chiefs from the major freight railroads, Amtrak, and multiple short line freight railroads and commuter carriers. As a principal responsibility, the RSWC conducts the recurring reviews and updates of the industry security plan and manages the annual exercise program. Open and candid dialogue by committee members with officials at TSA, DHS, the FBI, DOT and Transport Canada has led to innovative, cooperative approaches for addressing actual and potential security threats, incidents and significant concerns, which enhance preparedness for prevention and response.

- **Rail Information Security Committee (RISC):** The RISC — an industry-formed and led group — was established in 1999 by the seven Class I railroads and Amtrak to coordinate the industry's unified efforts for cybersecurity. The RISC is comprised of chief information security officers and information assurance officials for railroads and industry organizations. It is augmented by AAR security staff, and cooperates with federal cybersecurity agencies, including DHS's Cybersecurity and Infrastructure Security Agency (CISA), the FBI and TSA to share timely information on cyber threats and develop effective countermeasures.

Railroad's nationwide workforce plays a vital role in protecting the network.

The vast majority of U.S. freight and passenger rail employees receives security training during orientation upon initial hiring and continuing with periodic sessions throughout their tenure. Training focuses on enhancing awareness and understanding of indicators of potential security concerns and reinforcing timely reporting of observations per the procedures maintained by the respective railroads.

The effectiveness of this recurring security training is clear. Rail workers account for the vast majority of reports of suspicious activity in and around rail facilities and operations, facilitating effective, efficient industry coordination with and regulatory reporting to TSA, the FBI, Transport Canada and others. Their informed vigilance can, and does, make the essential difference.