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 cybersecurity 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.

**Cybersecurity**

The Rail Information Security Committee (RISC) — an industry-formed and led coordination group — is the focal point of the industry’s unified, cooperative cybersecurity efforts. The RISC comprises chief information security officers and information assurance officials for railroads and industry organizations, augmented by AAR security staff. Representatives of the then seven Class I railroads and Amtrak established RISC in 1999, meaning the railroad industry has proactively enhanced cybersecurity through a dedicated forum for over 20 years.

Immediately following the 9/11 attacks in 2001, railroads came together to assess security risks. The assessments focused on operations, infrastructure, hazardous materials (hazmat) transportation, military shipments, and communications and computer systems with the goal of detecting and preventing terrorism.
Security Plan Testing

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 and procedures using lessons learned. This exercise involves security, police and operations professionals from freight and passenger railroads in the U.S. and Canada; the security team and other functional staff from the AAR; IT 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 prevent and respond to physical and cyber threats.

Information Sharing

Timely and consistent information sharing increases security. The daily efforts of the Railway Alert Network (RAN) are a good example of the rail industry’s commitment to information sharing. 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 information with counterparts in other transportation modes and government security officials in the U.S. and Canada.

Working Committees

Two dedicated industry committees coordinate with government agencies.

- **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 comprises 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 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 was established in 1999 by the seven Class I railroads and Amtrak to coordinate the industry’s unified efforts for cybersecurity. The RISC comprises 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.

**Employee Vigilance**

Rail employees play a vital role in protecting the network. Most U.S. freight and passenger rail employees receive security training during orientation upon initial hiring and continue with periodic sessions throughout their tenure. Training focuses on enhancing awareness and understanding indicators of potential security concerns and reinforcing timely reporting of observations per the procedures maintained by their respective railroads. The effectiveness of this regular security training is clear. Rail workers account for most reports of suspicious activity in and around rail facilities, facilitating effective industry coordination with and regulatory reporting to TSA, the FBI, Transport Canada and others. Their informed vigilance is essential.