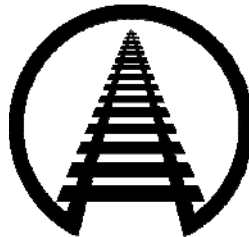


TESTIMONY OF
THOMAS L. FARMER
ASSISTANT VICE PRESIDENT — SECURITY
ASSOCIATION OF AMERICAN RAILROADS



BEFORE THE
U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION
HEARING ON INDUSTRY PERSPECTIVES REGARDING THE
AUTHORIZATION OF THE TRANSPORTATION SECURITY
ADMINISTRATION FOR FY 2012 AND 2013

July 12, 2011

Association of American Railroads
425 Third Street SW
Washington, DC 20024
202-639-2100

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to appear before the committee and discuss the reauthorization of the Transportation Security Administration (TSA) and rail security issues generally. In freight rail, AAR members account for 72 percent of track mileage, 92 percent of the industry's employees, and 95 percent of revenue. North American freight railroads provide the vital link for goods and commodities used by industries and consumers throughout the continent and in the global market. Indeed, one third of all U.S. exports are transported by rail at some point en route to their destinations worldwide. Amtrak, America's national passenger railroad, is a member of AAR, as are several commuter railroads. A joint Freight and Passenger Coordinating Committee established by AAR provides a forum to advance an integrated approach on matters relating to rail safety, operations, and security.

Overview of the Rail Industry Security Program

The Industry Commitment. Safety and security are top priorities for railroads, freight and passenger, for their employees, for their operations, and for the communities they serve. In early May, following the raid that resulted in the killing of Osama bin Laden and the seizure of a high volume of materials on al-Qaeda's operational status and plans – an achievement for which all involved in the United States government and military deserve the highest commendation – widespread media reporting focused on a document indicating al-Qaeda interest as of February 2010 in attacking trains, potentially in connection with the tenth anniversary of the terrorist attacks on the United States on September 11, 2001. This revelation produced a unique opportunity – insight into the adversary's thinking, gained from a place believed impregnable to intrusion or seizure. However, al-Qaeda's inclusion of rail as a target is not surprising. The extensive efforts devoted to security enhancement since the 9/11 attacks, by the railroads at their

initiative and by the Federal security and intelligence agencies, have been premised on this reality.

In the immediate aftermath of those attacks, a security task force consisting of some 150 officials representing railroads, supported by experts in security and intelligence, conducted a comprehensive risk assessment with the objective of developing an industry-wide security plan. Using national intelligence community best practices, five critical action teams scrutinized different aspects of the railroad system: hazardous materials transport; rail operations; critical infrastructure; information technology and communications; and military movements. Collectively, this analysis examined and prioritized railroad assets, evaluated potential vulnerabilities, and assessed threats, and then identified a range of countermeasures.

This effort culminated in December 2001 with issuance of the Terrorism Risk Analysis and Security Management Plan, a comprehensive, priority-based blueprint of actions that remains the foundation for the industry's proactive, coordinated approach and for individual railroads' security programs. The plan included more than 50 permanent security-enhancing countermeasures that were immediately implemented and provided for elevated security based on increases in the terrorist threat.

Continuous Improvement. But no one is resting on laurels. The Class I railroads, and many regional and short line carriers, have adapted the plan to their unique operating circumstances. Implementation of the plan is exercised on a recurring basis – by railroads individually and collectively as an industry on an annual basis. These exercises appraise the effectiveness of the industry's security plan in realistic terrorism prevention and response scenarios. The most recent industry-wide exercise occurred on October 15, 2010; the next is scheduled for October 13, 2011. For this year's event, we have invited direct participation by Federal entities – TSA, DHS,

FBI, and the Federal Railroad Administration (FRA) – specifically to assure effective implementation of an efficient, understandable, and sustainable process for sharing of intelligence on security threats and incidents with the rail industry, freight and passenger.

The industry security plan is regularly evaluated and modified as needed to ensure maximum continued effectiveness. Lessons learned from exercises and experiences in actual security-related incidents inform reviews and updates of the plan with the specific purpose of assuring its viability to meet changing threat circumstances. A comprehensive review completed in 2009 evaluated the plan’s guiding assumptions, risk methodology, and countermeasures, yielding an updated version that took effect in November of that year. Indeed, railroads – in conjunction with the TSA, other Federal security partners, rail customers, and others – are constantly evaluating approaches to further enhance rail security as part of a continuous improvement process.

Persistent Coordination. An integral element of this effort is the Rail Security Working Committee, supported by AAR’s security staff. Reporting to the railroads’ chief operating officers in the industry’s Safety and Operation Management Committee, the Security Committee consists of senior executives, security officials, and police chiefs with our member railroads, coordinates the overall rail industry security effort, and reflects the industry’s ongoing commitment to work in a coordinated fashion, amongst railroads and with government agencies at all levels. Through monthly consultations, the Committee identifies issues of concern, develops and coordinates implementation of solutions, and presents proposals for coordinated effort with the Federal government. The Committee also participates in joint security coordination meetings with TSA’s Freight Rail Division under the Intermodal Security Training and Exercise Program (I-STEP). These sessions sustain constructive relationships and effective

communication between the railroads' security and law enforcement officials and their counterparts in TSA, DHS's Office of Infrastructure Protection, FRA, and the FBI. The I-STEP forum allows for open and candid discussion of current programs and initiatives, future priorities, and prevailing security issues and concerns.

Information Sharing. Essential to success in the security mission is timely access to accurate and relevant intelligence and security information – an area on which the rail industry security committee places particular emphasis. To sustain effectiveness, the railroads maintain two standing capabilities focused on the railroads security information needs – the Surface Transportation Information Sharing and Analysis Center (ST-ISAC) and the Railway Alert Network – and assign highly experienced liaison officers with the FBI's National Joint Terrorism Task Force and Southwest Border Joint Terrorism Task Force.

Originally established in the 1990s in coordination with the Department of Transportation, the ST-ISAC applies analytical expertise for threats and security incidents that either affect or have significant implications for critical infrastructure, physical and cyber. Working in secure facilities, the ST-ISAC taps a broad range of sources daily, including analytical products from the Federal government (classified and unclassified), to develop and disseminate material to aid in the protection of physical assets and information technology networks and systems. Especially noteworthy are the ISAC's efforts in cyber security. Each day the ISAC issues multiple advisories to the railroads each day addressing potential vulnerabilities in specific software or equipment and providing guidance on protective measures. This material directly supports the extensive and effective cyber security programs maintained by the major railroads. A standing Rail Information Security Committee provides a forum for regular

consultations amongst professionals across the industry and a mechanism for the sharing of effective security practices.

The Railway Alert Network (RAN) serves as the security information center for the rail industry, focused on providing immediate alert notification of serious incidents and emergencies and on analysis of the implications to freight and passenger railroads of intelligence and security information relating to threats, incidents, suspicious activity, and terrorists' capabilities, tactics, and techniques. Functioning within a secure facility with classified communications capabilities, the RAN performs a daily review of information from a broad range of sources for relevance to rail and homeland security. Targeted security information and awareness messages are developed for the railroads and shared with security partners in their operating areas at the local, State, and Federal levels.

A particularly noteworthy initiative is the Transit and Rail Intelligence Awareness Daily (TRIAD), produced jointly with the American Public Transportation Association (APTA), the ST-ISAC, and the Public Transit Information Sharing and Analysis Center (PT-ISAC). TSA supports this cooperative effort through a joint information sharing working group and funding of the PT-ISAC, pursuant to the authorization of section 1410 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act). The purpose of TRIAD is to present the most significant matters of the day in the areas of suspicious activity and incident reporting, counterterrorism analysis, general security awareness, and cyber security. The target audience is senior executives, and security and law enforcement officials with railroads and mass transit agencies and local, State, Federal, and private sector security partners.

Partnership for Security. Maintaining a constructive relationship with TSA is a top priority of the rail security effort. In 2006, both the freight railroads and passenger railroads, the latter in

conjunction with mass transit agencies, agreed with TSA on a series of security action items and on inspection of the effectiveness of their implementation by TSA Transportation Security Inspectors-Surface. The action items focus on areas foundational to an effective security program – planning, training, exercises, physical security, information security, personnel security, means to raise security posture in response to threats, and related matters. The cooperative program proved quite effective. For passenger railroads and transit agencies, TSA gained a wealth of information on security posture that informed program development, grant program priorities and awards, and identification of “smart security practices.” In freight rail, the demonstrably successful partnership produced substantial reduction of risk associated with transport of toxic inhalation hazardous (TIH) materials. For the DHS Annual Performance Report (2008-2010), TSA reported a 53.6% reduction in risk as of the end of 2008 against the baseline defined in 2006. Significantly, all of this risk reduction, which exceeded the 50% target set by TSA, occurred under the agreed action items, without regulatory compulsion. AS of 2010, TSA reports “an industry-wide risk reduction variance of 95.73% against the original 2005/2006 baseline.” Again, the measures and procedures that made this significant achievement possible predated the promulgation of the Rail Transportation Security Rule (49 CFR Part 1580), their having been implemented by the railroads either on their own initiative pursuant to the industry security plan or to meet the agreed security action items.

Complimenting this progress are cooperative efforts with emergency responders in local communities to enhance awareness and elevate preparedness to respond to hazardous materials (HAZMAT) emergencies. These initiatives include funded, in-depth, hands-on training under realistic conditions for first responders at the Security and Emergency Management Training Center, a component of the rail industry’s Transportation Technology Center, Inc., in Pueblo,

CO. This premier first responder training center is a member of FEMA's National Domestic Preparedness Consortium. Individual railroads conduct training programs and joint exercises with local and regional emergency response units as well.

The rail industry remains committed to cooperative efforts with the Federal government for sustainable security enhancement. In this context, there are several areas that warrant attention.

Issues of Security Concern to the Railroads

Rail Security Strategy. We are approaching the 10th anniversary of the 9/11 attacks. The timing is opportune for a thorough review of the strategy and programs for rail security generally (freight and passenger). What are we doing? Why are we doing it? What are the core priorities? How can we be more efficient and effective? TSA's Freight Rail Division has agreed to discuss these issues at a meeting to be held next month.

Intelligence Support for Rail Security. The foundation for the effectiveness of any security strategy is intelligence. On multiple occasions since May 2010, the rail industry has submitted, separately to DHS and to TSA, a priority intelligence requirement seeking expansion of the depth of analysis of past terrorist attacks, attempts, and plots targeting rail. The objective is to know what we can know – as fully as possible – through in-depth analysis of the preparatory actions in successful terrorist attacks, failed attempts, and foiled plots that have targeted rail. The purpose: to draw insights into the mindset and thinking of the adversary, of how terrorist operatives function, and thereby enable better informed and more effective security measures.

DHS and FBI intelligence products commonly reference the Terrorist Planning Cycle as a means to “assist organizations with their development and implementation of protective measures to deter, detect, disrupt, and defend against attacks from both domestic and

international terrorists.” Substance needs to be added to this good advice. For rail security, this substance entails a breakdown against each phase of the cycle, in as much detail as the available information allows, of the known or inferred elements of target selection, planning, preparation, and execution, either by single operations targeting rail or by a composite analysis of multiple such operations. With preparatory and execution activities so delineated, opportunities can be identified where particular types of security measures and activities may prove effective in deterrence or disruption. In essence, we are seeking to expand the concept of “actionable intelligence” to include analysis that creates opportunities for security.

Rail Security Inspection Activities. In multiple forums over an extended period, the railroads have expressed concern with inspection activities by TSA’s Transportation Security Inspectors-Surface. The industry’s principal concern is the inconsistency and lack of standardization in inspectors’ interpretations of TSA’s security regulations and expectations regarding rail security in general. There are disparities between the policies and guidelines set by TSA’s Freight Rail Division and the actions of surface inspectors in the field. Actions accepted by some TSA field offices result in official citations as violations by others. Another problem is repeated bypassing of the communication and coordination process – with the Rail Security Coordinators (RSCs) – appointed pursuant to TSA regulations. TSA, and other DHS components, sometimes directly engage with rail employees in the field, who often lack the authority and means to address the issues raised by the inspectors.

AAR believes the Regional Security Inspectors (RSIs) appointed as liaison to the Class I railroads and Amtrak offer a viable and sustainable means to resolve these concerns. However, organizationally they are not in the chain of command of the surface inspectors in the field. Yet, the official correspondence sent to the railroads that announced the appointment of the RSIs

defines a scope of authority and responsibility well-tailored to attaining this objective. Key points from these letters include:

- “the RSIs-Surface will act as the points of contact for the Class 1 and Regional Railroads”;
- “to ensure consistent application of regulations both nationally and across a railroad’s operating system”;
- “coordinate TSA field activities...to minimize negative impact on your railroad operations”; and
- “use your new RSI-Surface to the fullest extent.”

Substantively engaged, consistent with the above commitments, we do believe the RSIs can bring about greater consistency and standardization in inspection priorities and activities, with benefits for the government in quality of results and for the railroads in operational efficiency. Further, this approach can assure early and efficient resolution of issues of security concern – using the communications process TSA has established by regulation and expressly referenced in the RSIs’ appointment letters.

Effective Deployment of Visible Intermodal Prevention and Response (VIPR) Teams. The rail industry acknowledges the potential value of the VIPR program’s random and unpredictable security measures for deterrence and disruption of terrorist planning and preparations. Indeed, some railroads, passenger and freight, have hosted deployments and derived substantial benefits from the visible security enhancement. Across the industry, however, inconsistency in the implementation of this program remains a significant concern – in management (conflicts and duplications between TSA field offices) and in execution of operations (continuing instances of inadequate notice to and coordination with railroads on operations). For mass transit and

passenger rail, TSA abides by agreed protocols for notice, coordination, planning, preparation, execution, and after action review. A similar approach should be used for the rail industry as a whole. Fundamental aspects of the program should include:

- Prior notice to the railroad by TSA of all proposed VIPR deployments at least two weeks in advance, unless a credible threat or other emergency circumstances dictate otherwise.
- Joint development by TSA and the affected railroad(s) of the operations plan for each VIPR deployment or group of deployments.
- Integration of local law enforcement in the VIPR deployment(s) to foster informed partnerships and elevated preparedness for joint security enhancement actions.
- Clearly stated risk-based justifications for the deployments.

Analysis and Use of Reports on Significant Security Concerns Submitted to the TSA

Freedom Center (TSOC). The Rail Transportation Security Rule, at 49 CFR section 1580.105 for freight railroads and 49 CFR section 1580.203 for passenger railroads, requires the reporting of significant security concerns to the TSA Freedom Center. To date, despite its substantial volume, this reporting has not produced consistent analysis for trends of concern in rail security or for educative value from the security awareness and heightened vigilance perspective.

However, the Freedom Center does widely disseminate the railroads' reports to an extensive audience of Federal, State, and local government officials, selected public transportation authorities, and other private sector representatives. The criteria for this distribution are unclear, as many recipients have no responsibilities for rail security. Meanwhile, the railroads do not receive directly the TSOC reports or any significant feedback on the analysis or implications of the reports they submit. Yet, this reporting does create an opportunity to identify potentially "high value" information, discern developing trends of potential concern or their absence, and

disseminate analyses that will inform steps to elevate preparedness and capabilities to prevent and immediately respond to acts of terrorism. A consistent process would enable a continuing educational opportunity for application by railroads in their efforts to assure continuous vigilance and security awareness. The existing intelligence and security information dissemination process maintained through the Railway Alert Network (RAN) would assure distribution of these analytical products to appropriate officials with railroads nationally, freight and passenger.

Flexibility in Grant Investments to Expedite Security Solutions. DHS manages a wide range of grant programs aimed at enhancing capabilities to prevent, respond to, and recover from acts of terrorism and natural disasters. Often, investments in these capabilities yield benefits for resiliency that offer advantages in both categories of risk. Unfortunately, however, the rules associated with these grant programs frequently impose limitations on the ability to apply them in effective ways for expedited and sustainable solutions. As all of these programs aim to achieve a similar purpose, the guiding principle should be: enable the grants to solve the most pressing problems instead of allowing program rules to limit the problems that can be solved. Wherever practicable, the benefits of unity of effort and economies of scale should inform decisions on funding for projects. As a representative example, TSA's Freight Rail Division has worked in coordination with the railroads to complete vulnerability assessments on more than 70 rail bridges in the Western Rivers System – principally crossings of the Mississippi, Missouri, and Ohio rivers. The resulting reports make recommendations on mitigation measures, ranking the bridges in priority. A composite approach to Federal support through grant funding of bridge hardening projects – drawing upon not just the Freight Rail Security Grant Program but also the State Homeland Security Grant Program, the Urban Area Security Initiative where applicable, the Transit Security and Intercity Passenger Rail Security Grant Programs for structures with

passenger train service, and the Port Security Grant Program – can expedite redress of the potential security concerns identified in the assessment process.

To TSA's credit, significantly broader flexibility has been shown in the outreach forums to grant-eligible entities for the FY 2011 cycle. Support has been expressed for composite projects, both those integrating different functional areas, such as a single application seeking funding of technological enhancements and operational activities to enhance security at a critical rail station, and those that offer the potential to link funds from the Freight and Transit Security Grant Programs. We hope this positive trend continues.

Commuter Rail Security Enhancement. As noted at the outset, AAR has established a joint Freight and Passenger Rail Coordinating Committee to foster sustained, cooperative effort on issues of security concern. Major terrorist attacks overseas have targeted commuter trains in major cities, with the bombings in Madrid (2004) and Mumbai (2006) as dramatic examples. In the United States, commuter rail has been the subject of threats, notably the expressed interest in targeting commuter trains revealed in November 2008. A collaborative project, integrating government and industry, focused on development of a sustainable security enhancement strategy for commuter rail would provide substantial benefits. This effort should combine varied joint operations with local law enforcement departments and testing of tailored security technologies, with resource support from security grant allocations.

Conclusion

Assuring the security of the nation's passenger and freight railroads requires a multifaceted, cooperative effort that taps the full range capabilities – in the private sector and at all levels of government – and applies them to best effect to assure preparedness and enhance capabilities to prevent and respond to acts of terrorism.

Our nation's railroads look forward to working with policymakers and others in a true public-private partnership to see that this objective is met successfully.