

**STATEMENT OF FRED E. WEIDERHOLD
INSPECTOR GENERAL
AMTRAK**

**BEFORE THE
U. S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY**

**Hearing on the
Rail and Public Transportation Security Act of 2007**

March 6, 2007

**AMTRAK
OFFICE OF INSPECTOR GENERAL
10 G STREET, NE
WASHINGTON, DC 20002
(202) 906-4600**

Thank you for the opportunity to appear before you today to discuss rail security issues and the Rail and Public Transportation Security Act of 2007 draft bill. I share the Committee's concern and sense of urgency that much more can be done to secure and safeguard our nation's rail and transit assets. The responsibility to act is shared among federal, state, and local governments, and the private sector, and your bill will help jump start some long overdue initiatives.

You have heard testimony from many witnesses about the complexity of the rail environment, the challenges to secure such an 'open system', and the need to balance vulnerabilities, threats, and risks in allocating federal security dollars --- these are real challenges. Having worked intimately with passenger rail safety and security issues for over twenty years, I will tell you the work to secure the railroad is very difficult, and often frustrating; however, I will also tell you that collectively we can greatly improve our readiness.

Before offering specific comments on the draft bill, I would offer some over-arching observations for your consideration:

- **The time to take action to possibly prevent, mitigate, and recover from a terrorist attack involving rail and transit assets is quickly passing -- we need to act now.**

The reality, as the Committee Members are very well aware, is that we are operating our rail services in the wake of Madrid, London, Mumbai, and other cities where terrorist have elected to wage their war. I suspect that every witness who testifies before you about rail and transit security will invoke the names of the cities attacked, but how much have we really accomplished over the past several years --- clearly, not enough. The Committee has received testimony from the GAO regarding delays to the Transportation Sector Specific Plan, and the Committee is taking action to ensure better coordination of transportation security strategies and plans. Amtrak is not waiting; its Board, its new Chief Risk Officer, and management have made new commitments to increase significantly its canine resources, place more of its own, and other, police and security on its trains and in its stations, review its screening protocols, re-direct capital monies to critical asset protection, and 'build-in' security wherever possible. Your bill, and the specific inclusion of funds to address Amtrak's security investment needs, is welcome and appreciated.

- **Capitalize and leverage the collective knowledge and experience that cuts across Departmental boundaries and the public and private sectors.**

Your bill requires greater cooperation and real coordination between and among those Departments and agencies with responsibilities for homeland security; this is a great message. It is an understatement to say we are not using all of our resources optimally. The GAO has commented that the sheer number of public and private stakeholders, and the complexity of our rail systems, may lead to duplication of effort, communications challenges, and confusion about roles and responsibilities --- that has happened. The good news is there has been some progress -- in well executed, risk-based vulnerability assessments, in meaningful state and local law enforcement cooperation, in emergency response training, in advancing security technologies (helpful, but not a panacea), and, mostly, in very good people stepping forward, trying very hard

to work the issues. DHS and DOT must continue to reach out and tap these resources, and rail and transit security should not be compromised or relegated to turf struggles.

- **Ensure security standards and best practices are fully developed before regulations are promulgated.**

One of the difficulties we have encountered in evaluating Amtrak's efforts to improve its security posture is the lack of security standards that have been fully vetted, practiced, and iterated. Although some security directives were prepared by TSA in May 2004, these directives are not necessarily the comprehensive bases for an effective rail passenger security strategy or effective regulations. The Committee may want to direct a joint Department review of the effectiveness, lessons learned, and potential enforceability, of the existing TSA Security Directives (RAILPAX 04-02) before additional directives are enacted.

The Committee should look to organizations like APTA, which is recognized as a Standards Development Organization, as a starting point to develop baselines for rail security and emergency preparedness best practices. Amtrak also is re-examining its protocols and will most likely redefine its own baseline security standards, working closely with domestic and international rail and transit partners, as well as DHS and DOT.

- **Ensure linkage between security and safety.**

One of the definitions we are using within Amtrak to determine when we have achieved adequate security awareness is when security has the same status as safety on our railroad. All rail operators --- be they freight, passenger, or transit --- live and practice safety in their daily work lives. Railroaders begin their day with safety messages and safety inspections; we train for it, we measure it, we have recognition ceremonies to celebrate it, and we do not take it for granted. In the new world of terrorism, especially terrorism directed at rail and transit, the same must become true for security. Certainly, there are protocols, practices, and skill sets that differentiate security from safety, but the work is performed over the same assets and the same operations. Whenever possible, security and safety should be addressed concurrently.

Specific Comments for Draft Bill:

Section 3 – National Strategy for Rail and Public Transportation Security

This section requires that the Secretary of the Department of Homeland Security (DHS), in consultation with the Secretary of the Department of Transportation (DOT), develop a comprehensive modal plan for covered transportation. While consultation is certainly a prerequisite for effective working relationships between the two Departments, there will also be occasions where close coordination is required, where interdepartmental, cross-functional teams should be established, and where joint operations may be warranted.

At Section 3 (a) (4), the Committee includes a requirement that DHS and DOT develop a process for expediting security clearances and facilitate intelligence and information sharing. The Committee may wish to prioritize this requirement by mandating an expedited security clearance

process for select senior rail and transit officials (CEO, COO, Chief Security Officer or equivalent) for all carriers assigned to the high risk tier. Senior railroad officials have had to wait well over one year for such clearances. Additionally, the Committee may want to direct that the processes for facilitating intelligence and information sharing be evaluated by the Department OIGs.

At Section 3 (a) (7), the Committee requires that the joint modal plan include, “a framework for resuming the operation of covered transportation in the event of an act of terrorism and prioritizing resumption of such operations”. This directive is highly significant because it requires DHS and DOT to become attentive to continuity of operation planning, not just for individual carriers, but for transportation systems.

Section 4 – Assignment to Risk-Based Tiers

We agree that it is extremely important to establish criteria by which those carriers and systems that face the greater risks are prioritized. Terrorists’ strikes against rail targets have historically involved light rail passenger systems and transit, often focusing on multiple targets, and, as we saw in the London bombings, follow-up attacks on connecting bus services. For these reasons, we encourage assignment based on modal and inter-modal “systems” as well as individual providers within those systems.

Section 5 – Rail and Public Transit Assessments and Plans

We agree with the Committee’s direction to mandate vulnerability assessments and security plans for the rail sector. We know the Committee will find many carriers have already completed such assessments, and security plans have been prepared and are exercised during heightened threat levels.

Using DHS Office of Domestic Preparedness (now Grants & Training) funds, vulnerability assessments for Amtrak’s Northeast Corridor and Chicago Union Station were completed in May 2006. Vulnerability assessments for the balance of most of Amtrak’s other system assets should be completed this fiscal year. The methodology used for Amtrak’s vulnerability assessments are consistent with that used for the majority of the transit properties. We believe these assessments, while not exhaustive, provide a valuable mapping of the vulnerabilities of key Amtrak, and Amtrak-used, assets, but these are only starting points.

The Amtrak OIG has observed that many of the vulnerability assessments are carrier-specific and not necessarily linked to larger system or nodal vulnerabilities. An appropriate role for a DHS Area Rail and Public Security Committee, or larger DHS entity, would be to link the assessments and plans into a larger rail transportation security matrix.

An interesting provision that the Committee recommends in Section 5 (f) is for Security Performance Requirements (for the security plans). We presume the performance requirements are intended to answer the question of ‘how effective’ the security plans are in adding to value to security preparedness. These performance requirements may evolve into the ‘successor’ guidelines to the RAILPAX Security Directives.

The Committee, and DHS and DOT, need to appreciate the complexity of the passenger rail operating environment and impact on stakeholders with respect to conducting vulnerability and threat assessments and preparation of security plans. For example, Amtrak serves over 500 rail stations across the country, but owns less than 80. Initially, Amtrak began its vulnerability assessments of Amtrak-owned properties, and, only later, expanded its assessment approach to include other ‘Amtrak-used’ assets. Even using an “owned assets” approach, there are difficulties in implementation with the myriad of stakeholders sometimes present.

For example, here at Washington Union Station, part of the facility is directly owned by Amtrak (from the gate areas north), the Main Hall and retail facilities are owned by the Union Station Redevelopment Corporation (USDOT, Amtrak, DC), areas of Columbus Circle are owned/controlled by the U.S. Park Police, Capitol Police, and the District of Columbia. In addition, Virginia and Maryland operate state-supported commuter services into the station (using both Amtrak and CSX operating crews and equipment). Which entity should have responsibility for vulnerability assessments and security planning for a complex property or inter-modal facility?

Given the criticality and iconic value of an asset such as Washington Union Station, Amtrak, appropriately, elected to undertake assessments that involved all property owners, all operators and users, and other stakeholders. At other stations and facilities, it may be less clear.

Section 6 – Strategic Information Sharing

The goal of this requirement is to develop an information sharing plan to ensure the development of both tactical and strategic intelligence products for the rail sector, with special attention being paid to the coordination of intelligence analyses between TSA and other intelligence groups. We agree with this recommendation.

Amtrak has access to several sources of intelligence information today, both through DHS and DOT, as well as through other sources. Amtrak participates in the Surface Transportation Information Sharing and Analysis Center (ST-ISAC), which was established and is maintained by the Association of American Railroads (AAR). The ST-ISAC provides useful information to Amtrak, especially in the areas of cyber-security and after-action threat analyses. Amtrak also participates in the Railway Alert Network (RAN), another AAR-maintained information and intelligence sharing system.

More recently, Amtrak placed personnel on the FBI’s New York and Washington Field Office’s Joint Terrorism Task Forces (JTTFs), and the National Joint Terrorism Task Force (NJTTF), with access to those units’ intelligence centers. Additional Amtrak and OIG staff are assigned to various Department of Justice sponsored Anti-Terrorism Advisory Councils (ATACs) and working groups.

I would rate the dissemination of unclassified information, For Official Use Only (FOUO), and Sensitive Security Information (SSI) to Amtrak as good and improving. However, we absolutely

share the AAR's concern about the critical need to safeguard and compartmentalize all classified information, including SSI.

With respect to Section 6 (e), regarding the relationship of Security Clearances to intelligence information dissemination, the Committee and DHS may want to consider greater use of intelligence 'tear sheets' to disseminate more critical information. Additionally, the Committee and DHS should be concerned about the availability and use of classified communications channels with rail sector officials.

The Committee should also be cognizant of the fact that rail service providers, when conducting vulnerability, threat, and risk analyses, as well developing security plans and mitigation and response strategies, are generating a considerable amount of highly sensitive data that can be easily exploited to the provider's, and the nation's, detriment. Amtrak has taken advantage of DHS's Protected Critical Infrastructure Information Program by submitting work product for protection under the Critical Infrastructure Information Act.

Section 7 – Rail Security Assistance

Amtrak strongly supports its inclusion as an eligible entity for security improvement grants. A stable funding mechanism for sustained security and emergency preparedness improvements at Amtrak, and within the passenger rail sector, is critically important.

Most of you know that Amtrak's financial condition has been precarious in recent years, and Amtrak's funding of police and security operations has been limited to its own internal police forces (about 350 persons) and work on a major fire and life-safety tunnel project in New York City. Amtrak was requested, on several occasions, by both House and Senate Members to delineate what it needs to advance its security and emergency preparedness, but well intended bills have never been enacted.

Since FY 2005, Amtrak has been allocated only about \$22 million in DHS grant funds. Amtrak has used some of these grant funds to conduct vulnerability assessments, install a pilot chemical sensor system in four stations, fund a Washington, DC tunnel security pilot project, and fund several other higher priority projects. However, there are many more security and emergency preparedness projects and initiatives for Amtrak that require the support contemplated by the Committee's bill.

In addition to those grant funds available to Amtrak under the Committee's bill, Amtrak's Board of Directors and its senior management are committed to doing as much as possible within the limits of Amtrak's internal finances. Amtrak's new Chief Risk Officer, a former high ranking DHS manager, has requested that Amtrak increase its canine units and work immediately to get more police and counter-terrorism security forces riding its trains. Amtrak has had great difficulty in filling its police and security staffing levels because its pay and retirement benefits are well below those of competing jurisdictions, resulting in double-digit attrition and a high vacancy rate. The Chief Risk Officer is working closely with Amtrak's authorizing committees to find relief for this most serious problem.

Section 10 – Fire and Life Safety Improvements

We strongly support the Committee's recommendation to provide additional grant authority to address security issues involving Amtrak's Northeast Corridor tunnels.

The New York City, Baltimore, and Washington DC, underground and underwater tunnels present special safety and security issues for Amtrak.

In New York City, over 1,100 trains daily use the 81,000 feet of tunnels into out of the City, with Amtrak and New Jersey Transit using the North River Tunnels beneath the Hudson River, and Amtrak and Long Island Rail Road using the East River Tunnels.

The scope of Amtrak's current Life Safety Program, valued at \$470 million for Phase One, with a completion date of 2009, encompasses the construction of three major ventilation structures in Weehawken, New Jersey, Queens, New York, and Manhattan. Also included in this project is the installation of a fire standpipe system throughout the New York Penn Station complex. The Weehawken Ventilation plant was placed into service in January 2005, and the dry standpipe was placed into service in January 2006. Through December 2006, \$279.6 million has been spent on this project, funded through Federal Railroad Administration grants, the Long Island Rail Road, and Amtrak.

Amtrak's Northeast Corridor rail services and Maryland Transit Administration's MARC services pass into the heart of Baltimore through a series of tunnels, which were constructed in 1872. The Baltimore & Potomac tunnels house vital electric power lines and are critical to Amtrak's mainline operations.

With regard to the First Street Tunnel here in Washington, DC, Amtrak is working closely with DHS and is participating in the National Capital Region's Rail Corridor Pilot Project program. This project, which has proceeded much more slowly than I would have hoped, is one which I would like to brief to the Committee at a later time.

Section 11 – Security Training Program

There is no substitute for having a well trained work force who can serve as the 'eyes and ears' and who act as the first line of defense in noticing suspicious activities and things that are 'out of place' on our railroad. Likewise, we need an alert and vigilant public, who know what to do and how to act before and during emergencies, and how to report to matters that warrant the carrier's attention.

Amtrak has followed the Federal Transit Administration's and the American Public Transit Association's lead in developing employee awareness training. Using security awareness training developed by Rutgers University National Transit Institute (NTI) for mass transit employees in 2003, the NTI's transit training modules were modified slightly and customized to address Amtrak's facilities and rail environment. An introductory and mandatory block of four hours of security training, including some class, Web-based, and CD-based training, was

delivered to all Amtrak employees (17,000+) in FY 2006. This training was intended to be equivalent to “Security 101” for railroad workers. An additional four-hour, instructor-led block training for up to 14,000 employees is being delivered in FY 2007, with the first classes started in January 2007. My Office reviewed this training, and we believe that it provides a good foundation of security awareness from which additional, more specialized training can be targeted for select employees. One of the challenges for security training is to keep it topical, customize the training for the scope and responsibilities of the employee’s position, and reinforcing the training through meaningful exercises.

Amtrak has also begun a limited version of the popular “see something, say something” program that is used by a number of transit properties. Amtrak has implemented a station and on-board announcements program, alerting the public to have control of their personal baggage and carry-on articles, and to report suspicious behavior during high threat levels declared at the national level. This program is being expanded to be a part of Amtrak’s normal business practice.

With regard to Section 11 (c) (3), requiring inclusion of “appropriate responses to defend oneself, including using non-lethal force,” as a part of employee security training, we believe this requirement may run counter to prevailing best practice. Amtrak, and most other carriers, recommend that employees, unless trained as police or full-time security staff, avoid physical confrontation, but instead be aware of their surroundings and contact qualified carrier and/or law enforcement personnel at the earliest opportunity.

Section 12 - Security Exercises

Most carriers, including Amtrak, have considerable experience with emergency response drills and exercises, with greater frequency of such activities since 9/11. There is a growing body of ‘lessons learned’ from the exercises, drills, and table-tops, and resulting after-action reports that assist in safety and security investment decisions, and facilitate changes in operational protocols.

From an OIG perspective, I have seen very well conducted and useful security exercises, and I have also seen poorly executed, artificially constrained, and little value added exercises. More importantly, I have seen very meaningful recommendations from exercises and assessments that have not been timely acted upon. I very much support the inclusion of the Remedial Action Management Program, using FEMA’s experiences, in monitoring implementation of lessons learned and best practices. My Office will also be monitoring the adoption and application of observations and recommendations generated by security exercises.

Section 13 – Security Research and Development

The Committee has recognized the need for more collaborative research and development and technology convergence to develop affordable and effective rail security solutions; we very much agree. There are considerable challenges for passenger carriers to find and apply the most appropriate security technologies to fit their environments. Much of what has been accomplished to date by passenger rail is accomplished by information exchanges through existing industry associations and through professional relationships and private sector

marketing. There has been some assistance provided by DHS in the form of providing screening equipment for pilot projects and special security events, but much more can be done in this area.

It is appropriate to recognize important work being done in security technology advancement by the rail industry. The AAR maintains a Transportation Technology Center (TTCI) in Pueblo, Colorado, which is used for both testing and training purposes; Amtrak routinely uses TTCI services. We support the Committee's adoption of the amendment to make TTCI a member of the National Domestic Preparedness Consortium (NDPC).

Amtrak has also established relationships with the Lawrence Livermore National Laboratory, working with the OIG to conduct CBRNE assessments at ten major urban stations; with Argonne Laboratories, to install chemical sensor technology; and with Minnesota State University to install a SMART CCTV system at four stations. Amtrak, and the Amtrak OIG, have also benefited from the work and ongoing support of the Technical Support Working Group in making critical vulnerability assessments of key passenger rail assets.

Section 14 – Whistleblower Protection

We very much understand the desire of the Committee to protect and safeguard those who would come forward to report violations of security-related statutes and regulations. Whistleblower statutes are intended to encourage vigilance using our greatest resource, our employees, by protecting them from retaliation and discrimination for such reporting.

As an Office of Inspector General, my Office responds to whistleblower allegations under the Railroad Safety Act; we also investigate allegations of harassment and intimidation under 49 CFR 225, regarding Railroad Accident Reporting. Additionally, under the Inspector General Act, we have responsibilities that are analogous to whistleblower protection applicable to Amtrak employees.

From our reading of the draft bill, and from an Amtrak OIG perspective, there does not appear to be any precedential equivalent to the allowable damages and criminal penalties for violations of this provision. The Committee may want to extend further inquiry into this area as well as be briefed on the extant DOT whistleblower statutes and regulations, including 49 CFR 42121, which involves whistleblower protection of employees providing air safety information, and applicable DOT reports on whistleblower cases.

Other Recommendations:

- Authorize railroad police officers to exercise law enforcement powers on the property of another railroad. This would allow railroads to better leverage their police and security assets. The proposal was included in earlier legislation from the 109th Congress, sponsored by the House Transportation & Infrastructure Committee.
- With regard to the Committee's proposed directives on background checks, we agree that September 11 altered the vigilance which we all must employ in the transportation industry with respect to third parties as well as employees and contractors. Thus the issue of background checks of certain employees is a somewhat complex issue, yet a critical

piece of the cloak of security. The difficulty lies in the determination of **which** employees should be subject to background checks and **what should be considered disqualifying factors**. In managing a personnel security program, the following factors are vital: assigning risk designations for all employee positions; determining who completes the background checks (carrier/DHS/DOT); determining which background check system is most appropriate (when should NCIC be allowed); ensuring that the background checks are timely and thorough; establishing controls to protect against terminations that are based upon inaccurate or stale information, including the right to submit promptly rebutting information (Amtrak fully complies with the Fair Credit Reporting Act, which already provides a level of protection for individuals to challenge inaccurate information contained in a background check); adopting document control policies for personnel security files; and, ensuring that those performing background checks are properly trained and audited.

For instance, some of the criteria for assessing risk would be unescorted access to secure areas, potential for dangerous activities or compromising one's duties and responsibilities, potential for greatest harm to passengers or human life, and the degree to which oversight can be exercised with respect to such personnel. Amtrak engineers who operate the trains, mechanical personnel who inspect, analyze and repair safety critical parts such as brakes, personnel who work in rail traffic control facilities, and baggage handlers would perhaps all be designated as requiring higher security clearances and the more extensive background checks. Under any contemplated program, carriers would be required to submit its comprehensive plan to be approved by either the Department of Homeland Security or the Department of Transportation.

Background: Amtrak Office of Inspector General

The Amtrak OIG is a fully statutory designated federal entity OIG established by the Inspector General Act of 1978. The OIG was established in 1989, has about 100 employees, and operates from seven field offices throughout the United States.

The OIG is responsible for oversight of all of Amtrak's programs and operations. For the past several years, the OIG has been heavily involved in evaluating and overseeing security operations within Amtrak. Immediately following the bombings in Chechnya, in December 2003, Amtrak's Board Chairman asked me to conduct an in-depth review of Amtrak's police and security operations. My Office worked with the Federal Railroad Administration (FRA) to obtain the services of the RAND Corporation to conduct this review. We were barely one month into our work when terrorists struck the Spanish rail system on March 11, 2004. In May 2004, we provided Amtrak with our observations and recommendations to improve security preparedness and to formalize and upgrade its police and security planning and operations. Amtrak has made some progress toward addressing some of the security shortfalls that were identified, but significant challenges remain.

We have been very forward leaning in our security assessments. During the past two years, my Office has conducted several 'red team' operations covering critical Amtrak assets; we have performed detailed CBRNE site assessments using the Lawrence Livermore National Laboratory

Homeland Defense Operational Planning System (HOPS) group; we have been greatly assisted by the California National Guard and the Technical Support Working Group (TSWG) in contracting for highly detailed, virtual digital mapping of key stations (for use by asset stakeholders and first responders); and we have been similarly assisted by the National Guard Bureau and their Full Spectrum Infrastructure Vulnerability Assessment (FSIVA) teams. We have also independently contracted and sponsored counter-surveillance training for select Amtrak police, OIG staff, and other railroad security staff. In short, we on our own have sought help from almost any quarter, be it federal, state, and private entities, to find those “right things” to do.

My Office and Amtrak also reached out to the international rail and security communities, sponsoring visits in February 2005 from the Guardia Civil, Spain’s premier counter-terrorism unit and Spain’s national railways operator, Renfe. In 2006, Amtrak officials were briefed by both British and Indian Railway officials regarding attacks in their countries, and as recently as last month, Amtrak senior managers were provided special briefings by the British Transport Police.

Another important development affecting Amtrak’s Northeast Corridor was the creation of Northeast Rail Police Coalition. Last year, NYPD Commissioner Ray Kelly called for a summit of police chiefs and other high ranking law enforcement officials from New York City to Washington DC. Commissioner Kelly proposed a coordinated approach by city, state, and local law enforcement to improve passenger rail security. The group, comprised of NYPD, Amtrak Police, Baltimore City Police, Delaware State Police and Delaware Homeland Security, Metropolitan DC and Transit Police, New Jersey Transit Police, Philadelphia Police, and other New Jersey and Pennsylvania State law enforcement, agreed to provide periodic support to Amtrak by boarding trains with officers and bomb dogs at key stations, conducting surveillance of the track and other facilities, and conducting other protective measures. This coalition began their work starting in July 2006, and we are pleased to report has become an integral part of Amtrak’s security operations.

The Amtrak OIG has also joined the President’s Council for Integrity and Efficiency (PCIE) Homeland Security Roundtable, chaired by DHS Inspector General Richard Skinner, where we will be sharing red teaming and other security assessment approaches with the OIG community. And we will begin using the PCIE’s *Guide to Evaluating Agency Emergency Preparedness (November 2006)* in our FY 2007 and FY 2008 evaluations of emergency planning at Amtrak.

We have had extensive involvement in the rail security and the anti-terrorism field.