STATEMENT OF FRED E. WEIDERHOLD
INSPECTOR GENERAL
AMTRAK

BEFORE THE
U. S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND INFRASTRUCTURE PROTECTION

"RAIL AND MASS TRANSIT SECURITY: INDUSTRY AND LABOR PERSPECTIVES"

February 13, 2007

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

Thank you very much for the opportunity to appear before you today to discuss rail security issues affecting passenger rail services and Amtrak. I share your belief that rail security must be a national priority, and I am pleased to attend this hearing. I will tell you today that, although some progress is being made, we are not at all where we need to be on rail passenger security; we have not moved far enough, or fast enough. There should be a strong and united urgency to do the right things that will protect rail infrastructure and rail passengers, and we collectively have much work to do.

As Amtrak's Inspector General, I am responsible for oversight of all of Amtrak's programs and operations. For the past several years, my Office 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 April 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 are a statutory Office of Inspector General (OIG), and 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.

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 evaluations of emergency planning at Amtrak.

Given our extensive involvement in the rail security and the anti-terrorism field, we make the following observations and recommendations to the Committee.

Significant Challenges Exist to Secure Rail Infrastructure and Passengers

The challenges to secure Amtrak and make passenger railroading safer from potential terrorists' attacks are daunting. Amtrak operates in 44 states serving over 500 cities and towns across the nation. Amtrak operates 260 inter-city trains daily, and the company has agreements with 15 states to operate and maintain trains for many intra-state corridor services. As the owner and operator of much of the Northeast Rail Corridor, between Washington, DC and Boston, Amtrak controls and dispatches hundreds more trains for its rail and transit partners, including New Jersey Transit and the Long Island Rail Road. Amtrak directly owns many other critical fixed assets, such as New York Penn Station and Chicago Union Station, and there are other customers and tenants that make use of Amtrak's rights-of-way and other properties. Outside of the Northeast Rail Corridor, Amtrak operates over thousands of miles of the rail lines of its freight partners, where train operations are controlled and monitored by the host railroads.

Our nation's rail system is one of the more open, and some say porous, passenger transportation systems in the world, both with respect to physical infrastructure and the very nature of the business itself. Amtrak's stations and trains are, by design, intended to allow persons to move freely unto and off its trains and through its station portals. There are multiple access points throughout our system and it is difficult to fence, gate, and lock down many parts of the system.

Amtrak also operates trains through various tunnels, in New York City, Baltimore, Maryland, and Washington DC, which present special safety and security issues. However, even given these challenges, effective access control and monitoring at critical nodes and around high value assets must be designed and implemented.

Any attempt to replicate a TSA-style aviation security architecture would most likely be extremely cost-prohibitive and ineffective. This does not mean that there are not significant lessons to be learned from TSA's aviation security model, and certainly some technologies and monitoring processes to be shared, but the final solution set for passenger rail security must be tailored to its unique environment.

Security Funding

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.

Amtrak was <u>not even eligible</u> for DHS grant monies until FY 2005, at which time Amtrak became eligible for approximately $6.0 million of $150 million that was provided for "intercity passenger rail, freight rail, and transit security grants". In subsequent appropriations, Amtrak

received $7.1 million in FY 2006 and $8.2 million in FY 2007. Amtrak has used some of these grant funds to conduct vulnerability assessments, install a pilot chemical sensor system in four stations, fund a Washington 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 your support.

Due to these pressing security funding needs, 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 some relief for this most serious problem.

Employee & Passenger Security Awareness

There is no substitute for having a well trained work force who can serve as the 'eyes and ears' and 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 Agency'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, the transit training modules were modified slightly and customized to address Amtrak's facilities and rail environment. An introductory block of security training, including some class, Web-based, and CD-based training was delivered to all Amtrak employees in FY 2006. This training was intended to be equivalent to "Security 101" for railroad workers. An additional four-hour training block for up to 14,000 employees is scheduled for FY 2007, with the first classes starting 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.

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 had 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.

The OIG believes Amtrak should consider other programs, to include programs for a LEO (law enforcement officer) rider's initiative and adaptation of the British Transport Police's HOT program, a more targeted employee training program to identify suspicious packages and reduce 'false-positive' results.

Vulnerability Assessments & Security Planning

We agree with the Committee's direction to mandate vulnerability assessments and security plans for the rail sector. We believe the Committee will find many carriers have already completed such assessments, but we suspect that many of these assessments are carrier-specific and not necessarily linked to larger system or nodal vulnerabilities. An appropriate role for an 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.

Using DHS Office of Domestic Preparedness (now Grants & Training) funds, an external firm completed a vulnerability assessment for Amtrak's Northeast Corridor and Chicago Union Station in May 2006. Vulnerability assessments for the balance of most of Amtrak's system assets are scheduled to be delivered very shortly. 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.

Vulnerability assessments must be tied to threat and risk-based analyses, which, in turn, drive coherent and coordinated defense, deterrence, mitigation, and recovery strategies. These strategies must be tied to 'best practices' to ensure that appropriate technologies, security and anti-terrorism processes, and human capital are invested wisely. Ultimately, the culmination of these efforts should result in an overall security plan that forms the bases for the "Deter and Detect (prevention) and Respond and Recover" activities.

Thus far, we have observed that certain aspects of rail security planning for the passenger sector are not mature and well integrated. For example, Amtrak shares space with a number of transit partners (over 20) in multi-modal stations but, with the exception of some operations and train movement protocols, the security plans of the rail partners are not all formally linked. Also, within certain facilities, not all stakeholders and facility users are fully aware of security and emergency response procedures. The overall security and risk focus appears to be very traditional in that security planning has been limited to facility ownership (and potential liability) rather than directed more broadly.

On the good news side, in many locations, there is strong information sharing between and among local operators and law enforcement on a daily basis, but these are oftentimes the result of personal relationships and networks. The strength of these relationships may change as personnel change, and we want to see stronger, more formal security networks between Amtrak and its rail and transit partners. Also promising, emergency response drills and exercises are being conducted with more regularity, and there is a growing body of 'lessons learned' from the exercises, drills, and table-tops after-action reports that will assist investment decisions and changes in operational protocols.

Information, Intelligence Sharing, & Special Security Efforts

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.

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.

During the last year, the Amtrak OIG has also placed a special emphasis on security at Washington DC's Union Station. Union Station is one of the most visited sites in the District and is a major transportation hub for Virginia and Maryland rail services as well as the anchor for Amtrak's Northeast Corridor. We have worked with Amtrak Police, local Amtrak managers, local property management, adjacent facility owners, and with transit and local police to establish a Station Action Team. This group is dedicated to sharing security and emergency preparedness information and will become a model for other major urban stations. The OIG facilitated the creation of this team, and we have prepared special security briefings that I would be happy to share with the Committee or interested Members in a closed setting.

Recommendations

Making rail security a national priority is a shared responsibility among a number of Federal departments and agencies, which also requires the full commitment of private and other public sector stakeholders.

1. **Technology Centers**

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 vendor 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 also 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, and Amtrak routinely uses TTCI services for equipment testing.

2. **"Building In" Security**

Wherever possible, there should be criteria to guide design, engineering, and procurement activity with an agreed-upon set of security standards and requirements for capital projects. There is considerable opportunity for all carriers to examine their general capital spending programs to determine where security improvements can be made.

Amtrak plans to work with international engineering standards groups to determine what other nation's inter-city rail carriers are doing to build-in security into retrofitting projects as well as new construction.

3. **Standards Development**

One of the difficulties we have encountered in evaluating Amtrak's efforts to improve its security posture is the lack of security standards. Although some security directives were prepared by DHS in May 2004, these directives are not necessarily the comprehensive bases for an effective rail passenger security strategy.

The Committee should look to 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 responsibilities and will most likely develop its own baseline and security standards, working closely with its rail and transit partners, as well as DHS.

4. **Passenger & Baggage Screening**

In testimony in March 2006, the GAO reported on the results of their evaluations of the security practices of domestic and selected foreign transit operators (www.gao.gov/new.items/d06557t.pdf). Included in their testimony were recommendations, with certain caveats, to consider implementing three practices they observed not being widely used: covert testing, random screening, and establishing a government-sponsored clearing house for technologies and best practices.

In my opinion, some level of passenger and limited baggage screening on Amtrak is inevitable, especially during times of high alert, when there is actionable intelligence, during special events, and when police and security believe such security steps add real value. Amtrak cannot go down

the path of the aviation experience, but it will have to develop criteria that are defensible, consistent with its business model, and effective.

Conclusions

There are a number of good people trying to do the 'right thing' about rail security, but these efforts are not yet well integrated into a larger transportation strategy. Our collective oars are not in the water at the same time. Through your efforts, and with the help of Amtrak's authorizing and appropriations committees, I hope we find the convergence that leads to unified approaches to formulating security plans and processes.

In a moment of decision, the best thing you can do is the right thing. The worst thing you can do is nothing. (Theodore Roosevelt)