High-Speed Rail in the US:

Will It Be a More Attractive Terror Target than Inter-city Rail?

Donna R. Maurillo

Thesis-Quality Research Project Submitted in Partial Fulfillment

of the Requirements for the Masters of Science in Transportation Management

Acknowledgments

Please allow me to express my gratitude to the many people who made this research paper possible. That includes the transportation experts who were generous enough to provide their professional insights and opinions, including Tony Daniels, Senior Vice President, Parsons Brinckerhoff and former Program Director, California High Speed Rail Authority; Paul Mosier, Senior Rail Operations Engineer, Parsons Brinckerhoff; Peter Loverso, Senior Security Specialist, Parsons Brinckerhoff; Richard Harnish, Executive Director, Midwest High Speed Rail Association; Joseph Shacter, Director, Public & Intermodal Transportation, Illinois Department of Transportation; Marc Magliari, Media Relations Manager, Amtrak; Christopher Kozub, Security Research Associate, Mineta Transportation Institute; David Morgan, Manager, Office of Fixed Guideway Safety/Security Oversight, New Jersey Department of Transportation; Bruce Wimmer, Director of Global Consulting, Pinkerton; Stephan Parker, Senior Program Officer, Transportation Research Board; Robert Melan, Security Specialist, Mass Transit, Transportation Security Administration; and T.C. Kao, Professor, University of Illinois.

Thanks also to William Medigovich, US Department of Transportation, Senior Executive Service, Ret.; Anthony Tisdale, Transit Security and Emergency Management Specialist, US Department of Transportation; and Dave Schlesinger, Training Manager, Metrolink Positive Train Control Project, Parsons for the volumes of security documents and connections to valuable contacts.

Particular gratitude goes to all of the faculty in the Master of Science in Transportation Management program, especially Peter Haas, PhD, who provided a compelling and challenging introduction to the topic issues; Frances Edwards, PhD, who made disaster management one of our most exciting courses; Daniel Goodrich, who gave his class perhaps the most interesting perspectives on security as he taught us how to "think like the bad guys;" and to Rod Diridon, Sr., for sparking my interest in high-speed rail and for encouraging me to enroll in this rewarding program.

Throughout the many months of study, Graduate Studies Manager Viviann Ferea has provided everything we students needed in terms of deadlines, applications, fellowship information, class schedules, enrollment procedures, video equipment instruction, encouragement, and plenty of good humor.

Finally, I would like also to recognize my parents, John and Mary DeLuca Maurillo, for expecting the best, valuing perseverance, and demonstrating that you are never too old for more education.

Table of Contents

List of Figures

Problem Statement

If President Barack Obama is successful, he will leave behind a legacy project that he has been passionate about – high-speed rail (HSR). This is a challenging endeavor for a president who leads a nation that is rooted in and tightly bound to its personal vehicles and the public roads on which to drive them. If successful, this completely new infrastructure could become as iconic as the interstate highway system inaugurated by his predecessor, President Dwight Eisenhower.

Already, nearly $20 billion has been set aside to bring high-speed rail into the American landscape. More than a dozen corridors have been selected as the most viable locations for the key "starter routes" that will open the door to the type of transportation network that has been long established in other parts of the world.

Japan began in 1964 with the first practical high-speed rail system, the Shinkansen, popularly known as the "bullet train." Within three years, more than 100 million passengers had used the trains, and that number reached one billion in 1976. The Shinkansen is serving not only the longer-distance traveler, but also the commuter who is no longer sitting idle in highway traffic.

By the 1970s, Europe was realizing the benefits of high-speed rail as a means to circumvent rising oil prices, as well as an effective way to minimize air pollution and traffic congestion. After building its famous TGV, France began to expand its high-speed rail network and then to connect it internationally as more European nations began to construct their own lines throughout the continent. Many of these came to maturity more than 20 or 30 years ago, while the US was still building out its highway system.

Today, China has leapfrogged ahead, building what may become the world's most innovative system – not only the trains, but also the infrastructure itself. It certainly is the world's longest system. Already, the Chinese are marketing their knowledge to other countries, including the United States. Only a few years ago, China was primarily an agricultural economy that posed little threat to American industrial leadership. Now it is poised to become a world leader in HSR.

The large, developed countries are not the only ones building high-speed rail. Many of the developing nations such as Morocco, Mexico, and Argentina are either planning or building their systems.

Meanwhile, the US highway system, once a source of pride for Americans, has become increasingly congested with vehicles as the country has fewer viable choices for commuters or short-distance travelers. The Northeast Corridor has remained the only area in the United States where people habitually commute by rail simply because it offers a workable alternative to driving or flying. Although it is heavily traveled and shared with freight lines, even that corridor would be greatly improved with a new system that would further decrease travel time while increasing comfort.

With so many high-speed rail systems coming into fruition around the globe, the US is facing increased pressure – whether internal or external – to compete with other nations or risk losing its reputation for innovation leadership. Today, China has become the world's second-largest economy, supplanting Japan. In time, it may overtake the US, usurping this nation's place as the economy against which all others are measured.

If the US succeeds in establishing such an ambitious national HSR system (and at this juncture, it still is not certain), a growing number of people may use rail as an alternative mode for short-hop travel – that is, trips of 350-400 miles. These are not cost-effective distances for airlines because of fuel inefficiencies. At the same time, these distances are sufficiently challenging for the "day tripper" or the business traveler to drive. Therefore, high-speed rail could become the mode of choice for a growing population that wishes to avoid the almost inevitable highway congestion.

Assuming, then, that high-speed rail does succeed in the US, it could become a target for domestic or global terrorist groups or individuals who specifically attack transportation modes. In that event, which security-related issues could be problematic?

Several possibilities exist. First, terrorist attacks against inter-city rail have occurred with almost predictable frequency around the globe. Crowded cars and easy access provide a ready target for anyone with evil intent. Although rail attacks may not deliver the spectacular devastation of an airline attack – such as that of September 11, 2001 – they still can provide sufficient carnage to deliver a stunning message of terror.

Second, the discovery of Osama bin Laden's trove of correspondence and terror-related documents has heightened America's sensitivity to possible attacks on its rail system. Although rail professionals and counter-terrorism experts have long recognized it, Americans are just beginning to realize that rail is much more vulnerable than the relatively closed airline system. In fact, a recent editorial in the *Peoria Journal Star* said, "It's clear that our enemies view our rail system as having some security holes. Furthermore, ridership on Amtrak continues to increase, up 10 percent so far over last year on Illinois routes for example.

"It has been said that 9-11 happened because of a failure of American imagination. We no longer have that excuse. High-speed rail investment is an Obama administration priority. Nothing would kill that concept faster than a high-profile train terrorist strike in the U.S. Passenger safety has to be a part of this discussion."[1]

Third, rail security is more difficult than airline security because it must address much larger numbers of travelers. Of necessity, screening must be brief to keep the crowds moving efficiently. This can allow lethal devices to pass through undetected into the cars. Even chemical-sniffing canines and random screening are imperfect enough to leave certain vulnerabilities in the rail system. And crowds standing in long screening lines can be vulnerable to attack, as well.

In addition, a new HSR system in the United States could become a tempting target for those who would wish to destroy any icon of Western values – especially if the nation had just invested a staggering sum of money into it. Attacking airlines is not an easy endeavor. The majority of US transportation security investment has focused on air travel, making another attack much more daunting. On the other hand, rail is so much more accessible and vulnerable not only at the stations, but also along the entire route, where derailments can be carried out in remote areas. By contrast, an airliner is reasonably safe once it has left the ground.

One also must consider that a well-placed explosive device planted on high-speed rail could be timed to coincide with that train traveling adjacent to key infrastructure, such as bridges, tunnels, water treatment plants, power stations, and the like. It also is possible to place an explosive device on an inter-city passenger train and time it to explode as the cars pass alongside a high-speed train.

And finally, because it would be a new infrastructure, high-speed rail most certainly would be operated with digital technologies throughout. These systems, while

[1] "Our View: Rail safety must be larger priority for U.S." *Peoria Star Journal*, May 13, 2011

more dependable and robust than mechanical systems on older lines, can be hacked in a way that could affect switches, warning lights, electrical circuits, and even the operating systems of the computer networks. Further, it is not difficult to purchase the means to create electronic identification badges and cards, thereby allowing a criminal to impersonate rail personnel and operate from inside the system. Many of these devices are readily available online, such as at http://idcardmaker.org/

It must be kept in mind that successful terrorist attacks are often imitated and can become part of the attackers' playbook. Past success makes future attacks more likely because the attackers would then know how to leverage a particular vulnerability.[2]

The RAND Corporation noted that in the decade between 1995 and 2005, there were almost 250 attacks against rail transportation, killing 900 people and injuring more than 6,000.[3] What is to prevent attackers from moving on to high-speed rail?

Another key issue is whether security planning has been considered while the newest part of the US transportation infrastructure has been working its way through the funding and planning phases.

Two questions will be addressed in this paper. First, the primary question is whether high-speed rail is inherently a more attractive target than inter-city rail, or whether it has only a similar or even a lesser degree of vulnerability. A secondary question is whether high-speed rail requires specialized security planning, or whether the same security strategies for inter-city rail would apply.

[2] Jenkins, Brian Michael, and Butterworth, Bruce Robert, *Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute Report CA-MTI-10-2875, March 2010

[3] United States Government Accountability Office, *PASSENGER RAIL SECURITY: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, Report to Congressional Requesters, September 2005

Methodology

For the purpose of this research paper, a great deal of literature has been collected about the status of America's planning for high-speed rail corridors, the background on attacks against surface transportation, the existing types of security in place for inter-city rail in the US and abroad, the expected trends in future attacks, and other related issues. In all, approximately 150 documents have been collected, including research reports, commentaries, news articles, statements made before US government bodies, law enforcement alerts, and other materials.

These were reviewed individually, culled for information of value to this report, and organized into an Excel spreadsheet that included easily-referenced columns for document titles, originating sources (i.e., newspaper, government agency, etc.), author, date, and URL (if any).

Some of these materials, especially those related to law enforcement alerts or other security-sensitive resources, have been designated as unclassified but for official use only (U/FOUO). Access has been given to this researcher by security sources with the understanding that any U/FOUO information made available to the public will be used only in aggregate. In any instances where U/FOUO documents have been quoted or made identifiable in this report, they have been identified as such.

Research Intent and Final Design

The original research intent was to collect both quantitative and qualitative data. The quantitative data would have been obtained by using rating scales to measure security planning time lines and the scaled importance of certain security elements and tools. However, the literature collection and early conversations with security professionals strongly indicated that these types of time lines and metrics do not yet exist, even in a rudimentary way. Therefore, a subsequent determination was made that it would be quite unlikely that any consistently measurable data could be collected at this early date.

Rather, the report focuses instead on qualitative information obtained by way of telephone and face-to-face interviews with professionals who have expertise in security for rail, transit, or the nation. These interviews first addressed the key questions listed at the end of the Problem Statement above. (A list of actual questions is included in Appendix B.) In addition, some guided discussion was included because each of the interview subjects was expected to have unique viewpoints due to their positions within agencies such as the US Department of Homeland Security, the US Department of Transportation, the Transportation Research Board, or the HSR corridors.

For example, any specific questions about the timing of security planning in a particular HSR corridor would not be applicable to an interviewee from the Transportation Research Board. This became apparent during preliminary interviews when some questions were deemed irrelevant to each interviewee’s particular role. Therefore, the primary questions (i.e., whether HSR is more vulnerable and whether it would require specialized security measures) were broad enough to be appropriate for all interview subjects, while some of the probing questions were tailored to address that interviewee’s particular expertise as it related to HSR security.

Additionally, the interviewed HSR and security officials did not have any consistency in job titles or responsibilities because each of the rail corridors is at a different point in its planning process, and not all the relevant organizations have the same type of management structure.

However, in all cases, questions were kept in the same general track. In most instances, after the prepared questions were asked, the conversation also moved into areas of specialization for that particular interview subject so this report could have a broad picture of security planning for rail modes.

Each interview closed with a standard question: "Is there anything you would like to discuss that I have not asked about?" This allowed the interview subject to bring up issues that may have been overlooked but that could add value to the report.

In the course of interviewing, it also became apparent that the corridors identified as "high-speed rail" in various corridor maps were in fact only incremental upgrades. This finding further narrowed the scope of the research, leaving only the Florida, Texas and California corridors qualifying for the "high-speed rail" parameters of this report. The research was further challenged when the governor of Florida turned back federal funding for the first phase of HSR construction in that state, putting the project on hold at least for the foreseeable future. Texas was later determined to be much too early in its project planning (in fact, it is only in the research phase) to have made any notable security considerations. This series of discoveries and events, which occurred during the course of research, left only California as a qualifying rail corridor.

The research design considered comparing US planning with that of other countries such as France and Japan in order to establish planning benchmarks. However, during the course of research, it was discovered that information from those foreign systems is not yet readily available in a way that could be used in this report. However, it will be available within a year or two when the Mineta Transportation Institute (MTI) completes a related security research project.

The research project also was expected to acquire and analyze at least some quantifiable data domestically, even with the paucity of metrics due to the newness of HSR in the US. At the very least, the report was expected to present a planning chronology from each corridor on which to base benchmarks or best practices. However, as noted above, it became evident that only California qualified for inclusion. Comparing quantifiable data became impossible with only one available sample.

It follows that most of the report's usable information has come primarily from the literature review and, secondarily, from interviews with security experts outside the HSR system. Indeed, it will require several years to build out many true HSR systems, so the long-term planning priorities may be focused primarily on obtaining funding, rights of way, and citizen support. At the very least, the findings from this paper may well lay the groundwork for a future research project.

With all these factors taken into consideration, this report will offer a broad look at high-speed rail security issues as noted in the questions above and then focus on general recommendations.

This research paper was especially challenging because it is "bleeding edge," with little existing directly-related data. Some conclusions regarding high-speed rail security planning and implementation had to be drawn from early qualitative information, with the recommendations based upon that and the rather limited hard data. Even so, this research project offers a reasonable place to begin if the US is to establish a process for uniform HSR security planning, policies, and best practices.

Interview Subjects

HSR corridor representatives who were contacted included:

- *The California Corridor:* Telephone interviews were conducted with Tony Daniels, Senior Vice President, Parsons Brinckerhoff and former Program Director, California High Speed Rail Authority; Paul Mosier, Senior Rail Operations Engineer, Parsons Brinckerhoff; and Peter Loverso, Senior Security Specialist, Parsons Brinckerhoff. California has one of the most advanced HSR planning organizations, with staff and a board of directors tasked with shepherding the state's plans through the planning, approval and construction process, and perhaps even into the operational phases. The California High Speed Rail Authority is currently developing a security threat analysis that will be leveraged to help formulate HSR security policy.
- *The Midwest Corridor:* Telephone interviews were conducted with Richard Harnish, Executive Director, Midwest High Speed Rail Association, and with Joseph Shacter, Director, Public & Intermodal Transportation, Illinois Department of Transportation. It was determined that they did not have the necessary oversight to provide usable information for this report. Mr. Shacter made a referral to Marc Magliari, Media Relations Manager, Amtrak, noting that he would be the most qualified to discuss the Midwest rail project. During a subsequent telephone interview, Mr. Magliari reported that none of the Amtrak corridors were true HSR at this time, and that none would reach that status until at least 2040 or later. The Midwest Corridor also has seen two states opt

out of participating – Ohio and Wisconsin – even given that this corridor includes only incremental upgrades. This loss of two states most likely will not affect the remainder of the system because it extends into a number of other states, with Chicago as its epicenter.

- *Northeast Corridor:* As noted above, contact was made with Marc Magliari, Media Relations Manager, Amtrak, who said that this corridor is not actively engaged in true HSR at the moment, although it is part of the company's long-term plans. This most heavily traveled of all the US rail corridors has a well-established ridership between Boston and Washington DC, including New York City and Philadelphia. It will include a combination of incremental upgrade and true high-speed rail, although the latter is not imminent. Attempts were unsuccessful to make contact with Al Engel, Vice President of HSR for Amtrak.

- *Texas T-Bone Corridor:* A true HSR corridor, this is in preliminary stages of research and planning and was determined to be inappropriate for purposes of this report.

- *Other HSR corridors:* The remaining corridors – such as the Empire (New York State), Keystone (Pennsylvania), Gulf Coast, Southeastern, Northwest, and others – are currently planning for incremental upgrades. Therefore, they did not meet the qualifications for this report.

Other experts who were interviewed included:

- *Mineta Transportation Institute:* Two telephone interviews with Christopher Kozub, Security Research Associate.

- *New Jersey Dept. of Transportation:* Telephone interview with David Morgan, Manager, Office of Fixed Guideway Safety/Security Oversight;

- *Pinkerton:* In-person discussion and seminar participation with Bruce Wimmer, Director of Global Consulting
- *Transportation Research Board:* Telephone interview with Stephan Parker, Senior Program Officer;
- *Transportation Security Administration:* Telephone interview with Robert Melan, Security Specialist, Mass Transit;
- *University of Illinois:* Obtained limited email and in-person information from T. C. Kao, Professor with deep experience in Taiwan's high-speed rail system;

Attempts to interview other experts were unsuccessful. These include

- *American Railway Engineering and Maintenance-of-Way Association:* Tom Farmer (attempted, no response)
- *Amtrak:* Al Engel, Vice President, HSR (attempted, no response)
- *Association of American Railroads:* Tom Farmer, Assistant Vice President of Security (attempted, no response – same contact as above; represents both organizations)
- *Federal Railroad Administration:* (No response to request for referral)
- *Federal Railroad Administration:* David Valenstein, Environmental Program Manager (attempted, no response)
- *Federal Railroad Administration:* Michael Lestingi, Office of Policy (attempted, no response)
- *Florida Department of Transportation:* Nazih Haddad, Chief Operating Officer (attempted, no response)

- *RAND Corporation:* JayEtta Hecker, former Adviser, GAO, Bi-Partisan Policy Organization (contacted; no longer involved, however, this report does include several quotes from her previous testimony)

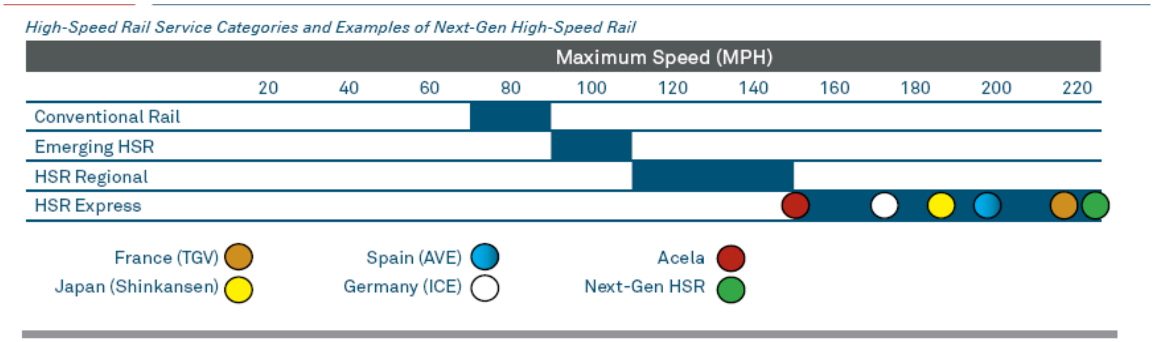
Interview responses were categorized according to topic and amalgamated with information from the literature to create a more complete view of the direction in which HSR security planning most likely is moving.

Findings

To fully understand the issues under investigation in this report, it is first necessary to understand the definition of high-speed rail in the US.

While there is no universal agreement about the exact parameters of high-speed rail, it is generally defined as a system that supports speeds of 150-220 mph, although those speeds can reach 250 mph and more. (See Figure 1.) These velocities necessitate completely smooth electrified “ribbon” tracks, without the noisy joints of traditional inter-city rail, making the operation significantly quieter. The rolling stock itself is also different because it is designed to withstand impact and to reduce derailments.

Figure 1 – Speed Comparisons for Various Rail Categories



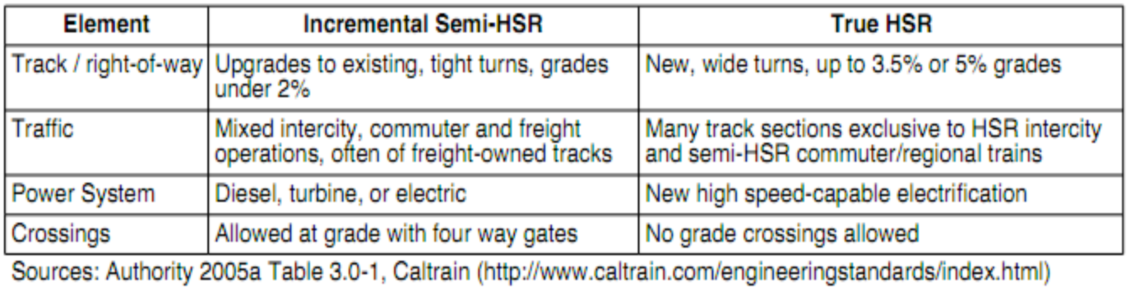
Source: Amtrak

Another difference is the way the track ballast is designed. This is typically crushed stone that railroad ties are laid upon. It helps stabilize the ties, allow drainage, and prevent vegetation from growing around the rails. Because of the increased speed of HSR, this crushed stone can be "kicked up" as the trains travel along the tracks. This requires HSR ballast to be formed from concrete, often in pre-cast sections that can be assembled at the rail site.

In the US, this new system will be integrated into designated corridors, along with "incremental upgrades" or "higher-speed rail." These are existing tracks that will be improved to support traditional rolling stock operating at speeds of 110-150 mph. (See Figure 2.) Currently, Amtrak's Acela line operating between Boston and Washington DC falls into this category, although only in limited sections of the corridor. Traditional inter-city rail will continue to operate at approximately 75 mph, although it sometimes operates at slower speeds because it must share tracks with freight rail. Because freight companies own most of the US rails, passenger trains are frequently moved aside and delayed.

Note that, although "true HSR" eventually will be integrated into these corridors, the new seamless "ribbon tracks" will be used exclusively by HSR train sets because of weight and other factors that make other train sets unsuitable for these rails, including freight and inter-city passenger. This will be another factor making high-speed trains more efficient. HSR trains, however, may use traditional rails when necessary to access stations.

Figure 2: Incremental vs. True HSR



Element	Incremental Semi-HSR	True HSR
Track / right-of-way	Upgrades to existing, tight turns, grades under 2%	New, wide turns, up to 3.5% or 5% grades
Traffic	Mixed intercity, commuter and freight operations, often of freight-owned tracks	Many track sections exclusive to HSR intercity and semi-HSR commuter/regional trains
Power System	Diesel, turbine, or electric	New high speed-capable electrification
Crossings	Allowed at grade with four way gates	No grade crossings allowed

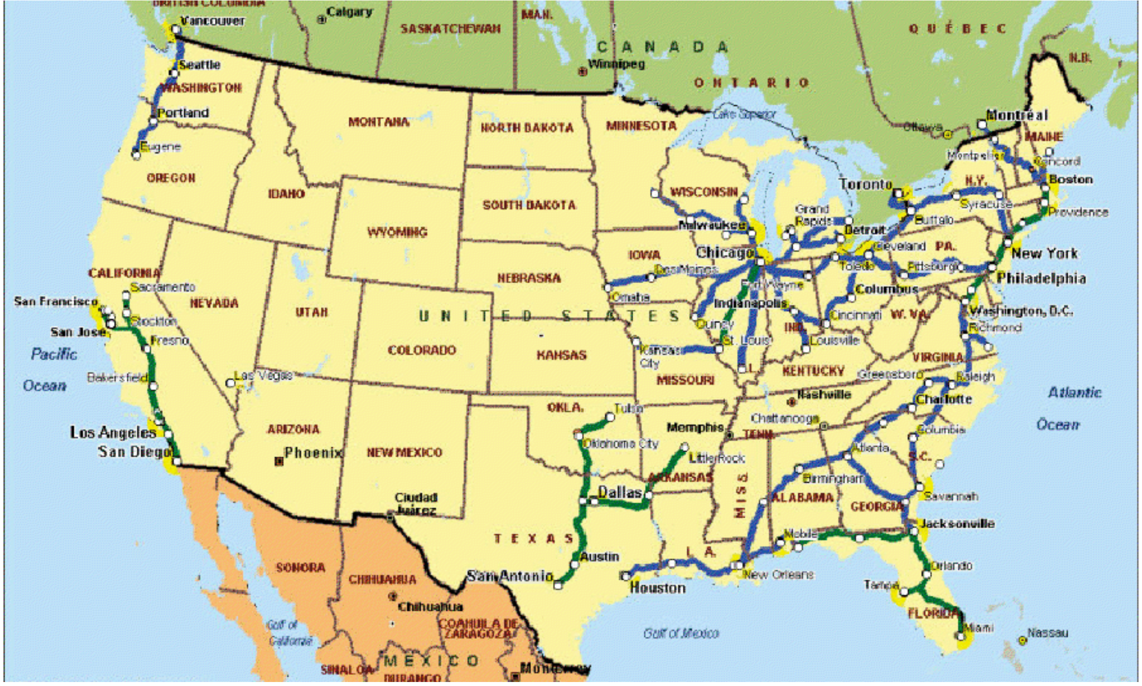
Sources: Authority 2005a Table 3.0-1, Caltrain (http://www.caltrain.com/engineeringstandards/index.html)

Several high-speed rail corridors have been designated for the US, although nearly all of them will include some or all incremental upgrades at build-out. (See Figure 3.) These corridors include:

- California Corridor – entirely HSR
- Chicago Hub Network – some HSR, some upgrade
- Empire Corridor (New York State) – entirely upgrade
- Florida Corridor – entirely HSR
- Gulf Coast Corridor – entirely upgrade
- Keystone Corridor (Pennsylvania) – entirely upgrade
- Northeast Corridor (primarily Amtrak Acela) – some upgrade, some HSR
- Northern New England Corridor – entirely upgrade
- Pacific Northwest Corridor – entirely HSR
- South Central Corridor (aka "Texas T-Bone") – entirely HSR
- Southeast Corridor – entirely upgrade

Figure 3: US High-Speed Rail Corridor Map

Green = True high-speed rail   Blue = Incremental upgrades



Of the more than 150 documents identified for this study, including news articles, commentary, research reports, blog articles, white papers, and other materials, most relate to rail security in general and only a few to HSR security in particular. However, none of the HSR documents include security policies related specifically to that mode. Rather, it appears that HSR policies are expected to mirror those of inter-city passenger rail, although this is not specifically spelled out.

An FAQ from the Florida High Speed Rail web site does state that, although HSR system security standards have not been created, "…they are likely to include some common features from systems in existence in other places. One major component is intrusion detection into the HSR right-of-way. The HSR system will be fully barrier protected both along the corridor and from overhead structures to prevent intrusion of any kind. The stations will have security as well, although not nearly as onerous or lengthy as at airports. Video surveillance will likely be provided both on trains and in stations."[4]

This pedestrian approach leads one to question whether experts believe that HSR has any particular attraction for terrorists, vandals, or "one-off" attackers. In a telephone interview[5] with David Morgan, Manager of the Office of Fixed Guideway Safety and Security Oversight at the New Jersey Department of Transportation, he stated, "HSR as a whole is not necessarily more vulnerable than other rail services. Transit in general is vulnerable. Look at it worldwide. [Terrorists] like to hit trains because there are so many passengers. In Madrid alone, they hit 11 targets in seven minutes… High-speed rail is vulnerable just because it's public transit, not because it goes fast."

In at least one other sense, HSR is less vulnerable because the trains are built to remain connected and "in line" – they do not "accordion" during a derailing or other incidents. As an example, Christopher Kozub, a security research associate for the Mineta Transportation Institute, noted that a German HSR train hit a flock of sheep in a tunnel. It derailed but remained upright, with only a few passengers sustaining injuries.

He said, "A non-HSR train would have many more casualties because they aren't built to withstand this type of crash. The design and construction standards for HSR make it less attractive for terrorists if they are looking for a high body count or a spectacular crash scene."[6]

Peter Loverso, Senior Security Specialist with Parsons Brinckerhoff, is currently planning security for the California high-speed rail project. He stated that HSR is more

[4] www.floridahighspeedrail.org/faqs: On the Track: Train Details > Will there be security on the trains and at the stations?
[5] Telephone interview, January 11, 2011
[6] Telephone interview, March 10, 2011

vulnerable in some ways and more secure in others. “When a train travels at more than 200 miles per hour, there is much less time to react to emergencies. Even with a good warning system, a high-speed train needs quite a distance to stop. That gives it a certain amount of vulnerability. On the other hand, high-speed rail will attract a higher-end clientele that will have to make reservations and go through a screening process. That offers more protection than inter-city rail,” he said. [7]

Others, such as *Politico* columnist Josh Gerstein, agree that there is a definite vulnerability. He wrote, “During a town hall meeting in Tampa today, President Barack Obama touted, as one of the benefits of high-speed rail that passengers wouldn't have to go through a security check that requires taking off their shoes... His remark got me wondering why rail security is so much more lax than airport security. And given that Obama was announcing that the federal government plans is [sic] awarding $8 billion in stimulus money for the planning and construction of high speed rail projects, wouldn't it be unwise to allow an Al Qaeda operative to blow up a chunk of that investment?” [8]

He goes on to say that it’s true that terrorists seem focused on blowing up passenger planes, but anything high-profile can be a target. Any attack that would derail a train traveling more than 200 miles an hour wouldn’t be pretty, he wrote.

Journalist Michael Scott Moore harbors a few concerns, as well. He wrote, “Simplicity is the best part of rail travel, and President Obama likes to say that American high-speed trains will involve no shoe checks. But Obama has his critics, and an

[7] Telephone interview, April 1, 2011

[8] Gerstein, Josh, *Obama: No shoe checks on high-speed rail*, Politico, January 28, 2010

expensive new high-speed line might look as tempting to an expansionist Transportation Safety Authority as to terrorists. So the question is worth some thought."[9]

Some experts also agree that HSR has special vulnerabilities. Jenkins, Butterworth, and Clair (March 2010) say that, "In addition to the publicity, body count, and disruption sought by today's terrorists, high-speed rail is an icon of technological progress, thus adding the emotional value that terrorists seek in their targets. For these reasons, the attempted derailment [of the French TGV], although fortunately a failure for the terrorists, takes on particular significance."[10]

Therefore, it would appear that HSR could have real value as a target, especially as groups such as al Qaida continue to reach into the US to attract and train homegrown "lone wolf" terrorists – especially those who blend well with the local population – in its quest to attack Western cultural and economic symbols.[11]

So, while it is entirely possible – and perhaps even probable – that terrorists or anyone else with a degree of malicious intent could attack HSR in some way, is it necessary to implement specialized security planning and policies that go beyond those of inter-city rail? To answer that question, first we must examine the pattern of threats and incidents worldwide, and then we must determine what types of security policies and practices are already in place to address them. Next, we must assess whether HSR brings into play any specialized conditions that may require particular types of security unique to this mode. And finally, we must recommend the means to secure that asset.

[9] Moore, Michael Scott, *High-Speed Rail's Weak Link Is Security*, Miller-McCune, May 4, 2011

[10] Jenkins, Brian Michael; Butterworth, Bruce R.; Clair, Jean-François; *Off the Rails: The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts*, Mineta Transportation Institute report CA-MTI-10-2501 , March 2010

[11] Bergen, Peter, and Hoffman, Bruce, *Assessing The Terrorist Threat: A Report Of The Bipartisan Policy Center's National Security Preparedness Group*, Bipartisan Policy Center, September 10, 2010

Patterns of Threats and Attacks

Around the globe, the favored tactic is for attackers to place IEDs inside baggage holds, passenger compartments, stations, or inside the track bed under the rails. These devices can be homemade, military grade, or commercial. All are entirely viable and effective, although none has been used recently in the US. [12]

The RAND Corporation analyzed threats to passenger rail systems (Wilson et al., 2007) and noted that "there is a high threat of attacks using small explosives; a medium threat of attacks using large explosives, small incendiary devices, or other weapons, sabotage, and hoaxes; and a low threat of attacks using large incendiaries and unconventional weapons. We assume that these threats apply to both rail freight and passenger rail, though the vast majority of recorded attacks have been against passenger systems."[13]

Jenkins, Butterworth, and Clair (March 2010) note that bombs were employed in 131 of the 181 events (72.4 percent) in the Mineta Transportation Institute's database on terrorist attacks on rail. They suspect track bombs in another 18 cases (9.9 percent), for a total of 82.3 percent of the derailments. Mechanical sabotage occurred in 21 cases (11.6 percent) and was suspected in six cases, for a total of 27 cases (14.9 percent). In five incidents, other sabotage methods were used.[14]

[12] Office of Intelligence and Analysis Assessment, *Threat Assessment: Mass Transit and Passenger Railroads*, June 29, 2010

[13] Ortiz, David S.; Weatherford, Brian A.; Greenberg, Michael D.; Ecola, Liisa [sic], *Improving the Safety and Security of Freight and Passenger Rail in Pennsylvania*, RAND Corporation, 2008

[14] Jenkins, Brian Michael; Butterworth, Bruce R.; Clair, Jean-François, *Off the Rails: The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts*, Mineta Transportation Institute report CA-MTI-10-2501, March 2010

In the same report, the authors noted that, while the number of incidents is small, terrorists achieve higher body counts per attack when they use mechanical means, such as removing bolts or track, than by using bombs.[15]

But that is not to say that methods are predictable and stable. The recent high-profile attacks in Mumbai targeted passengers at the station, as a two-man team sprayed bullets at the crowd, simply trying for as much slaughter as possible.[16] These deaths accounted for one-third of the total, with many others at the high-profile Taj Mahal Hotel. Predictably, as attack techniques prove to be successful, they become part of a growing manual for others to follow, shortening the planning cycle.[17] In turn, this compels security professionals to create new and better methods to harden those targets. The ideal plan is to anticipate every conceivable terrorist plot and to build a bullet-proof security system. Not only is that impractical, it's also impossible.

Jenkins and Butterworth (March 2010) also note "that terrorists are opportunists and are far more likely to attempt attacks that will, with high confidence, achieve a death toll of 25 to 50 than a risky, complicated operation that could kill 1,000 or more."[18]

Unlike airports, passenger rail systems are difficult to secure because they are much more open to the public, leaving them highly vulnerable because security personnel can't possibly monitor every person, package, or activity no matter how sophisticated the screening devices. Rail systems also are difficult to secure because the schedules are

[15] Ibid

[16] RAND Corporation, *Terrorists Can Think Strategically: Lessons Learned From the Mumbai Attacks*, Testimony presented before the Senate Homeland Security and Governmental Affairs Committee, January 28, 2009

[17] Jenkins, Brian Michael, and Butterworth, Bruce Robert, *Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute Report CA-MTI-10-2875, March 2010

[18] Ibid

usually consistent and widely publicized, and the stations have many uncontrolled access points.

These systems become especially attractive because of the expensive equipment and facilities, the large number of potential victims, typical location in dense urban areas, and the economic importance. Balancing the cost versus the payback is probably one of the most difficult challenges for security professionals.[19]

Another type of attack – the cyber attack – does not necessarily create high body counts, but that depends on the type of attack. Because it can disable or harm positive train control (PTC) and other digitally-based systems, a cyber attack certainly must be considered as a potential killing tool. Derailing and other disasters can be staged simply by hacking into the digital systems or introducing powerful malware. The recent Stuxnet virus, for example, was so elegantly designed that it was able to attack industrial systems and, according to Iranian officials, even enter computers of its nuclear project workers.[20]

However, not all hacking is aimed directly at the rail system itself. Some of it is directed toward identity theft as a means to impersonate operational staff, security officers, and others who have access to the systems' control rooms, restricted areas, train yards, tracks, and other non-public areas. It has become relatively simple to counterfeit the digital ID cards and badges that operators have come to trust as innately secure.[21]

(U/FOUO) According to a Metropolitan Transportation Authority briefing, identification fraud is a growing concern, with up to 10 million occurrences each year

[19] United States Government Accountability Office, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, Report to Congressional Requesters, September 2005

[20] Markoff, John, *A Silent Attack, but Not a Subtle One*, New York Times, September 27, 2010

[21] Wimmer, Bruce, Pinkerton Security, speaking at "The Insider Threat & Business Espionage in the 21st Century," San Mateo CA, March 10, 2011

globally. And the technologies are becoming more sophisticated, even to the point of counterfeiting holograms, UV microtext, and other features that were created to provide extremely secure documents. Now the counterfeit IDs can read perfectly in scanners.

(U/FOUO) The briefing notes, "These advances are especially alarming when we consider that terrorists rely on anonymity and readily use fraudulent travel documents to meet, plan, train, and carry out their attacks."[22]

Terrorists also engage in online searches to find information about "government personnel, officers, important personalities, and all matters related to them (residence, work place, times of leaving and returning, and children, places visited)."[23]

(U/FOUO) Even today, security reports are ripe with examples of trespassers in train yards, suspicious characters taking photos or videos of tracks and security devices, security badge deliveries that do not arrive, stolen transit keys, rumored al Qaida threats, and other incidents that may or may not add up to malicious intent.[24]

This is not to say that the threats are unknown in the halls of federal policy. Because al Qaeda and other terror groups have had spectacular success with passenger rail attacks in Europe and Asia, US lawmakers have long asked whether passenger rail security has been sufficiently addressed at home. This has become an especially vexing question following the high-profile attacks in London, Madrid, Mumbai, and Moscow.[25]

Although John S. Pistole, Administrator for the Transportation Security Administration (TSA) testified in his confirmation hearings that he would analyze

[22] Metropolitan Transportation Authority Police Department Daily Briefing, "Technological Advances on Fraudulent Identification Cards," March 2, 2011

[23] *Safe Social Networking*, www.ioss.gov, no date given

[24] New Jersey Common Operating Picture (NJ COP), New Jersey Regional Operations Intelligence Center, February 22, 2011, Prepared by the NJ ROIC Analysis Element, Threat Analysis Program AE201102-200

[25] McCarter, Mickey, "Homeland Security to launch rail security campaign," HSToday.com, June 30, 2010

whether TSA was positioning sufficient resources to protect passenger rail, the Government Accountability Office (GAO) reported as recently as June 2010 to Rep. John Mica (R-Fla), then ranking member of the House Committee on Transportation and Infrastructure, that TSA so far has all but abandoned its efforts to conduct those assessments.[26]

This is puzzling, given the continued reality of al-Qaida's and other terrorists' threats – and successful attacks – against transportation. (U/FOUO) While the Transportation Security Administration's Office of Inspection (TSA-OI) assesses "with moderate confidence" that the risk of an attack to the US freight rail industry is low, it also assesses "with high confidence" that passenger trains or stations are more likely to be targeted than freight trains.

(U/FOUO) In an intelligence report dated February 28, 2011, TSA-OI "judges that al-Qa'ida (AQ), its affiliates, and other terrorists motivated by violent extremist views would be the most likely actors to target the U.S. freight rail system. This judgment is based on recent attacks against freight rail and passenger trains overseas and the recent stated goals of al-Qa'ida's senior leadership to attack U.S. transportation."

(U/FOUO) The report also noted that "improvised explosive devices (IEDs) would be the most likely means of attack against the U.S. freight rail system." And while there is little evidence of a terrorist threat to industrial control systems for rail, the report says that "al-Qa'ida and other violent extremist groups have a sustained interest in acquiring the skills to conduct cyber attacks."[27]

[26] Ibid

[27] Transportation Security Administration, Office of Intelligence, *Freight Rail Threat Assessment, MTA-83409-(UFOUO)*, February 28, 2011

(U/FOUO) Those assessments proved accurate immediately following the killing of terror mastermind Osama bin Laden. Among the documents taken from his fortress were those that revealed an alleged plan to attack US rail transport on September 11, 2011, the tenth anniversary of the attacks on the World Trade Center.

(U/FOUO) According to an FBI and DHS Joint Intelligence Bulletin, "As one option, al-Qa'ida was looking at the possibility of tipping a train by tampering with the rails so that the train would fall off the track at either a valley or a bridge."[28]

And yet, just one week after those potential plans were revealed, two security breaches were successfully carried out on the New York subway system. According to the *New York Post*, "Two terrifying rail security breaches occurred within hours of each other in the city yesterday – including one at the World Trade Center, where a man slipped into the PATH tunnel and walked all the way to Jersey before saying he had left a bomb in the tunnel.

"That scare – and an unrelated escapade involving four 'urban explorers' infiltrating the under-construction Second Avenue Subway tunnel – come just days after the feds warned that al Qaeda could be targeting US trains." [29]

Particular Vulnerabilities in US Passenger Rail

Several transit and passenger rail security shortcomings were noted in "Detour Ahead: Critical Vulnerabilities in America's Rail and Mass Transit Security Programs," a report on transit and passenger rail vulnerabilities submitted to the US House Committee

[28] Federal Bureau of Investigation and Department of Homeland Security Joint Intelligence Bulletin, *Early 2010 Al-Qa'ida Interest in Targeting Trains on 11 September 2011*, May 5, 2011

[29] Celona, Larry; Messing, Philip; Doyle, John – "Two tunnel security breaches cause scare in city." *New York Post*, May 9, 2011

on Homeland Security.[30] One of the first items listed was a lack of information sharing among federal authorities, state governments, municipalities, and even the rail and transit operators.

Another shortcoming listed in the report was the piecemeal approach to security taken by the federal government, rather than creating an overarching transportation security strategy. A third was the failure of TSA to give as much attention to passenger rail as it has given to airlines. Instead, according to the report, the agency has continued to make excuses, saying that this kind of security is a shared responsibility among federal, state, and local partners.

The report also notes several other vulnerabilities, including “a disturbing lack of security” around rail yards; ongoing vandalism of rail cars, demonstrating the ease with which they can be accessed; the growing threat of cyber attacks, such as the attack on CSX in Jacksonville FL; the openness of the 300,000 miles of U.S. freight rail lines and more than 10,000 miles of commuter and urban rail system lines; the high number of passengers, such as the 306,000 daily passengers using the San Francisco BART System and the 500,000 passenger trips each day on the Chicago Transit Authority’s rail system; the lack of federal funding to help state and local governments provide rail and transit security; and several other shortcomings.[31]

Undoubtedly, these types of concerns would raise many red flags, and certainly a public outcry, if they were to occur in and around the nation’s air transportation network. Why are they not given the same consideration when it comes to the much more vulnerable rail transportation system?

[30] Report to the Democratic Staff of the Committee on Homeland Security, *Detour Ahead: Critical Vulnerabilities in America's Rail and Mass Transit Security Programs*, June 2006
[31] Ibid

With the recent killing of Osama bin Laden, rail security has suddenly become a priority, given his purported plan to attack US rail. In a May 6, 2011 news release from the office of US Senator Frank R. Lautenberg (D-NJ), Chairman of the Senate Commerce Subcommittee on Surface Transportation, he said, “The documents seized at Osama bin Laden’s compound are a wake up call for America. When it comes to threats to our national security, trains are a prime target and must be better secured. Terrorists have attacked rail systems around the world and we’ve seen the devastating consequences in Moscow, Madrid, London and Mumbai. Now we have a handwritten note from Osama bin Laden’s compound targeting rail systems in the United States. We need to stop cutting security funding for our surface transportation network, and get to work protecting our railways from real threats.”

He further noted, “The risk is enormous. On any given day, more than 70,000 people ride Amtrak, 450,000 people board New Jersey Transit, and eight million ride the New York City subway system. Imagine what it would mean if a terrorist managed to carry out an attack on one of these systems. We must be vigilant to prevent potential terrorist attacks from becoming a reality.”[32]

Why the sudden alarm from those who should have been aware of industry warnings? Perhaps a look at the current state of rail security would shed some light.

US Passenger Rail Security Policies and Regulations

According to Train Law Blog, every railroad is required to “immediately report potential threats and significant security concerns to the Department of Homeland

[32] Lautenberg, Frank R., US Senator, D-NJ, news release “Lautenberg Calls Bin Laden Documents Targeting Rail A ‘Wake Up Call,’” May 6, 2011

Security Freedom Center at 703-563-3240 or 1-877-456-8722." These include any evidence of rail car tampering, threatening letters received by rail companies, any suspicious items that disrupt rail operations, any interference with rail crews, and several other activities and concerns.[33]

The US Department of Homeland Security (DHS) also lays out its own rules and requirements for rail operators, including designating a Rail Security Coordinator who is available 24/7. Its rationale listed several reasons for this rule: "With respect to passenger rail, TSA recognizes that passenger railroad carriers, commuter operations, and subway systems are high consequence targets in terms of potential loss of life and economic disruption. They carry large numbers of people in a confined environment, offer the opportunity for specific populations to be targeted at particular destinations, and often have stations located below or adjacent to high profile government buildings, major office complexes, and iconic structures. Terrorist bombings since 1995 highlight the need for improved government access to, and monitoring of, transportation of passengers by rail. Terrorists have attacked the Tokyo subway system (1995); areas in and around the Moscow subway system (2000, 2001, and 2004); Madrid commuter trains (2004); the London Underground system (2005); and the train system in Mumbai (formerly known as Bombay), India (2006)."[34]

Despite this stated acknowledgement that TSA regards rail lines as "high consequence targets," the agency's budget does not support that claim. The San Diego

[33] Goetsch, Charlie, "New Regulations For Railroad Security To Kick In, *Train Law Blog*, February 17, 2009

[34] Department of Homeland Security, Transportation Security Administration, 49 CFR Parts 1520 and 1580 [Docket No. TSA-2006-26514; Amendment Nos. 1520-5, 1580-(New)] RIN 1652-AA51, Rail Transportation Security

Law Enforcement Center, which cited the U.S. Department of Homeland Security's *FY 2011 Budget in Brief*, said:

(U/FOUO) "Since its creation, TSA has spent the bulk of its budget, which is now over $8 billion, on airline security programs. In FY2011, for example, TSA budgeted $5.56 billion for aviation security. Only $1.4 billion was budgeted for surface transportation security, which includes rail, mass transit, highway, and pipelines."[35]

Further, a visit to the TSA web site (www.tsa.gov) revealed little or no focus on securing passengers, stations, or any other facet of rail transport. These findings fell in line with the criticisms listed above in the report, *Detour Ahead*.

For example, the TSA site includes a menu link for "Travelers." However, every page under that category – and there are many – is related only to air travel. The site does have a page for railroad security information, but it is exceedingly difficult to find because it is not listed under the "Travelers" information menu. If a traveler wishes to find rail security information and enters "rail travel" into the search bar, the search results would be confusing to all but the more experienced online user. (See Figure 4.) Only if the traveler enters "railroads" into the search bar will the desired destination – information for rail travelers -- be placed at the top of the search results list.

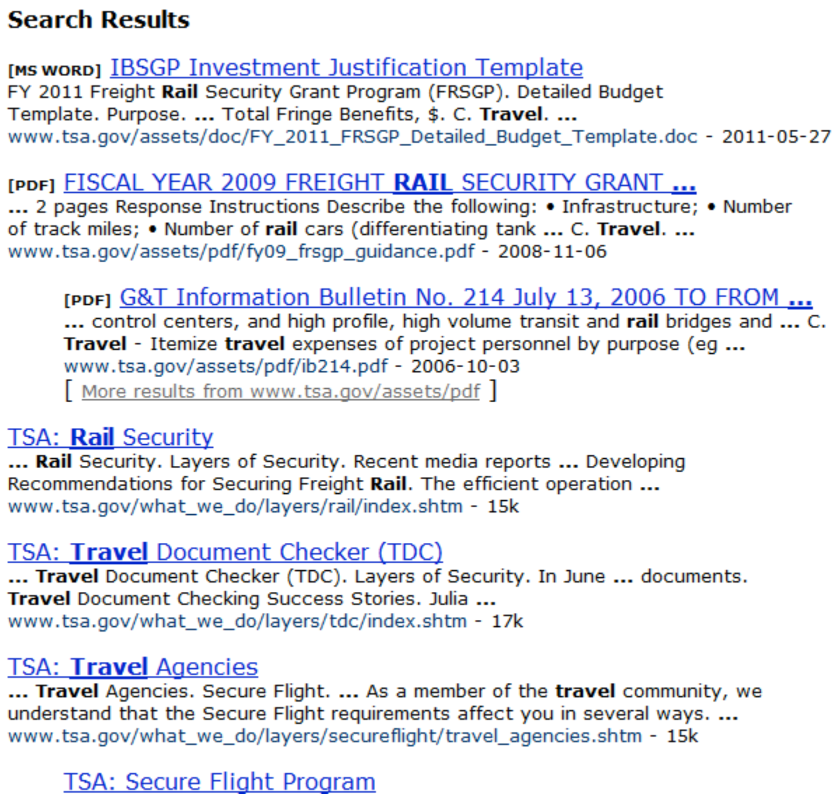
When the user does manage to reach the desired page for rail travel (see Figure 5), it offers almost no information of consequence. In fact, the links on that page lead to a second page that says the desired page cannot be found (see Figure 6). The links on that second page do not offer rail security information; rather, they return the user to the airline security pages.

[35] *San Diego - Law Enforcement Coordination Center Intelligence Bulletin 11-009*, May 4, 2011

The one link that does operate properly on TSA's railroad page – Security Awareness – takes the user only to a list of local mass transit systems. In fact, TSA's entire scope of rail security information is limited to mass transit, and even with that, the local and regional jurisdictions are left to create and enforce their own security policies.[36]

Can it be safely assumed that TSA's nearly exclusive focus lies with airline security rather than including anything more than rudimentary railroad security? Further, if TSA is tasked with maintaining "transportation security" as a whole, why does it channel the bulk of its attention to aviation when far more passengers travel by surface modes?

Figure 4: Top search results for "Rail Travel" on TSA web site



Search Results

[MS WORD] IBSGP Investment Justification Template
FY 2011 Freight **Rail** Security Grant Program (FRSGP). Detailed Budget Template. Purpose. ... Total Fringe Benefits, $. C. **Travel**. ...
www.tsa.gov/assets/doc/FY_2011_FRSGP_Detailed_Budget_Template.doc - 2011-05-27

[PDF] FISCAL YEAR 2009 FREIGHT **RAIL** SECURITY GRANT ...
... 2 pages Response Instructions Describe the following: • Infrastructure; • Number of track miles; • Number of **rail** cars (differentiating tank ... C. **Travel**. ...
www.tsa.gov/assets/pdf/fy09_frsgp_guidance.pdf - 2008-11-06

[PDF] G&T Information Bulletin No. 214 July 13, 2006 TO FROM ...
... control centers, and high profile, high volume transit and **rail** bridges and ... C. **Travel** - Itemize **travel** expenses of project personnel by purpose (eg ...
www.tsa.gov/assets/pdf/ib214.pdf - 2006-10-03
[More results from www.tsa.gov/assets/pdf]

TSA: **Rail** Security
... **Rail** Security. Layers of Security. Recent media reports ... Developing Recommendations for Securing Freight **Rail**. The efficient operation ...
www.tsa.gov/what_we_do/layers/rail/index.shtm - 15k

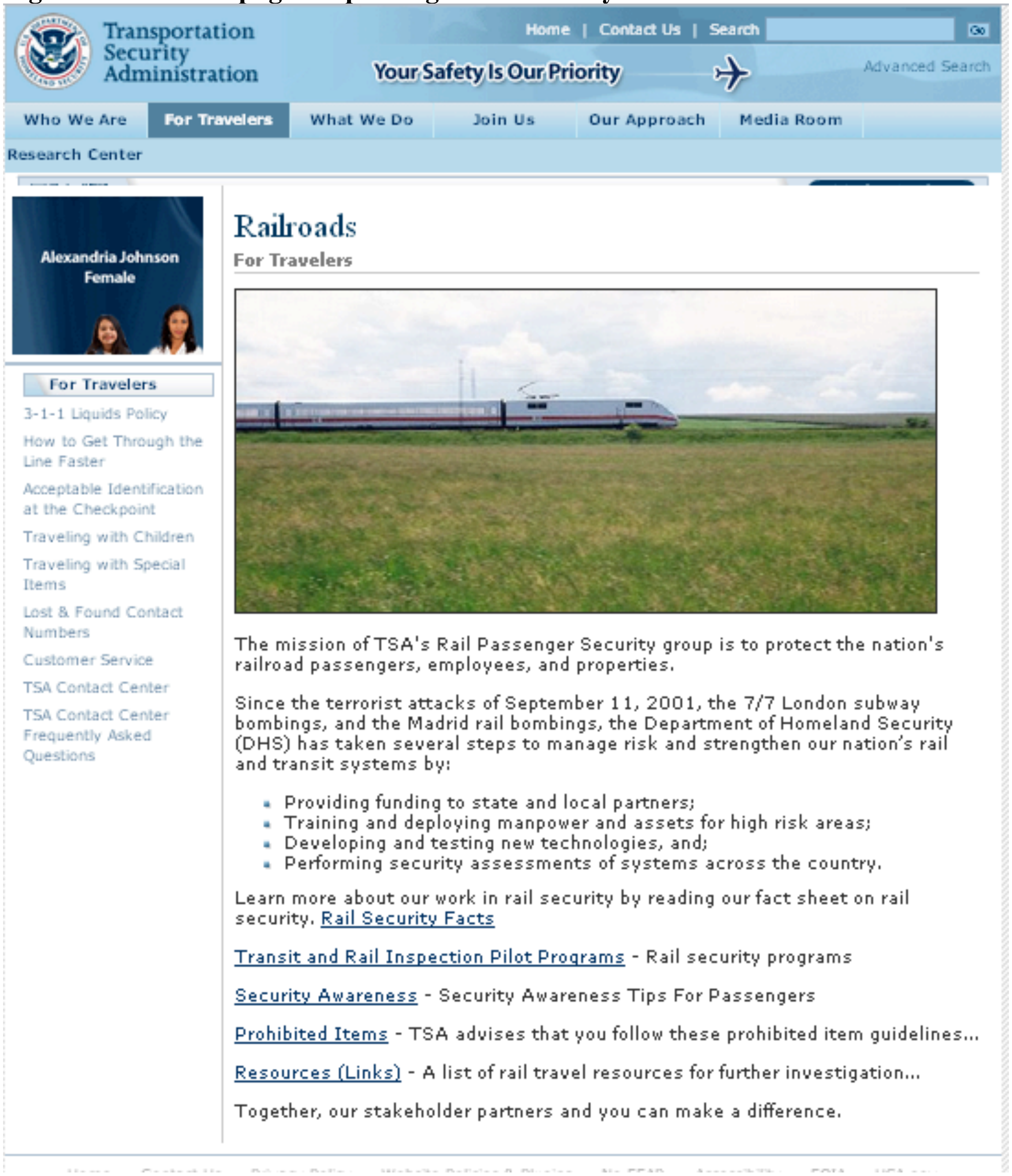
TSA: **Travel** Document Checker (TDC)
... **Travel** Document Checker (TDC). Layers of Security. In June ... documents. **Travel** Document Checking Success Stories. Julia ...
www.tsa.gov/what_we_do/layers/tdc/index.shtm - 17k

TSA: **Travel** Agencies
... **Travel** Agencies. Secure Flight. ... As a member of the **travel** community, we understand that the Secure Flight requirements affect you in several ways. ...
www.tsa.gov/what_we_do/layers/secureflight/travel_agencies.shtm - 15k

TSA: Secure Flight Program

[36] http://www.tsa.gov/travelers/rail/index.shtm

Figure 5: TSA web page for passenger rail security information


Transportation Security Administration
Home | Contact Us | Search
Go
Your Safety Is Our Priority
Advanced Search
Who We Are
For Travelers
What We Do
Join Us
Our Approach
Media Room
Research Center
Alexandria Johnson
Female
For Travelers
3-1-1 Liquids Policy
How to Get Through the Line Faster
Acceptable Identification at the Checkpoint
Traveling with Children
Traveling with Special Items
Lost & Found Contact Numbers
Customer Service
TSA Contact Center
TSA Contact Center Frequently Asked Questions

Railroads

For Travelers

The mission of TSA's Rail Passenger Security group is to protect the nation's railroad passengers, employees, and properties.

Since the terrorist attacks of September 11, 2001, the 7/7 London subway bombings, and the Madrid rail bombings, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen our nation's rail and transit systems by:

- Providing funding to state and local partners;
- Training and deploying manpower and assets for high risk areas;
- Developing and testing new technologies, and;
- Performing security assessments of systems across the country.

Learn more about our work in rail security by reading our fact sheet on rail security. Rail Security Facts

Transit and Rail Inspection Pilot Programs - Rail security programs

Security Awareness - Security Awareness Tips For Passengers

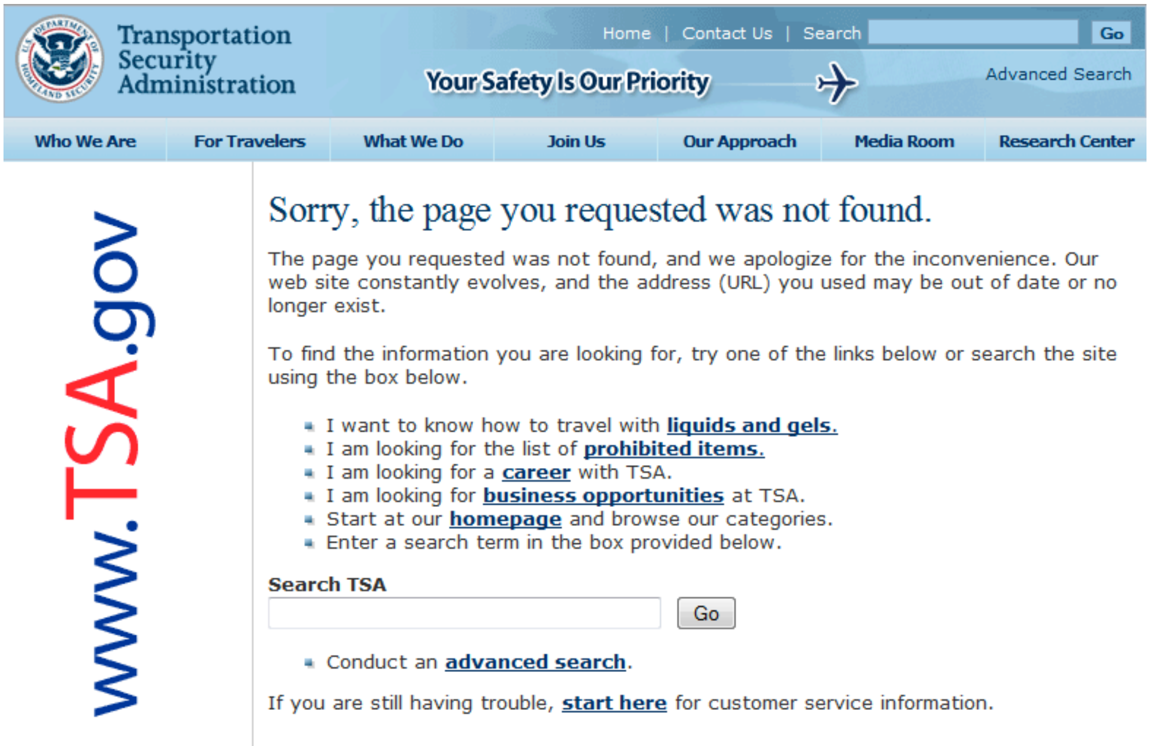
Prohibited Items - TSA advises that you follow these prohibited item guidelines...

Resources (Links) - A list of rail travel resources for further investigation...

Together, our stakeholder partners and you can make a difference.

Source: www.tsa.gov

Figure 6: Results from rail travel information links



Sorry, the page you requested was not found.

The page you requested was not found, and we apologize for the inconvenience. Our web site constantly evolves, and the address (URL) you used may be out of date or no longer exist.

To find the information you are looking for, try one of the links below or search the site using the box below.

- I want to know how to travel with **liquids and gels.**
- I am looking for the list of **prohibited items**.
- I am looking for a **career** with TSA.
- I am looking for **business opportunities** at TSA.
- Start at our **homepage** and browse our categories.
- Enter a search term in the box provided below.

Search TSA

Go

- Conduct an **advanced search**.

If you are still having trouble, **start here** for customer service information.

Source: www.tsa.gov

Yet in 2004, TSA issued a news release detailing the launch of its new passenger rail security pilot project, which purported to test bomb detection equipment. The news release noted that rail passengers still could carry many of the items that were restricted from airlines.[37] However, none of this information is included in TSA's railroad page.

(U/FOUO) A discussion with a security expert, who did not wish to be directly identified or quoted, revealed in detail that many of his experiences with TSA were frustrating because rail security was not taken seriously and oversight was sometimes lax. Terrorist attacks were TSA's primary concern, said this expert, along with weapons of mass destruction. Little concern was given to other potential security breaches.

[37] Department of Homeland Security, news release, "TSA Launches New Passenger Rail Security Project," May 3, 2004, http://www.tsa.gov/press/releases/2004/press_release_0413.shtm

A visit to the TSA web site on May 30, 2011, a full month after the killing of Osama bin Laden, showed a TSA statement in relation to transportation security – "TSA Statement on Airline Security Following the Death of Osama bin Laden." A single statement from the Department of Homeland Security was posted to the TSA web site on May 5, 2011, regarding rail security. However, TSA made no statement of its own, as it had for airline security three days previously.

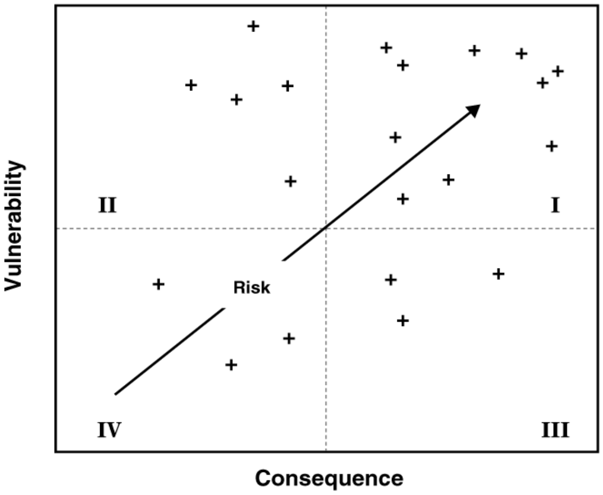
Special HSR Conditions

As noted above, HSR is likely an attractive target if only by virtue of its potentially iconic status. As an entirely new infrastructure, it will require billions of dollars in public and private funds, along with many years of construction. This investment should be protected not only from the terrorist, but also from vandals, criminals, taggers, trespassers, or anyone else planning to harm the system.

Why protect the system from seemingly harmless taggers and trespassers? A condition known as "the broken window syndrome" commonly attracts harmful activity. That is, when graffiti or other forms of vandalism are evident, it indicates that security is lax, at least in that geography and perhaps within the entire system. This lack of internal control can attract others who could take more serious measures, believing that their activities will not be monitored immediately or even for some time.

Peter Guerrero and Norman Rabkin, in their testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, noted that a risk management approach to security is best. They stated that "the highest priorities emerge where threats, vulnerabilities, and criticality overlap. For example, rail infrastructure that is determined to be a critical asset, vulnerable to attack, and a likely target would be at most risk and therefore would be a higher priority for funding compared with infrastructure that was only vulnerable to attack."[38] (See Figure 7.)

Figure 7: Sample of a Relative Risk Diagram



(+) Assets and scenarios

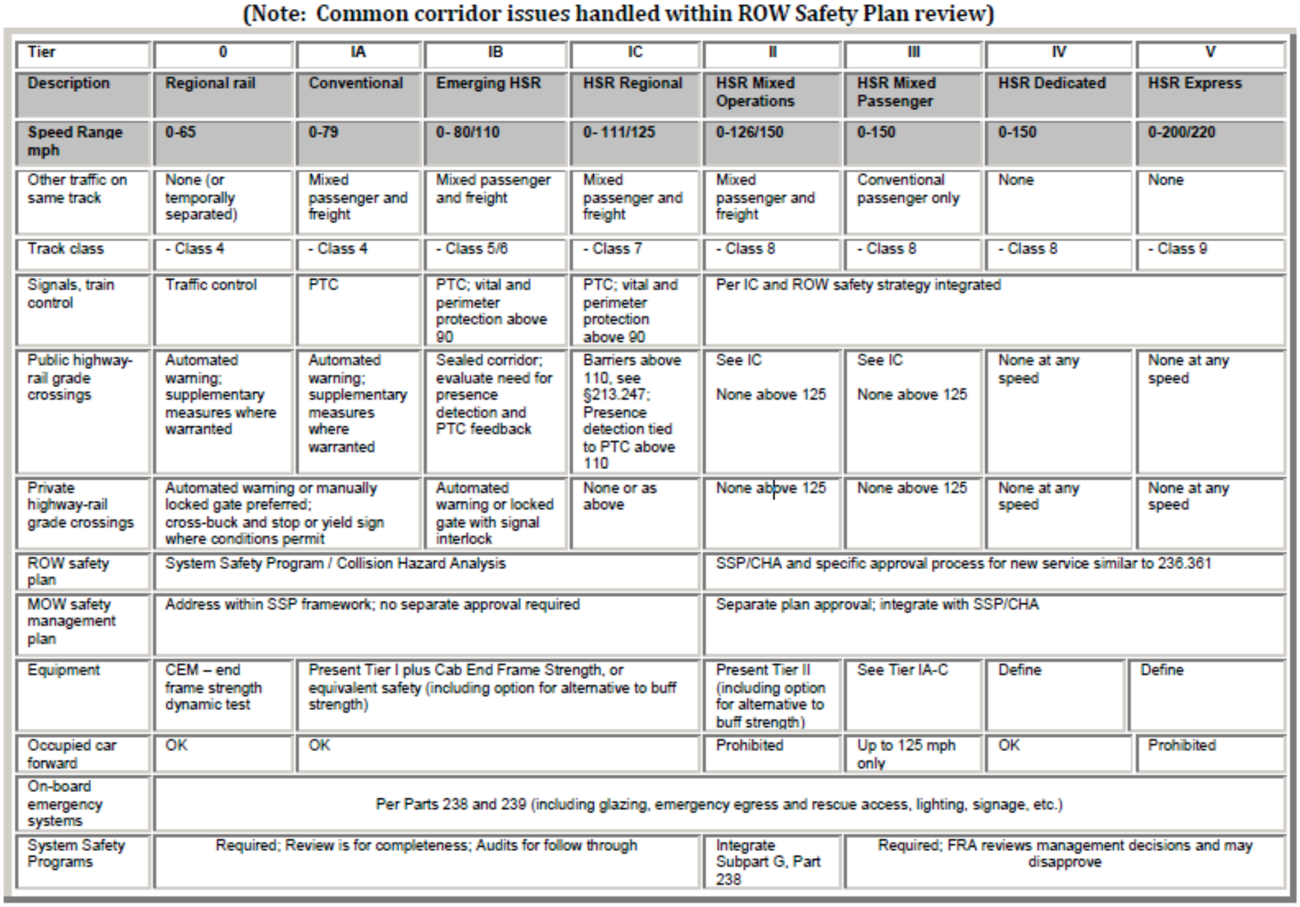
Source: ODP.

Does HSR fit that "first priority" profile? It most likely does for several reasons. First, HSR (including the incremental upgrades) will form a new national infrastructure. As such, it will be subject to greater scrutiny and held to higher standards than today's inter-city rail system. The effects of certain risks could be much greater on HSR, justifying a greater level of security. Because of the wider geography covered by HSR, it may require not only the standard local-area controls, but also a larger, national involvement with several agencies participating. The larger distances also could affect a greater number of stakeholders with a variety of standards and practices. Therefore, HSR

[38] Guerrero, Peter F., Director, Physical Infrastructure Issues; and Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, *RAIL SECURITY: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, March 23, 2004

security may require a more equitable approach to unify those security controls.[39] (See Figure 8. A larger version is included in Appendix C.)

Figure 8: Potential Tier Structure for Passenger Systems



(Note: Common corridor issues handled within ROW Safety Plan review)

Tier	0	IA	IB	IC	II	III	IV	V
Description	**Regional rail**	**Conventional**	**Emerging HSR**	**HSR Regional**	**HSR Mixed Operations**	**HSR Mixed Passenger**	**HSR Dedicated**	**HSR Express**
Speed Range mph	**0-65**	**0-79**	**0- 80/110**	**0- 111/125**	**0-126/150**	**0-150**	**0-150**	**0-200/220**
Other traffic on same track	None (or temporally separated)	Mixed passenger and freight	Mixed passenger and freight	Mixed passenger and freight	Mixed passenger and freight	Conventional passenger only	None	None
Track class	- Class 4	- Class 4	- Class 5/6	- Class 7	- Class 8	- Class 8	- Class 8	- Class 9
Signals, train control	Traffic control	PTC	PTC; vital and perimeter protection above 90	PTC; vital and perimeter protection above 90	Per IC and ROW safety strategy integrated			
Public highway-rail grade crossings	Automated warning; supplementary measures where warranted	Automated warning; supplementary measures where warranted	Sealed corridor; evaluate need for presence detection and PTC feedback	Barriers above 110, see §213.247; Presence detection tied to PTC above 110	See IC None above 125	See IC None above 125	None at any speed	None at any speed
Private highway-rail grade crossings	Automated warning or manually locked gate preferred; cross-buck and stop or yield sign where conditions permit		Automated warning or locked gate with signal interlock	None or as above	None above 125	None above 125	None at any speed	None at any speed
ROW safety plan	System Safety Program / Collision Hazard Analysis				SSP/CHA and specific approval process for new service similar to 236.361			
MOW safety management plan	Address within SSP framework; no separate approval required				Separate plan approval; integrate with SSP/CHA			
Equipment	CEM – end frame strength dynamic test	Present Tier I plus Cab End Frame Strength, or equivalent safety (including option for alternative to buff strength)			Present Tier II (including option for alternative to buff strength)	See Tier IA-C	Define	Define
Occupied car forward	OK	OK			Prohibited	Up to 125 mph only	OK	Prohibited
On-board emergency systems	Per Parts 238 and 239 (including glazing, emergency egress and rescue access, lighting, signage, etc.)							
System Safety Programs	Required; Review is for completeness; Audits for follow through				Integrate Subpart G, Part 238	Required; FRA reviews management decisions and may disapprove		

Source: High-Speed Passenger Rail Safety Strategy, US DOT/FRA November 2010

That said, how far can HSR security go? Here in the US, people expect a greater amount of personal freedom, including the freedom to go where they wish with a minimum amount of inconvenience. Because Americans own so many private cars, they have come to expect that travel is a personal right that allows them to choose the route, mode, price, speed, distance, and even their traveling companions. As general experience

[39] Chang, Monica, "High-Speed Movement on Rail Security," ASMag.com, November 17, 2010

with Transportation Security Administration screening in airports has shown, Americans don't like to be slowed down (even for five or 10 minutes in a security line), to have their personal effects x-rayed and searched, and especially to have their bodies touched, scanned, or viewed in any state of undress.

This is perhaps the reason that one major selling point for HSR is that "you won't have to remove your shoes." For now, that may be true. And for now, one may expect that HSR security measures will be at an acceptable level for most travelers – that is, at a less intrusive level than for air travel.

Some foreigners may find this puzzling, especially if they have experienced – directly or indirectly – the effects of terrorism on public transportation. Because of this, they have come to accept a higher level of screening when they travel, and to expect armed guards, surveillance cameras, and other means of security.

A report to the US GAO says, "According to foreign rail operators, these experiences have resulted in greater acceptance of certain security practices, such as random searches, which the U.S. public may view as a violation of their civil liberties or which may discourage them from using public transportation."[40]

That may be true, but at least one researcher believes that, even following an attempted attack on the TGV, the French people still want convenience and a minimum of barriers when they travel. In *Terror on the TGV? The Terrorist Threat to France's High-Speed Rail Network*, Dylan Kissane of the School of International Studies at the University of South Australia, writes, "(P)assengers would no longer be able to arrive and board the train moments before departure, passengers would endure longer waits should

[40] United States Government Accountability Office, *Passenger Rail Security Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, Report to Congressional Requesters, September 2005

they be taking multiple pieces of baggage aboard the train, family members will be barred from assisting elderly or disabled passengers from boarding and ticket purchasers would be required to book tickets in the name and with the photo identification of other passengers. This may encourage passengers to seek alternate transport – personal vehicle, bus or TER train – to avoid the inconvenience of the TGV network under a counter-terrorist screening regime."[41]

However, HSR passengers are generally traveling longer distances than with inter-city or commuter rail – usually up to 350 or 400 miles from home. This means they carry more baggage, which must be screened. In addition, many more passengers ride the rails than fly, which means that thorough screening would be cumbersome. But even if only HSR passengers are given special screening, how does an agency determine who to screen when those passengers arrive at the station? In some instances, separate boarding areas have been set up for HSR travelers so screening can be accomplished without undue inconvenience to commuter rail passengers or other more casual riders.[42]

These and other considerations qualify HSR for special security treatment, with the caveat that those measures should not then add so much time that the mode is no longer high speed.

On another front, DHS is investing $40 million in 14 areas of cyber-security research through its Science and Technology Homeland Security Advanced Research

[41] Kissane, Dylan, *Terror on the TGV? The Terrorist Threat to France's High-Speed Rail Network,* presented at the Contemporary Challenges and Future Trends in International Security conference, American Graduate School of International Relations and Diplomacy, Paris, France, June 20-21, 2007
[42] Chang, Monica, "High-Speed Movement on Rail Security," ASMag.com, November 17, 2010

Projects Agency (HSARPA). The Department is seeking proposals in each of these areas, with research focusing on both traditional and more forward-thinking security methods.[43]

Evidence shows that DHS is wise to be concerned. Clever social engineering practitioners can gather a great deal of sensitive information – or at least clues that lead to sensitive information – simply by talking their way into it. Cyber attacks can quickly follow if those hackers can create malware specifically for a particular target or category of targets.

According to an article on DarkReading.com,[44] a competition was held in August 2010 at Defcon, a conference for hackers, in which 17 contestants were tasked with obtaining as much secure information as possible from targeted companies within 25 minutes. Those companies included Google, BP, McAfee, Symantec, Shell, Microsoft, Oracle, Cisco, Apple, and Walmart. The greatest success came primarily from contacting the companies' call centers, and secondarily from asking a receptionist for a specific person they had researched in advance.

One-third of the callers posed as company employees, and another one-third or so posed as poll takers. Some companies put up resistance, but contestants generally succeeded when they called back and reached a different employee. "More than half of the targets gave the name of their operating system version, browser version, email client, and antivirus package," the article said.

Given that a new HSR system will most certainly include a great deal of digital technology, hacking into the system could prove devastating. A social engineering attack

[43] Montalbano, Elizabeth, "DHS To Invest $40 Million On Cybersecurity Research," *InformationWeek*, February 1, 2011

[44] Higgins, Kelly Jackson, "Social Engineering Report Shows Corporate America At Risk," DarkReading.com, September 15, 2010

can easily circumvent even the most sophisticated electronic protection because humans often can be the weakest link in a security protocol. According to Pinkerton counter-espionage expert Bruce Wimmer, if a company experiences one type of cyber attack or social engineering attack, it should prepare for other security issues because attackers always use more than one technique.

Information "silos" are a particular vulnerability, according to Mr. Wimmer, because when information is not shared across the organization, no one person or group will have the entire scope of the attack. "If you detect a cyber issue," he said, "you're under attack everywhere else – if not now, then soon. If you see anyone diving into your Dumpster, you have a problem and should prepare for a threat. Attackers go after their targets with multiple methods."[45]

Approaches to Secure the Asset

From most indications in the literature research, it appears that many of the federal approaches to rail security are "suggestions" rather than "requirements." This may leave too many facets of protection up to the discretion of the operators or the local agencies, resulting in a diverse collection of policies and practices.

For example, the Office of Intelligence and Analysis says, "DHS/I&A and TSA *recommend* and support a robust program of protective measures for the mass transit sector. The TSA security *recommendations* below stress vigilance, integration, and unpredictability. They are *intended* to extend the frequency and duration of terrorists' preoperational research, surveillance, reconnaissance, and other preparations; to create

[45] Wimmer, Bruce, CPP, Director of Global Consulting & Logistics, Pinkerton Consulting & Investigations seminar on Business Espionage in the 21st Century, San Mateo CA, March 10, 2011

opportunities for them to make noticeable mistakes; and to detect their activities and disrupt their plans."[46] [Emphasis added.]

In following up with more detail, the same document says, "Suspicious activities *should* be reported to authorities," "Mass transit and passenger rail agencies *should* strive for unpredictability in their security procedures," and "*Consider* establishing surveillance at key entrances and areas of high consequence or high pedestrian traffic."[47] [Emphasis added.] These measures use "soft language" that merely proposes rather than requires particular actions, which means that individual operators, agencies, and other relevant parties may pick and choose what they wish to follow, creating inconsistencies across the board.

Peter Guerrero and Norman Rabkin, in their testimony before the U.S. Senate, have noted that it is important to coordinate rail security across the nation or risk duplication and confusion. They also recommend the above-mentioned risk management principles as a key to helping make difficult decisions, especially regarding budgetary concerns.[48]

Other documents noted that rail regulations and enforcement are not always uniform across the US because of the number of operators, agencies, governments, and other stakeholders having an interest in securing rail assets. For example, the Federal Railroad Administration regulates rail safety for commuter rail and Amtrak. Individual states and municipalities have their own interests regarding rail that passes through their

[46] Office of Intelligence and Analysis Assessment, *Threat Assessment: Mass Transit and Passenger Railroads*, June 29, 2010

[48] Guerrero, Peter F., Director, Physical Infrastructure Issues; and Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, March 23, 2004

jurisdictions. Rail operators and private industry have a stake, each with its own policies. If those operations cross several state or local jurisdictions, it typically brings into play several different – and perhaps conflicting – policies and regulations. Even emergency response to rail incidents may fall to various government agencies.[49]

These issues suggest that HSR has the opportunity to set a precedent by creating and implementing a model for uniform regulations, policies, and best practices.

In fact, the landscape may be changing already. In a telephone interview with Paul Mosier, senior rail operations engineer at Parsons Brinckerhoff, he said that the Federal Railroad Administration is transitioning into having more responsibility to broker federal funds and to handle the reviews for stimulus money.

"They are very much in tune with enhancing the regulations and requirements, and I expect they will use stronger and different language," he said. "The role for FRA is becoming more clear. They will become what the [Federal Aviation Administration] is for the airlines. Previously, FRA's primary oversight was for safety and regulations. Now they will be responsible for funding, oversight, and all the regulations in the FRA code – including freight, passenger rail, and high-speed rail."

This is especially important as it relates to HSR, he said, because it is technically different from inter-city rail, requiring more precision and a different degree of tolerance for remaining within specifications. Even safety and security will be a priority now for FRA, although the role is still evolving.[50]

[49] United States Government Accountability Office, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, Report to Congressional Requesters, September 2005

[50] Telephone interview, April 12, 2011

Sample US Passenger Rail Security Practices

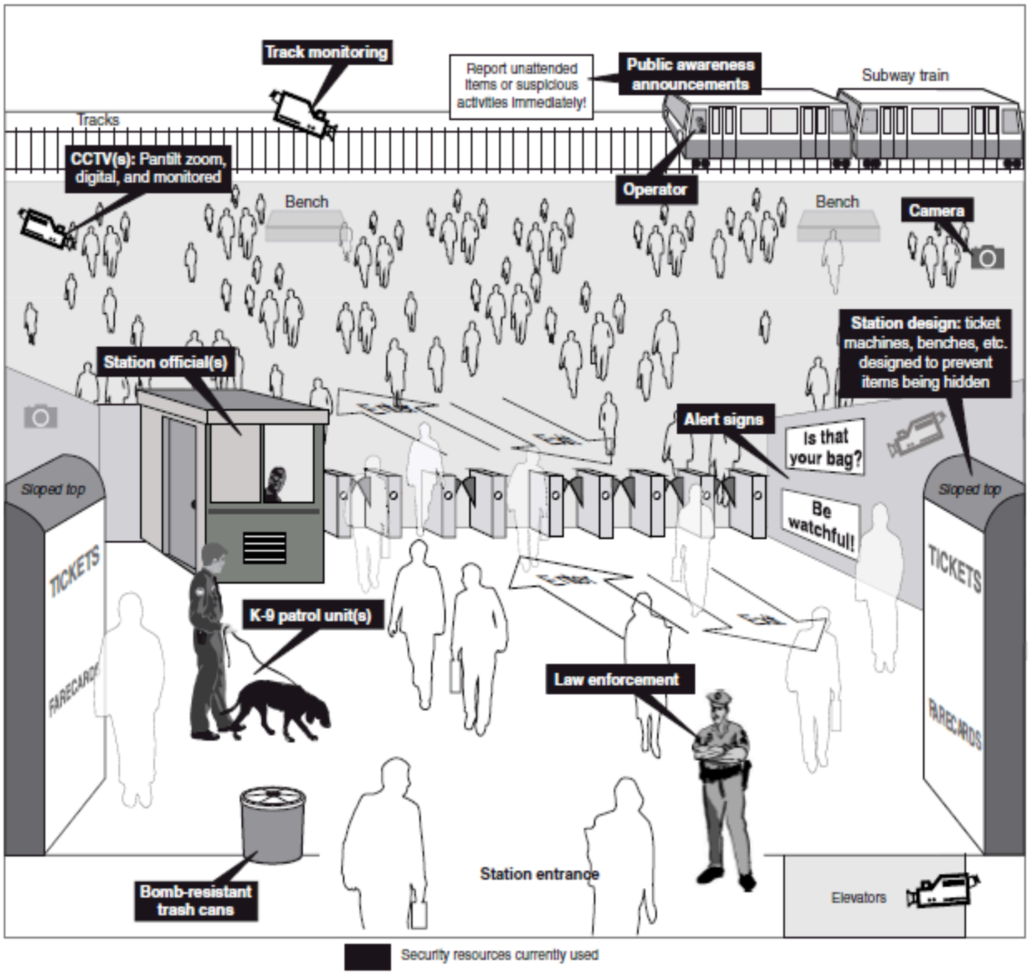
Despite the historically lower interest in rail security (versus air security) by government regulators, some rail operators in the US and abroad have instituted a number of security measures that have certain effectiveness. For example, many rail operators and stations do use barriers, surveillance, alarms, and inspection. These include fences, closed circuit television (CCTV), sweeper trains for periodic inspections of rails and rights-of-way, citizen awareness campaigns, manual inspections, cooperation with local law enforcement and first responders, specially-designed vending machines and trash receptacles to minimize bomb placements, random bag inspections, chemical-sniffing canines, crash avoidance systems, and other security methods. (See Figure 9.)

In an article for *Emergency Management* magazine, author Margaret Steen suggested four avenues for taking rail security to a higher level. These include screening passengers and luggage, at least on a random basis to avoid bringing the system to a complete halt; reinforcing train windows to withstand greater force than the current standard of a .22-caliber rifle; air conditioning the locomotives [or with HSR, the operator compartment] so windows and doors need not be opened in warm weather; and involving citizens to report any suspicious behavior, packages, or other situations.[51]

According to a statement by JayEtta Z. Hecker, Director of Physical Infrastructure Issues, foreign operators have much that the US can learn from, although domestic operators have implemented many similar measures, such as citizen awareness, improved technology, better perimeter and access protections, and certain risk assessments. Some of these foreign controls may not be acceptable to the American traveler, however. These

[51] Steen, Margaret – "Safeguarding the Rails: Four Avenues for Increasing Security," *Emergency Management*, November 29, 2010

Figure 9: Some current security resources


Track monitoring
Report unattended items or suspicious activities immediately!
Public awareness announcements
Subway train
Tracks
CCTV(s): Pan/tilt zoom, digital, and monitored
Operator
Bench
Bench
Camera
Station design: ticket machines, benches, etc. designed to prevent items being hidden
Station official(s)
Alert signs
Is that your bag?
Be watchful!
Sloped top
Sloped top
TICKETS
FARECARDS
TICKETS
FARECARDS
K-9 patrol unit(s)
Law enforcement
Bomb-resistant trash cans
Station entrance
Elevators
Security resources currently used

Source: GAO and NOVA Development Corporation

include covert testing to ensure employee alertness, and centralized clearinghouses on rail security technologies, such as chemical sensors. “While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges,” Ms. Hecker noted, “the practices may nevertheless warrant further examination.”[52]

[52] Hecker, JayEtta Z., Director of Physical Infrastructure Issues, *Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts*, March 29, 2007

Ms. Hecker also noted that closed-circuit television (CCTV) was popular among the operators they interviewed, even though it was not perfect. It is not possible for personnel to monitor all places at all times, but the cameras were credited with deterring crime, helping security personnel determine how to respond to incidents, and allowing personnel to monitor certain areas if a credible threat is received or suspected.

As an example, she said, "One rail operator, New Jersey Transit, had installed 'smart' cameras, which were programmed to alert security personnel when suspicious activity occurred, such as if a passenger left a bag in a certain location or a boat docked under a bridge. According to the New Jersey Transit officials, this technology was relatively inexpensive and not difficult to implement. Several other operators said they were interested in exploring this technology. Abroad, all 13 of the foreign rail operators we visited had CCTV systems in place."[53]

Sample Foreign Passenger Rail Security Practices

In other nations, a variety of security practices have been implemented. This list, while not comprehensive, includes several examples of those practices that already are or that could be applied to HSR. All were obtained through literature review.

Spain – ObjectVision, a security equipment company, detailed how the Spanish HSR system was addressing its vulnerabilities, especially following the attacks in Madrid. In its marketing data sheet, the company noted that the Spanish rail operators were concerned about opportunistic crime (theft, vandalism, etc.) as well as more serious safety and security issues. They already had an extensive network of CCTV equipment, but they wanted to leverage it better with enhanced security features.

[53] Ibid

Using ObjectVideo's intelligent video surveillance capability, Spanish HSR security personnel can set rules using virtual "areas of interest" to monitor the rail tracks and any sensitive areas around them such as bridges and tunnels. The system identifies abnormal activity, classifies it, tracks it, and reports it to security personnel in real time.[54]

France – According to Jenkins, Butterworth, and Clair (March 2010), French authorities try to control rail and metro security costs by relying on unpredictability to keep terrorists on their guard, compelling them to believe that they can be apprehended at any time. The French also leverage intelligence operations, obtaining general security insight about terrorist activities and groups.

The researchers note that, "In contrast to the heavy security at rail and metro stations, the situation in Lyon posed little risk for the saboteurs. The TGV operated on a dedicated line, which, because of the high speed of the train, was protected by a fence. The fence did not prove to be much of a barrier—the terrorists merely cut their way through it. There were no alarms and few security cameras."[55]

The report further notes that "sweeper trains" are deployed before daily operations begin so they can detect any abnormalities along the tracks. On the day of the TGV attack, the sweepers did not detect the bomb as it sat adjacent to and just below the tracks. Now, inspections are done in teams of two, with one person watching specifically for any suspicious devices or obstacles.[56]

Russia – According to an online article, Russia had already begun its planning to increase security at the country's train stations before the January 2011 fatal

[54] ObjectVideo marketing data sheet, "Keeping Track: Rail Security," reviewed March 4, 2011
[55] Jenkins, Brian Michael; Butterworth, Bruce R.; Clair, Jean-François, *Off the Rails: The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts*, Mineta Transportation Institute report CA-MTI-10-2501, March 2010
[56] Ibid.

attack at the Moscow airport. Since then, the rail stations have responded by enhancing security with 80 metal detector frames in Moscow, 22 in St. Petersburg, and two each at Tver and Vyborg. [Numbers are current as of the article date.]

Russian Railways also employs nearly 100 private security personnel, as well as transport police that protect Moscow stations. Last July, inspection systems were installed in 34 stations to screen passengers and baggage. Rail personnel also are being trained how to respond in emergency situations, and CCTV has been installed in many stations, sending images to police and other law enforcement.[57]

The UK – A few foreign rail systems are using detection devices to monitor for chemical, biological, or radiologic elements, at least on an experimental basis. In the UK, officers from the British Transport Police (BTP) use pagers that detect these elements in the air. Thus, they can respond immediately to any likely threats. The BTP also have special vehicles fitted with equipment that can detect suspected bombs inside unattended baggage.[58]

The same article notes that one foreign rail operator was retrofitting its passenger cars with windows that can be opened in case of a chemical attack. It also notes, "In addition, the London Underground, one of the oldest rail systems in the world, incorporates security into the design of all its new stations as well as of modifications to existing stations. We observed several security features in the design of Underground stations, such as the use of vending machines that have no holes that someone could use to hide a bomb, and sloped tops to reduce the likelihood that a bomb can be placed on top of the machine. In addition, stations are designed to provide staff with clear lines of sight

[57] Samuel, A., *Russian Railways step up security measures*, rail.co article, February 23, 2011

[58] Hecker, JayEtta Z., Director of Physical Infrastructure Issues, *Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts*, Testimony on March 29, 2007

to all areas of the station, such as underneath benches or ticket machines, and station designers try to eliminate or restrict access to any recessed areas where a bomb could be hidden."[59]

Germany – In Germany, rail security isn't perfect, but it works, notes Moore. Surveillance is key, with CCTV implemented on train platforms, while security personnel in uniform walk the trains and the larger stations. But that's about as far as it goes. Moore says, "Even after two young Lebanese men left dud bombs on two separate trains in Germany in 2006, Deutsche Bahn officials said it would be impractical to search all rail baggage."[60]

Further, HSR in Germany runs along the same corridors as freight and inter-city rail. It would be impossible to tease out maximum security for HSR without affecting the others, and it would inhibit all rail movement if high security were integrated into all three. They've decided it isn't practical, so they accept the risk and move on.[61]

Germany also has highly trained "rapid response" teams that handle rail emergencies with precision techniques. In essence, they are the railroad version of a SWAT team. (In the US, only CSX has a similar police force.)

Unidentified countries – To ensure that security personnel remain sharp, a minority of countries use "covert testing" to keep security and rail personnel on their toes. In these situations, an event is staged to observe how well personnel react to the incident. These may include setting off alarms or placing unattended bags or other items around the stations to observe how the staff responds.

A rail company in Asia will break seals on fire extinguishers or open alarmed doors to test personnel reaction time. These tests, which are conducted daily, let the rail

[59] Ibid
[60] Moore, Michael Scott, *High-Speed Rail's Weak Link Is Security*, Miller-McCune, May 4, 2011
[61] Ibid

personnel know that real incidents can happen without warning at any time, so they are more likely to remain vigilant.[62]

Unidentified countries – Some nations randomly screen passengers and bags, with security personnel approaching passengers anywhere in the station or aboard the trains. Any passenger who refuses inspection must leave immediately.[63]

"The difference between America and Europe, at the moment," writes Moore, "is that security theater carries no political reward in Europe: No mainstream politician wants to inconvenience a lot of voters for security that will never be airtight. Europeans have lived with bustling, open-plan train stations for centuries; they know the odds."

In America, he goes on, good rail travel is evolving into something new and unknown. If U.S. politicians start clamoring for airline-style security practices, the advantages of rail travel will evaporate.[64]

HSR Security Challenges

Some particular challenges face HSR security in the United States, and a few will require new approaches to address them. For example, out of necessity, *some HSR lines will share rights-of-way with highways*, such as the route between Victorville CA and Las Vegas NV, which will follow Interstate 15. When the Florida project is finally underway, the first segment will use the highway median between Orlando and Tampa. When trains run at speeds in excess of 150 miles per hour so close to automobile traffic, it becomes especially critical to secure the HSR rights-of-way to prevent vehicle intrusion.

[62] *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, United States Government Accountability Office Report to Congressional Requesters, September 2005
[63] Ibid
[64] Moore, Michael Scott, *High-Speed Rail's Weak Link Is Security*, Miller-McCune, May 4, 2011

Currently, the Federal Railroad Authority has no standards for integrating a rail line with a highway system, and already it has caused problems with a commuter rail system that shares a highway right-of-way.

The New Mexico Rail Runner Express is a commuter rail system that uses the Interstate 25 median to run between Santa Fe and Albuquerque NM. No special guard rail provisions are given, which means the median is treated the same, regulation-wise, whether or not there is a rail system in place. Since the service was inaugurated in December 2008, some safety incidents have occurred, including an automobile on the tracks when the driver tried to avoid hitting a coyote on the roadway.[65]

- **Recommended Best Practice →** Create a standard that will allow safe and secure right-of-way sharing between rail and highways or other infrastructure. Ideally, the standard will permit optimum operation for both subjects.

Although HSR will eliminate any grade crossings, there still remains *a potential issue with highway overpasses*. As an example, the Massachusetts Bay Transit Authority (MBTA) reported on February 15, 2011, that a motor vehicle was driven off an overpass, landing on the MBTA commuter rail tracks below and impeding traffic. The driver reportedly had a medical condition that likely contributed to the accident.[66]

Is there a method to ensure that vehicles will not fall from an overpass onto the HSR tracks? What about vandals or terrorists who could drop bombs, incendiary devices, or obstacles ahead of the trains? Will HSR in the US include intrusion detection nets or other safety and security measures, as they do in Europe? And what about pedestrian and

[65] US DOT/FRA, *High-Speed Passenger Rail Safety Strategy*, November 2009
[66] MBTA Transit Police intelligence report, emailed version, February 15, 2011

bicycle pathways along the rail corridors? Currently, they are permitted adjacent to inter-city and commuter rail lines. Will they be permitted along HSR lines as well?[67]

- **Recommended Best Practice →** Create a standard that prevents intrusion from overpasses, tunnels, bridges, pathways, or other infrastructure.

Security is not cheap, as evidenced by the millions upon millions of dollars invested in air transport security across the US. And yet, that system still remains imperfect and ever-changing. With each new threat comes another round of new and more expensive equipment and training.

What would prevent any rail operator from implementing only those security measures that do not over-burden the company's operating budget? And if those measures were mandated, who would pay for them? If it's the rail operator, the costs would be passed along to the passengers. If it's the federal government, where would the budget come from? Given today's anti-tax atmosphere, it would be difficult to generate sufficient revenue to pay for such a staggering expense – at least, not in a time when certain voting blocs are clamoring for more highways or for the government to repair and maintain the existing highway infrastructure.

In their testimony before the US Senate's Committee on Commerce, Science, and Transportation, Guerrero and Rabkin (March 2004) stated that some security improvements are inexpensive, but most require substantial funding. They noted, "Given the tight budget environment, state and local governments and transportation operators, such as transit agencies, must make difficult trade-offs between security investments and other needs, such as service expansion and equipment upgrades."

[67] Ibid

They explained that the problem is worsened by the additional costs the passenger and freight rail providers incur when the federal government elevates the national threat condition.[68]

- **Recommended Best Practice →** Create a standard that clarifies uniform "required" security measures as well as "recommended" security measures. Ensure that these measures do not unreasonably burden the responsible parties, and recommend revenue sources that could fund these measures, perhaps with matching grants. Or realize that perfect security scenarios never will be attainable, and agree to accept certain risks.

The California High Speed Rail blog argues that *thorough screening for every HSR passenger and bag probably isn't the best way to spend what already are limited funds for private rail security*. It notes that random spot checks on everyone could be one option for providing greater security at less cost. But, to be effective, the practice would have to be applied to the passengers of all rail operators and even to those who may be loitering on the property or even just outside it.

"In practice," the blog says, "that would mean replacing railway security staff with regular TSA or police officers. They would already have the legal authority to enforce checks, so attackers cannot just beg off and try again at some other time."[69]

However, given the current financial condition of the US government, it may be unlikely that TSA would have sufficient funding to provide these services – unless they

[68] Guerrero, Peter F., Director, Physical Infrastructure Issues; and Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, "*Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*," March 23, 2004

[69] "Homeland Security Theater," California High Speed Rail Blog, Apr 16, 2011

were reimbursed by the rail companies. That, again, would mean the costs would be passed along to passengers, who may decide the price point is out of reach.

According to Mr. Kozub, it's often difficult for regulators to require certain security measures because of the expense it would entail for the operators.

"CCTV is expensive," he said in a telephone interview. "So are security personnel, inspectors, X-rays, body scanners, and all the other technology. If the regulators tell a rail company that they must take certain measures, the rail company either has to raise its ticket prices, or it has to ask the regulator to help pay for it. So the rail companies may not be required to take certain measures because the cost could be prohibitive, especially when the actual threat is not great enough to justify it."[70]

But at least the technology is improving. The California High Speed Rail Blog noted, "Fortunately, ever-improving software is reducing both the overheads and the risk of human error through partial automation. CHSRA has already budgeted for this in the scope of the engineering work to be done for the California network."[71]

- **Recommended Best Practice →** While retrofitting existing rail infrastructure may be costly, it is easier and more cost effective to build in automation and other security measures when constructing the new "true" high-speed rail infrastructure. Create requirements for HSR and any areas affected by the incremental upgrades. Bring freight and the remaining passenger lines into compliance over time.

Interstate or long-distance passenger rail has security challenges of its own. Any such operator typically traverses remote areas as it connects larger urban centers. These

[70] Telephone interview, March 10, 2011
[71] Homeland Security Theater, California High Speed Rail Blog, Apr 16th, 2010

remote areas are more difficult to patrol with technology, personnel, or both. Even if an intrusion were detected immediately, it could take an hour or longer for security or law enforcement personnel to reach the area, at which time the damage already could have been done.

- **Recommended Best Practice →** Create a standard that requires electronic monitoring of remote areas as well as those that are close in. Require periodic drills to ensure that safety and security personnel and first responders can reach any affected areas within a specified time.

This also brings up the question of *law enforcement responsibility*. When a rail system operates across several jurisdictions, who is responsible for protection? Currently, the practice in the US is to involve the local first responders. But with many communities reducing their staffing because of budget cuts, how many of them will be able to share their remaining law enforcement officers or other emergency personnel with a for-profit rail system? Would they be compelled to charge yearly or even *ad hoc* for such services? And who would pay for them?

- **Recommended Best Practice →** Create a standard to address inter-agency coordination and clear lines of responsibility for emergencies. Determine at least partially self-supporting means to fund enforcement and response.

In many other countries, *a dedicated law enforcement organization protects the entire rail system*. In essence, they are a national police force, demonstrating that their rail systems also are part of the national infrastructure. Here in the US, our rail systems are privately owned, and HSR is expected to follow suit – or at least to be run as a public-private partnership. Could those partnership entities create one unified police force operating under security regulations that would be consistent across the system? If so, who would pay for it – the HSR operators, the federal government, the states, or some combination? What would be the revenue source?

- **Recommended Best Practice →** Investigate the feasibility of creating a national railroad police force with proper law enforcement training. Determine whether it is most feasible to operate through public or private entities.

Another challenge would be *the level of security that would inaugurate the new HSR system*. Travelers are accustomed to removing shoes, screening bags, carrying limited liquids, and now passing through body scanners when they travel by air. They endure it because they have witnessed the shocking results of an airborne terrorist attack, along with thwarted attempts since then.

But so far, no such threats or successful attacks have been carried out against the US rail systems. Travelers are expecting an easier time boarding HSR, especially because part of HSR marketing has been to assure them that they can avoid airport-type security. Is this a wise approach? Are we unwittingly communicating to terrorists that the new HSR system will be wide open? If we do not institute high levels of security from the start, how will HSR operators later retrofit their facilities and rolling stock?

In a telephone interview, David Morgan of the New Jersey Department of Transportation expressed his opinions. He said, “When initiating HSR security, it should start like airline security. If you implement at a low level, with just random searches, and then are required to increase security later, the passengers won't react well. If you implement high security from the start, they'll be much more accepting because they already are familiar with air transport screening."

He noted that most transit implements only random bag searches today. "You can opt out, but you won't ride the transit," he said. "Through TSA, Amtrak did a pilot study on random searches on the trains, and it didn't work well. People didn't like it because, I suspect, they were not accustomed to that level of security on a train." [72]

HNTB conducted a survey of 1,007 randomly selected Americans about air travel security. It showed that 62 percent of respondents said they valued security over convenience, which was favored by 21 percent, or over sustainability, which was favored by 12 percent.[73] Would these results be reasonably applicable to rail travel? One could conjecture that people would be less tolerant of delays on a rail system because the US has not yet experienced a shocking attack on that mode. However, such assumptions cannot be made without a scientifically accurate survey.

Or perhaps Americans should be more sanguine about their safety and security. Nothing ever will be perfect, and the most any reasoned person can expect is "adequate security." Europeans have lived with bombings and the threat of attacks for many years – not only on transportation, but also in night clubs and other public venues. They've endured terrible world wars on their soil, with entire cities destroyed in a few hours. What relative importance can a rail bomb have when it kills only a handful of people? It may be realistic to play the odds; what real chance does an individual have of becoming a direct victim of a terror attack? But would Americans go along with that approach? As a

[72] Morgan, David - Manager, Office of Fixed Guideway Safety/Security Oversight, New Jersey Department of Transportation, telephone interview, January 11, 2011

[73] HNTB news release, "Americans seek air travel security," March 10, 2010

nation, we are accustomed to living in safer conditions than most other regions of the world. Is it time we faced reality?

- **Recommended Best Practice →** Determine the most appropriate level of rail passenger screening that would provide an optimum balance of security and convenience. Accept that no standard will provide flawless protection.

Each of these questions provides a springboard for further research that could help public and private entities to create a greatly improved and standardized strategy for addressing the complex issue of high-speed rail security.

Analysis and Conclusions

Until the recent capture of Osama bin Laden's trove of al Qaida planning documents and other records, rail transport security was considered the poor step-sister of air security. Even with the weighty evidence of research and news reports showing that surface transportation is much more vulnerable to attack because of its open system, that reality was ignored until the bin Laden planning documents were in hand. Further, certain Senators have been fighting mightily to reduce rail security funding in the upcoming fiscal year budget.

Senator Lautenberg's May 6, 2011 news release noted, "During this year's budget debate, House Republicans tried to drastically cut rail security grant funding by 67% compared to 2010. Democrats were able to secure $150 million more than the Republican proposal by providing a total of $250 million for rail security for Fiscal Year (FY) 2011."[74]

Although this news release has a certain political slant, it does demonstrate a strong partisan debate about the value of rail security and the vulnerability of its funding. Will that change as a result of recent events in Pakistan? That remains to be seen.

For all practical purposes, TSA has virtually ignored rail security, even with its mandate to protect all transportation modes. That must change. *TSA must equally include high-speed rail – and all other rail modes – in its security planning and implementation.* Otherwise, one can expect high-speed rail security strategies to follow the same second-class path as that of inter-city rail.

Perhaps the time is at hand for serious change to come about. As this nation has reached the confluence of a new rail system creation and the knowledge that rail transport is highly exposed, perhaps the US has at last reached the ideal time to review and reform its security strategy not only for inter-city and transit rail, but especially for high-speed rail. Certainly, some may argue that passenger safety and security are the responsibility of the operators. However, operators have typically included only those measures that are required by law. *Higher authorities must mandate change before it will happen.*

Although high-speed rail will have unique safety and security features built into the system, this new mode also will have particular vulnerabilities, including speed, tilting, iconic status as a significant infrastructure investment, "high-value" passengers, and other attractive reasons to use it as a target. *California, with its pioneering and completely new HSR system, is the ideal candidate to become the nation's model for HSR*

[74] Lautenberg, Frank R., US Senator, D-NJ, news release "Lautenberg Calls Bin Laden Documents Targeting Rail A 'Wake Up Call,'" May 6, 2011

security. In fact, a comprehensive approach – and more important, a uniform approach – to HSR security would be a significant step toward building a strategy for rail and other surface modes. Because California is a center of innovation and a leader of change, it is the ideal place to develop a groundbreaking approach for national HSR security and, by influence, for other rail, as well.

Geographies and other particular factors certainly will influence the details of security strategies for each corridor. *But a comprehensive and standardized model can be created* if it is based on well-researched threat analyses, workable plans to meld HSR security forces and local first responders, realistic expectations for performance, a reasonable funding plan, clear accountability, current technology, and other factors that can be applied across the board.

Threat analyses must form the basis for a successful HSR security strategy. These analyses must examine not only general threats to the system, but also particular threats that could be unique to certain locations and situations. Once those threats are synthesized and prioritized, the plan must address them in order of priorities based on likelihood, potential body counts, proximity to other critical infrastructure such as bridges or power plants, environmental features such as adjacent high-rise office buildings versus open stretches of farmland, cost/benefit ratios, and other relevant factors.

Completed HSR systems can support the security strategy most effectively only if *vulnerabilities are addressed in the design phase, when they can be "engineered out."* For example, cars could be specified with oxygen systems similar to those found in airliners, allowing passengers to use masks in the event that a toxic gas is released. Tunnels engineered with efficient ventilation systems would serve the same purpose.

Specifications must require that manufacturers use carriage materials that meet NFPA-130 (National Fire Protection Association) standards. Operator cabs could be specified with air conditioning to preclude leaving windows and doors open to intruders. Platform specifications could require elements to protect waiting passengers from explosives and debris. Ideally, these considerations would be included in the bid process.

Likewise in those design requirements, specifications could *include security elements that assist first responders, allowing them to maximize their ability to perform.* For example, CCTV could be required in operator cabs and in coaches, and specifications could be included for CCTV inter-operability with emergency responder technology. In practical application, this can allow emergency personnel to receive live images from inside the cab and coaches so they can plan and execute an optimum response.

Any security strategy also *must include a policy for information sharing, thereby eliminating the hazards of "information silos."* These silos are highly detrimental to security because they prevent individual teams from amalgamating the small clues that can create the complete picture of a given threat. Best practices must be specified so all operational and management functions – including those that interface with the public – can easily and effectively share ownership of HSR security. Federal, state, and local authorities must be included in that information sharing.

The HSR security strategy must also address *a right-of-way safety plan, especially in areas where it will share corridors or rails* (e.g., when approaching stations) with inter-city or freight rail or with highway systems or other infrastructure. Although HSR systems do not permit grade crossings, authorities must address the particular dangers that can be associated with corridors that use highway medians, pass under bridges, or operate through urban centers.

Even with all these recommended approaches, *HSR must not overlook what is perhaps the most valuable first line of defense – American citizens and especially rail passengers*, all of whom greatly outnumber security personnel on or around rail property. These are the “auxiliary security” who may notice trespassers, abandoned bags, suspicious behavior, clandestine conversations, vandalism, and other telltale clues long before a security officer may become aware. This key group of potential watchdogs will act in the interest of counter-terrorism if they are made aware of the threats and if they know how to take the appropriate action.

The national “See Something, Say Something” campaign is an excellent start, but it does not go far enough. It does not instruct anyone what to do or where to make the report. Nearly everyone has a cell phone, but phone numbers are not always provided in the event that security personnel are not readily visible. No precautions are given instructing people to stay away from suspicious packages or to clear the area of bystanders. To this researcher’s knowledge, no rail operator or security provider actively engages in assessments to determine the effectiveness of public information campaigns, if any. We believe this is a serious oversight that should be rectified not only for the future of high-speed rail, but for other public modes as well.

As demonstrated by passenger willingness to become involved during perceived airline threats, people feel more secure and empowered when they know how to react and how to take care of themselves and others around them. When given the proper information and the motivation to act, the public can become the ideal first line of defense when a threat materializes. More important, their vigilance can play a key part in helping to thwart the intentions of any terrorist or other criminal.

Finally, no matter how carefully crafted, *a given set of HSR security strategies, tactics, and practices cannot be considered as the entire makeup of the security landscape*. It would be naive to distribute an instructional manual and believe it is the final word. Security must be an organic process, ever evolving to address new threats, technologies, environmental conditions, and myriad other mutable factors that will continue to change.

Appendix A

Additional Elements to Consider in HSR Security

- For airliners, primary security is applied to passengers and their bags. High-speed rail must consider not only that, but also sabotage of the rail lines, including cyber-security to protect switches, signals, and other digitally-controlled systems. HSR protection could include low-voltage currents in the ribbon rails, with alarms that notify security personnel if the current is interrupted. Robotic "inspectors" can be operated by remote control to scrutinize isolated stretches of rail, perhaps with video transmission to security screens at a control center.
- HSR could also follow Amtrak's new Partners for Amtrak's Safety and Security (PASS) program, which relies on rail enthusiasts and other citizens to notify the company of any anomalies they happen to notice. These "rail fans" already are familiar with the details of rails, cars, yards, and other facets of railroad equipment and property. PASS provides a way to enhance the "See Something, Say Something" citizens' involvement program.
- Creating a system-wide security police force would allow HSR to move personnel throughout the system to areas of threat when necessary. It also would support a more homogenized application of policies and procedures rather than following the diverse rules of several public law enforcement agencies. CSX has had its own rapid-response team for some time to protect its freight cars against smugglers and sabotage. This does not preclude the use of local law enforcement, which can be called in for mutual aid, especially if they have been trained and regularly exercised in rail emergency response. European operators are already attempting

to address differences in security regulations and law enforcement as their rail operations cross international borders.

- Cameras that have a DVR can be specified to download recordings passively as the train enters the yard and passes an electronic download device that stores and archives images for later review.
- Within the constraints of law, criminal background checks could be required on all HSR employees and contractors. This includes anyone working in or around the rail properties. Saboteurs can infiltrate through seemingly innocuous positions, such as restroom attendant, yard maintenance worker, and office cleaner.
- Recently, warnings have been distributed regarding suspicious inquiries for training and/or positions within the rail industry. Recipients have been asked to submit those requests to the Federal Bureau of Investigation for vetting, especially if those messages originate in the mid-east and/or come from supposed military personnel based there.

Other specific security elements may include practices and features that have proven effective or that have the potential to increase security when implemented as part of an overall security plan, such as:

- Sensors to detect chemical, radiologic, and biological agents;
- Pagers to notify security personnel so they can react quickly to emergencies or potential emergencies;
- Stations designed with clear sight lines so security personnel can have unobstructed views;

- Enforced and monitored restricted access to certain areas of the station, rail yards, rolling stock, and other property;
- Intrusion detection systems, such as movement sensors on fences, especially in remote geographies that may not afford continuous monitoring by CCTV;
- Other security features that have proven effective or that have shown potential on inter-city rail.

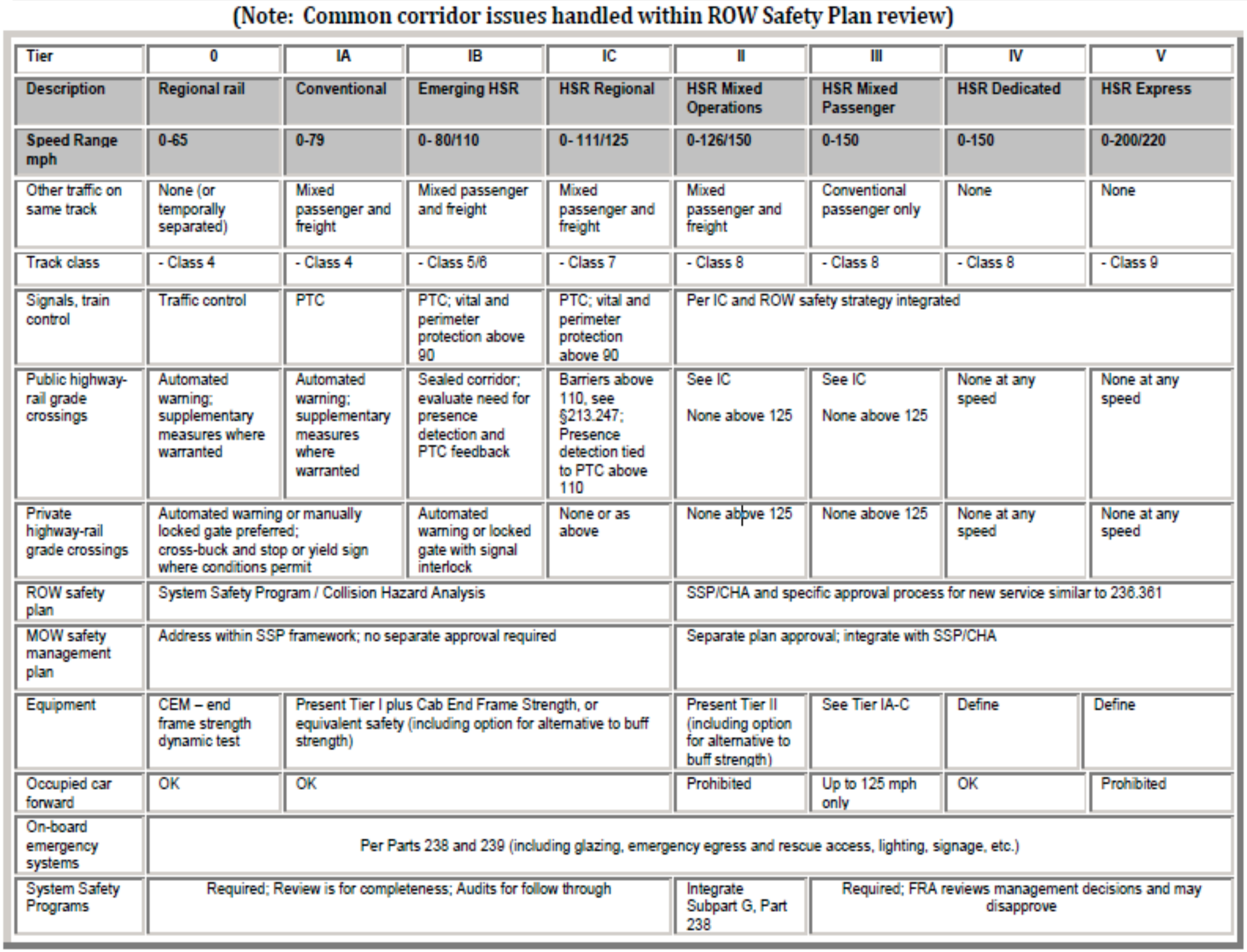
Appendix B

Interview Questions

1. In your opinion, is HSR more vulnerable than conventional rail? Less vulnerable? Or about the same? Why or why not?
2. In your opinion, does HSR require or does it not require unique security approaches?
3. Is it or is it not necessary for HSR to plan for special infrastructure along the ROW, such as bridges, tunnels, power plants, etc? If so, how?
4. If you are planning any HSR security at this point, what will you base it on? FRA regulations for conventional rail? HSR policies from other countries? Something else?
5. What types of threats are being considered in your security planning? (If clarification is needed: Attacks on stations? Attacks in the cars? In the engine compartments? Attacks on or from facilities along the ROW?)
6. Is anyone in charge of security planning at this point? If yes, who is that person and what is their function? If no, at what point do you expect to have someone in charge of security planning?
7. Does your organization expect to include security planning with its HSR plans? If yes, at what point will it be included? If no, why not?
8. Do you believe that HSR should follow or should not follow security policies similar to what the airlines practice? Or do you believe a hybrid policy would work better? What is your reasoning?
9. Do you wish to address anything we have not covered?

Appendix C

Larger View of Figure 6: Potential Tier Structure for Passenger Systems



(Note: Common corridor issues handled within ROW Safety Plan review)

Tier	0	IA	IB	IC	II	III	IV	V
Description	**Regional rail**	**Conventional**	**Emerging HSR**	**HSR Regional**	**HSR Mixed Operations**	**HSR Mixed Passenger**	**HSR Dedicated**	**HSR Express**
Speed Range mph	**0-65**	**0-79**	**0- 80/110**	**0- 111/125**	**0-126/150**	**0-150**	**0-150**	**0-200/220**
Other traffic on same track	None (or temporally separated)	Mixed passenger and freight	Mixed passenger and freight	Mixed passenger and freight	Mixed passenger and freight	Conventional passenger only	None	None
Track class	- Class 4	- Class 4	- Class 5/6	- Class 7	- Class 8	- Class 8	- Class 8	- Class 9
Signals, train control	Traffic control	PTC	PTC; vital and perimeter protection above 90	PTC; vital and perimeter protection above 90	Per IC and ROW safety strategy integrated			
Public highway-rail grade crossings	Automated warning; supplementary measures where warranted	Automated warning; supplementary measures where warranted	Sealed corridor; evaluate need for presence detection and PTC feedback	Barriers above 110, see §213.247; Presence detection tied to PTC above 110	See IC None above 125	See IC None above 125	None at any speed	None at any speed
Private highway-rail grade crossings	Automated warning or manually locked gate preferred; cross-buck and stop or yield sign where conditions permit		Automated warning or locked gate with signal interlock	None or as above	None above 125	None above 125	None at any speed	None at any speed
ROW safety plan	System Safety Program / Collision Hazard Analysis				SSP/CHA and specific approval process for new service similar to 236.361			
MOW safety management plan	Address within SSP framework; no separate approval required				Separate plan approval; integrate with SSP/CHA			
Equipment	CEM – end frame strength dynamic test	Present Tier I plus Cab End Frame Strength, or equivalent safety (including option for alternative to buff strength)			Present Tier II (including option for alternative to buff strength)	See Tier IA-C	Define	Define
Occupied car forward	OK	OK			Prohibited	Up to 125 mph only	OK	Prohibited
On-board emergency systems	Per Parts 238 and 239 (including glazing, emergency egress and rescue access, lighting, signage, etc.)							
System Safety Programs	Required; Review is for completeness; Audits for follow through				Integrate Subpart G, Part 238	Required; FRA reviews management decisions and may disapprove		

Bibliography

Bergen, Peter, and Hoffman, Bruce, *Assessing The Terrorist Threat: A Report Of The Bipartisan Policy Center's National Security Preparedness Group*, Bipartisan Policy Center, September 10, 2010

California High Speed Rail Blog, "Homeland Security Theater," April 16, 2011

Celona, Larry; Messing, Philip; Doyle, John, "Two tunnel security breaches cause scare in city," *New York Post*, May 9, 2011

Chang, Monica, "High-Speed Movement on Rail Security," ASMag.com, November 17, 2010

Department of Homeland Security, Transportation Security Administration, 49 CFR Parts 1520 and 1580 [Docket No. TSA-2006-26514; Amendment Nos. 1520-5, 1580-(New)] RIN 1652-AA51, Rail Transportation Security

Federal Bureau of Investigation and Department of Homeland Security Joint Intelligence Bulletin, *Early 2010 Al-Qa'ida Interest in Targeting Trains on 11 September 2011*, May 5, 2011

Gerstein, Josh, "Obama: No shoe checks on high-speed rail," *Politico*, January 28, 2010

Goetsch, Charlie, "New Regulations for Railroad Security to Kick In," *Train Law Blog*, February 17, 2009

Guerrero, Peter F., Director, Physical Infrastructure Issues; and Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, *"Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain,"* March 23, 2004

Hecker, JayEtta Z., Director of Physical Infrastructure Issues, *Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts*, Testimony on March 29, 2007

Higgins, Kelly Jackson, "Social Engineering Report Shows Corporate America At Risk," DarkReading.com, September 15, 2010

Interagency OPSEC Support Staff (IOSS), *Safe Social Networking*, www.ioss.gov

Jenkins, Brian Michael, and Butterworth, Bruce Robert, *Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute Report CA-MTI-10-2875, March 2010

Jenkins, Brian Michael; Butterworth, Bruce R.; Clair, Jean-François, *Off the Rails: The 1995 Attempted Derailing of the French TGV (High-Speed Train) and a Quantitative Analysis of 181 Rail Sabotage Attempts*, Mineta Transportation Institute report CA-MTI-10-2501, March 2010

Kissane, Dylan, *Terror on the TGV? The Terrorist Threat to France's High-Speed Rail Network,* presented at the Contemporary Challenges and Future Trends in International Security conference, American Graduate School of International Relations and Diplomacy, Paris, France, June 20-21, 2007

Lautenberg, Frank R., US Senator, D-NJ, news release "Lautenberg Calls Bin Laden Documents Targeting Rail a 'Wake Up Call,'" May 6, 2011

Markoff, John, "A Silent Attack, but Not a Subtle One," *New York Times*, September 27, 2010

McCarter, Mickey, "Homeland Security to launch rail security campaign," HSToday.com, June 30, 2010

Montalbano, Elizabeth, "DHS To Invest $40 Million On Cybersecurity Research," *InformationWeek*, February 1, 2011

Moore, Michael Scott, "High-Speed Rail's Weak Link Is Security," *Miller-McCune*, May 4, 2011

New Jersey Common Operating Picture (NJ COP), New Jersey Regional Operations Intelligence Center, February 22, 2011, Prepared by the NJ ROIC Analysis Element, Threat Analysis Program AE201102-200

Office of Intelligence and Analysis Assessment, *Threat Assessment: Mass Transit and Passenger Railroads*, June 29, 2010

Ortiz, David S.; Weatherford, Brian A.; Greenberg, Michael D.; Ecola, Liisa [sic], *Improving the Safety and Security of Freight and Passenger Rail in Pennsylvania*, RAND Corporation, 2008

Peoria Star Journal, "Our View: Rail safety must be larger priority for U.S." May 13, 2011

RAND Corporation, *Terrorists Can Think Strategically: Lessons Learned From the Mumbai Attacks*, Testimony presented before the Senate Homeland Security and Governmental Affairs Committee, January 28, 2009

Samuel, A., "European project aims to step up rail security," Rail.co article, May 5, 2011

Samuel, A., “Russian Railways step up security measures,” rail.co article, February 23, 2011

San Diego - Law Enforcement Coordination Center Intelligence Bulletin 11-009, May 4, 2011

Steen, Margaret, “Safeguarding the Rails: Four Avenues for Increasing Security,” *Emergency Management*, November 29, 2010

Transportation Security Administration, Office of Intelligence, *Freight Rail Threat Assessment, MTA-83409-(UFOUO)*, February 28, 2011

US DOT/FRA, *High-Speed Passenger Rail Safety Strategy*, November 2009

United States Government Accountability Office, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, Report to Congressional Requesters, September 2005

Wimmer, Bruce, CPP, Director of Global Consulting & Logistics, Pinkerton Consulting & Investigations seminar on Business Espionage in the 21st Century, San Mateo CA, March 10, 2011

Additional Reading

Kandek, Wolfgang, *The Inconvenient Truth About the State of Browser Security,* Qualys, Inc., presentation at RSA 2011 Conference

Rohlich, Nina; Haas, Peter; Edwards, Frances - *Exploring the Effectiveness of Transit Security Awareness Campaigns in the San Francisco Bay Area*, Mineta Transportation Institute, Research Report 09-19, June 2010

Stanke, Brian, *An Analysis of the French Urban Areas and Implications for the California Central Valley,* June 2009

United States, *High Speed Rail in the United States*, Congressional Research Service, December 8, 2010

United States, *High-Speed Passenger Rail Safety Strategy*, US DOT/FRA, November 2009

United States, *Vision for High-Speed Rail in America*, High-Speed Rail Strategic Plan, The American Recovery and Reinvestment Act, April 2009

Acronyms and Abbreviations

AAR – Association of American Railroads

AQ – Al Qaida or al-Qa'ida

BART – Bay Area Rapid Transit

BTP – British Transit Police

CCTV – Closed Circuit Television

CHSRA – California High-Speed Rail Authority

DHS – Department of Homeland Security

DHS/I&A – Department of Homeland Security Office of Intelligence and Analysis

DVR – Digital Video Recorder

FAQ – Frequently Asked Questions

FRA – Federal Railroad Authority

GAO – Government Accountability Office

HSR – High-Speed Rail

HSARPA - Homeland Security Advanced Research Projects Agency

IED – Improvised Explosive Devices

MBTA – Massachusetts Bay Transit Authority

MTI – Mineta Transportation Institute

NFPA – National Fire Protection Association

PATH – Port Authority Trans-Hudson

PTC – Positive Train Control

SWAT – Special Weapons and Tactics

TGV – *Train a grand vitesse* (French HSR)

TRB – Transportation Research Board

TSA – Transportation Security Administration

TSA-OI – Transportation Security Administration – Office of Inspection

U/FOUO – Unclassified/For Official Use Only

URL – Uniform Resource Locator

About the Author

Donna R. Maurillo is Director of Communications and Technology Transfer at the Mineta Transportation Institute. Previously, she held executive and management positions with Silicon Valley technology companies and public relations agencies. For 20 years, she operated a successful corporate communications consulting business.

Ms. Maurillo majored in French at St. John's Academy in Syracuse NY and earned her undergraduate degree in liberal arts from the University of California, Santa Cruz, where she delivered the commencement address. She co-authored two books on self-employment and has been a contributor to several newspapers and magazines. Her goal has been to earn her graduate degree before qualifying for full Social Security. She did it with a month to spare.