Homeland Security

Office of Intelligence and Analysis / Directorate for Preparedness

Homeland Infrastructure Threat
& Risk Analysis Center (HITRAC)

24 May 2006

(U) Distribution Notice: Requests for further dissemination must be approved by the DHS/Office of Intelligence & Analysis (I&A) – Production Management Division at IA.PM@hq.dhs.gov.

(U) Under the National Infrastructure Protection Plan, the Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) has the responsibility to produce assessments that support the strategic planning needed to enhance the protection and preparedness of the Nation's critical infrastructure and key resources. HITRAC analyzed information about terrorist goals, objectives, and attack capabilities to assess the potential terrorist attack profiles that might be used against each sector.

Strategic Sector Assessment

(U//FOUO) The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System

(U) Attention: Federal Departments and Agencies, State Homeland Security Advisors, Emergency Managers, Tribal Government, State & Local Law Enforcement, and Information Sharing and Analysis Centers.

*(U) **Warning**: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.*

(U) This product contains U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label ^{USPER} and should be handled in accordance with the recipient's intelligence oversight or information handling procedures. Other USPER information has been minimized. Should you require the minimized USPER information, please contact the DHS/I&A Production Management Division at IA.PM@hq.dhs.gov.

(U) Scope

(U) This Strategic Sector Assessment is one in a series that provides an overall assessment of the potential terrorist threats to critical infrastructure and key resources, and provides decision makers with the broad, analytically-based threat information necessary to inform strategic investment priorities and program design. It also provides the overarching analytic foundation for incident reports and threat warnings produced by the Department of Homeland Security (DHS) and other Federal partners. This assessment was prepared with input from the Federal infrastructure partners and the private sector.

HITRAC

(U) Key Findings

(U//FOUO) DHS has no credible or specific intelligence regarding imminent attacks against the commercial passenger and freight rail sectors in the United States. Previous reporting on al-Qa'ida, combined with the March 2004 Madrid commuter train bombings and the July 2005 bombings on the London public transit system, however, demonstrate the intent and capability of al-Qa'ida, and its affiliated groups and sympathizers, to attack these transportation systems.

— ***(U//FOUO) The U.S. commercial passenger and freight rail systems are vulnerable to terrorist attack because of their public accessibility and the difficulty in securing a vast array of railroad assets.***

— ***(U//FOUO) Passenger trains and stations are especially attractive terrorist targets because of the large number of people in a concentrated area. A terrorist attack against freight rail would require more complex planning, timing, and execution to cause high casualties or costly economic damage.***

*(U) **Photos**: (L to R): London Subway; Graniteville, South Carolina; Madrid Commuter Train*

— ***(U//FOUO) Terrorists' effective use of improvised explosive devices (IEDs) in rail attacks elsewhere in the world suggests that this method is preferred and poses the greatest threat to U.S. rails, although DHS cannot discount the possible use of chemical, biological, or radiological attacks.***

(U//FOUO) Steps the industry has taken since the September 2001 attacks have improved rail security, but additional measures are needed, including larger numbers of security personnel and greater use of technological tools.

(U) Threat Overview

(U//FOUO) Al-Qa‘ida and Affiliated Groups Remain the Greatest Threat to U.S. Commercial Passenger and Freight Rail

(U//FOUO) The most likely targets considered by al-Qa‘ida or affiliated extremists are passenger trains loaded to capacity during peak ridership periods, underwater rail tunnels, and heavily used stations in large metropolitan areas. Within the United States, heavily used stations include Pennsylvania Station (hereafter referred to as Penn Station) and Grand Central Station in New York, and Union Station in Washington, D.C. Union Station is not the most heavily trafficked station in the United States, but its location within the National Capitol Region provides an important symbolic motivation for terrorists.

(U//FOUO) Following the March 2004 bombing of commuter trains in Madrid, Spain, foreign terrorists expressed a strong interest in attacking passenger trains in the United States. The terrorists specifically were interested in striking an above-ground passenger train traveling between two major cities, and considered New York City and Washington, D.C., as possible targets. The ultimate target selection would depend on detailed surveys and surveillance reports by the designated operatives, who have not been found. The identification of operatives who could actually travel to Western countries to perpetrate the attacks was a main problem for the terrorists. Numerous methods were considered for attacking trains, to include derailment, explosions with gas canisters, igniting fires, and ramming a vehicle into a train. The preferred method was to cause a powerful explosion from inside a rail passenger car.

— (U//FOUO) Terrorists considered a variety of techniques for obtaining and using explosives. The terrorists believed it would be easier to manufacture or buy explosives in the United States than to smuggle them into the country. Possible explosive mixtures would include ingredients such as acetone, aluminum powder, fertilizer, nitric acid, peroxide, petroleum jelly, and yellow sulfur. The manufactured explosives would have to fit inside backpacks or carry-on items similar to those used in the London and Madrid attacks.

— (U//FOUO) The terrorists did not believe it was necessary to inflict massive casualties through train attacks. Rather, their goal would be to create many explosions in many different trains in order to terrify the ridership and consequently adversely affect the U.S. economy. A train attack was the preferred type of attack in the United States because it was the easiest to conduct and would not require significant time to plan and prepare.

(U//FOUO) A review of all-source reporting reveals that 57 actual or possible threats to the U.S. rail system were reported since January 2004, ranging from threats to blow up identified trains or train stations to general threats against unspecified trains and stations. Included in these threats are nine incidents involving explosive devices placed on or near railroad tracks. The majority of reported threats were made against subways or mass transit systems nationwide, and at least 10 involved identified Amtrak^USPER trains and stations. Most of the threats to date can be attributed to factors other than terrorism, such as criminal sabotage, vandalism, tampering with and theft of railroad equipment, and intentional harassment, all of which are common in the rail industry. These incidents are not considered credible indicators of al-Qa‘ida or affiliated extremists' capabilities to conduct attacks.

(U) Other Domestic Threats

(U//FOUO) Domestic political, criminal, and terrorist groups present a limited threat to rail targets in the United States. According to the FBI, special interest extremism has increased. For example, the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF) have used crude incendiary devices and large-scale incendiary attacks. These groups have targeted the auto, fur, and timber industries—including bombing work sites and auto dealerships on at least three occasions. These groups may consider freight rail that moves goods such as sport utility vehicles and lumber as possible targets, although there is no reporting to date to suggest that attacks are either imminent or planned.

(U//FOUO) Members in criminal gangs such as the Mara Salvatrucha (MS-13) and Mara-Mexicana have reportedly discussed bombing subways, light rails, and streetcars in San Francisco. DHS has no separate reporting to corroborate these claims regarding alleged criminal gangs and potential mass transit attacks, and views such reports with skepticism.

(U//FOUO) Right-wing extremist members of the Georgia Republic Militia^USPER were convicted in 1996 of possession of explosive devices, illegal weapons, and conspiracy related to their threat to attack infrastructure such as bridges.

(U) U.S. Commercial Passenger and Freight Rail System Overview

(U) Commercial Passenger Rail

(U//FOUO) U.S. commercial passenger rail systems operate on an open interstate system and on the same tracks as freight rail companies. Commercial passenger rail systems include Amtrak, Virginia Railway Express (VRE),^USPER Maryland Rail Commuter (MARC),^USPER the Long Island Railroad (LIRR),^USPER the Southern California Regional Rail Authority,^USPER and the Alaska Railroad (AKRR).^USPER Amtrak operates more than 22,000 miles of track, and serves approximately 24 million people annually at more than 500 station stops. The vast majority of the 22,000 miles on which Amtrak operates are owned by freight railroads. Amtrak owns approximately 750 miles of railroad, primarily from Boston to Washington, D.C.

(U) Freight Rail

(U//FOUO) Freight railroads are critical to the economic well-being and global competitiveness of the United States. As an indispensable part of our nation's transportation system, the country's 550 common carrier freight railroads serve nearly every industrial, wholesale, retail, and resource-based sector of the U.S. economy. They move 42 percent of our nation's freight (measured in ton-miles)—from raw materials to sophisticated finished products—and connect businesses with each other across the country and with markets overseas. Freight railroads are overwhelmingly private property, and billions of dollars are spent each year building and maintaining their rights-of-way. Freight railroads also contribute billions of dollars each year to the economy through investments, wages, purchases, and taxes.

(U) Likely Attack Methods

(U//FOUO) Passenger Trains Are the Most Likely Target of a Terrorist Rail Attack

(U//FOUO) The most likely target for a terrorist attack against the U.S. rail industry probably would be commercial passenger or mass transit trains. A terrorist attack against the freight rail system is possible, but less likely because it would require more complex planning and execution to achieve substantial casualties or economic damage. Railroads already deal with derailments, equipment malfunctions, deliberate acts of sabotage, and weather-related damage with no perceived long-term effects to the freight rail industry.

(U//FOUO) IEDs Appear to Be the Terrorists' Weapon of Choice and the Greatest Threat to Rail

(U//FOUO) The effective use of IEDs in the majority of attacks against various rail targets worldwide demonstrates the intent, capability, and success of various terrorist groups in attacking passenger rail systems. IEDs will likely remain the preferred method of attack against rail assets because they can be constructed from common materials, contained in inconspicuous bags or packages, and carried or placed without attracting attention. The use of vehicle-borne improvised explosive devices (VBIEDs) is another method that can be used to attack rail assets. The following are worldwide examples of recent attacks against rail targets using IEDs:

— (U//FOUO) **July 2005:** Four suicide bombers detonated explosives contained in backpacks on three London underground trains and one London bus.

— (U//FOUO) **August 2004:** A suspected Chechen suicide bomber detonated a shrapnel-filled IED at a metro entrance in Moscow.

- (U//FOUO) **March 2004:** Islamic extremists placed 13 remotely-detonated IEDs (10 of which exploded) on four commuter trains in Madrid.

- (U//FOUO) **February 2004:** A suspected Chechen suicide bomber detonated an IED on a metro train in Moscow, causing a fire that spread to other cars.

- (U//FOUO) **December 2003:** A suspected Chechen suicide bomber detonated a shrapnel-filled IED on a passenger train in the Republic of Chechnya, Russia.

- (U//FOUO) **September 2001:** A HAMAS suicide bomber detonated his explosives as passengers exited a train station in Nahariya, Israel.

- (U//FOUO) **July 2001:** An Islamic Jihad suicide bomber detonated his explosives near the train station in Binyamina, Israel.

- (U//FOUO) **December 2000:** Members of the al-Qa‘ida-affiliated Philippine terrorist organization Abu Sayyaf Group detonated five bombs on the Manila Light Railway Transit station, and a passenger bus in Manila, Philippines.

(U//FOUO) ***Photos**: Detonating IEDs such as these is one method terrorists could employ to attack a crowded train or train station.*

(U) Sabotage and Insider Attacks

(U//FOUO) Among the various threats to the U.S. rail system, the most difficult to predict and prevent is the industry insider who can use unique knowledge and access to sabotage rail operations. Approximately 3,300 trains accidentally derail in the United States every year; however, intentional derailments are not common.

(U) Cyber Attacks

(U//FOUO) Cyber attacks, also known as computer network attacks, against the U.S. rail industry pose a potentially critical threat, given the dependence of the rail industry on automated control networks, information systems, and telecommunications. The disruption resulting from a cyber attack on control networks, such as Supervisory Control and Data Acquisition (SCADA) systems, which are generally used to automate control processes, could lead to costly power outages, equipment damage, or interruption of safety-related equipment. The U.S. Department of Transportation requirements and railroad regulations require back-up procedures to maintain safety of operations in the event of a power failure or signal outage. Cyber attacks do not generally produce casualties or achieve spectacular results, but a successful cyber attack would likely undermine public confidence in infrastructure safeguards.

(U//FOUO) Terrorist Attacks to Take Over a Train

(U//FOUO) A terrorist takeover of a passenger or freight train to seize hostages or drive the train into derailment is probably less likely than an explosive attack.

- (U//FOUO) Hostage-taking would be unlikely to have the disruptive or spectacular effect that terrorists typically seek to achieve and would not cause the high number of casualties or create the level of panic and fear among rail passengers that occurred as a result of the London and Madrid train bombings. An attack of this type would require a longer time to plan, practice, and conduct.

- (U//FOUO) Because of controls built into the rail system, no one individual can commandeer a train and drive it to the location of his or her choosing. Track availability and routing are controlled by central dispatching stations, making it impossible to manually re-route these trains from the engine. In the event of an unplanned acceleration or other deviation in operation, control center personnel can re-direct trains onto potentially less hazardous lines, such as those outside urban areas.

(U) Maritime or Riverine Attacks

(U//FOUO) Maritime and riverine terrorist attacks against U.S. rail systems are of low probability because of the difficulty in planning and timing an operation large enough to cause significant casualties or to damage the economy. Methods of attack could include a rocket or automatic weapons attack from a moving or stationary vessel, or ramming a barge or large vessel into a railroad bridge to cause a derailment. Signal systems now in place will alert engineers and stop train movements before entering onto a damaged bridge.

(U) Chemical, Biological, or Radiological Attacks

(U//FOUO) Terrorists show continuing interest in ***toxic chemical dispersion devices,*** given the relative ease with which toxic materials can be acquired or produced, the potential for large numbers of casualties, disruptions at the scene of the event, and psychological impact on the population. Improvised chemical attacks against the U.S. passenger rail systems pose a serious threat, as evidenced by the liquid sarin attack on the Tokyo subway system carried out by the Japanese religious cult Aum Shinrikyo in March 1995 that killed twelve passengers.

(U//FOUO) Aum Shinrikyo also was responsible for an ***attempted biological attack*** in March 1995 in the Tokyo subway system involving three briefcases left in the Kasumigaseki train station. Although no injuries resulted, an Aum Shinrikyo member later confessed this was a failed biological attack involving the use of botulinum toxin.

(U//FOUO) A ***radiological attack*** against a rail target could be conducted by exploding a radiological dispersal device close to unshielded individuals, rolling stock, and other rail equipment.

(U) Hazardous Material Attacks

(U//FOUO) U.S. freight trains carry more than 1 million tons of hazardous chemicals daily, 50 percent of the nation's total. The vast majority of these chemicals, if released, will not cause mass casualties. A number of chemicals, however, can be fatal if inhaled. Nonetheless, an attack to release hazardous material (HAZMAT) as a weapon would be difficult for terrorists to execute and probably would not produce the desired effect, given the number of variables such as wind speed and direction, train timetables, and the capability of railroad HAZMAT teams to control and contain the effects of a release rapidly.

(U) Toxic Inhalation Hazard Chemicals: A Rail Transportation Concern

(U//FOUO) Of all toxic inhalation hazard (TIH) chemicals, chlorine is of greatest concern to the freight rail industry, because of the high number of chlorine-filled tank cars on the nation's tracks each day, and due to the high demand and criticality of chlorine in water purification and other commercial uses.

(U) Demolition or Sabotage of Rail Bridges and Tunnels

(U//FOUO) The destruction or sabotage of rail bridges and tunnels is another possible method of terrorist attack against the U.S. rail system. Tens of thousands of rail bridges throughout the country vary widely in design, from reinforced wooden bridges to heavy steel trestle bridges. The simple sabotage of the rails on a bridge can cause a derailment, the momentum of which could force the engine and at least some of the cars to drop from the bridge. Demolition or sabotage of rail tunnels may increase casualties when they involve hazardous materials or are under water.

(U//FOUO) The al-Qa'ida Training Manual states, " … by using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."

(U) Other Factors Affecting Rail Security

(U//FOUO) Possible Terrorist Exploitation of Open-Source Rail Information

(U//FOUO) Information available on corporate Web sites could be used to facilitate terrorist operational planning. All seven major passenger and freight rail companies using the U.S. rail systems have posted detailed information regarding routes, rail lines, ports, hubs, and other commercial data on their public Web sites. Passenger schedules also are posted as a matter of necessity. Terrorists can legally, and with little fear of detection, find out from these sites when a given passenger train is departing or arriving at a specific station.

— (U//FOUO) Since 11 September 2001, freight train schedules are no longer posted on public Web sites, and public Web sites do not contain specific information about the types of cargo being transported, or their specific departure or arrival times. Tracking information is often available, however, with a secure password and logon.

(U) Trainspotters and Railfans

(U//FOUO) Another area of consideration for rail security is the tens of thousands of hobbyists—“trainspotters” or “railfans”—who photograph and discuss passenger and freight rails for their personal interest. Trainspotters regularly visit rail stations, bridges, rail yards, and other facilities to photograph and document trains. This information frequently is shared on Internet Web sites, and is available for public viewing. The following types of information on passenger and freight systems gathered by trainspotters and posted to the Internet could be used for terrorist operational planning:

— (U) Photographs of engines and cars, including chemical cars.

— (U) Details of train routes and schedules.

— (U) Radio frequencies for specific rail lines and dispatchers.

— (U) Details of rail bends and tunnels.

— (U) Web cams (real-time video feeds) of stations and rail lines.

— (U) Live audio feeds of train communications.

— (U) Details about rail communications equipment, such as engine radios, ground stations, and towers.

(U//FOUO) Suspicious Activity In and Around Rail Infrastructure

(U//FOUO) Since the terrorist attacks of 11 September 2001, numerous reports of suspicious incidents on the rail systems in major cities such as Chicago, New York, and Washington have been called in to local police departments and government agencies daily. Some reports involve individuals who may appear to be acting suspiciously or asking suspicious questions, while many others involve suspicious packages and possible surveillance, including photographing and videotaping of trains and train stations. Some of the reported activity could be part of pre-operational terrorist planning or attempts to assess the type and timing of responses by authorities. Nonetheless, there is no corroborating intelligence to link these events to actual operational planning against the U.S. rail systems.

(U//FOUO) Obvious Vulnerabilities May Create Targeting Opportunities

(U//FOUO) The ***large number of railroad assets,*** including rail passenger and freight cars, train stations and depots, bridges, tunnels, and thousands of miles of unprotected tracks, offer many targeting opportunities for terrorists. The vast infrastructure, however, also provides redundancy and rerouting capabilities that can mitigate the threat and limit the effectiveness of attacks.

(U//FOUO) Passenger rail systems have ***open and multiple access points*** and, in some cases, have no barriers in loading and unloading areas. These access points, which allow for easy passenger movement, make it difficult for security personnel to screen and detect potential terrorists. Commercial rail and mass transit passengers are not screened as they enter and leave trains or train stations, making it easy to carry out an attack using tactics such as detonating remote-controlled or timed explosive devices or using suicide bombers.

(U//FOUO) The entry and exit locations of ***enclosed stations*** are vulnerable to chemical/biological agent dispersion attacks because the systems have limited intake and exhaust stacks.

(U//FOUO) A ***high volume of ridership*** in densely populated areas makes passenger trains and mass transit an appealing target for terrorists because of the potential for high numbers of casualties and media coverage. The large number of people present in trains and train stations makes it difficult to closely monitor packages, briefcases, and suitcases that could contain weapons or IEDs. Rail operators are training employees and educating passengers on how to identify and report suspicious items and activity. Evacuation and rescue operations are especially challenging for attacks occurring during peak hours in transit tunnels, subways, on bridges, and on elevated structures; however, rail operators have procedures in place to respond to such emergencies, whether intentional or accidental, and routinely exercise those capabilities.

(U//FOUO) ***Central command and control centers*** serve as the coordination points from which various aspects of the rail system, such as signaling, switching, and communications, are controlled. Loss of a central command and control center could slow down a rail system, forcing it to operate under its backup manual procedures.

(U//FOUO) ***Rail systems are generally lightly protected*** and have limited monitoring favoring openness and convenience. The multiple entrances and exits of trains and train stations are typically unsupervised and lack camera surveillance, making it easier for individuals to maintain anonymity. Many rail systems have their own police force and engineering crews that monitor the trains, stations, and tracks; however, the small size of these units limits their ability to provide protection.

(U//FOUO) Commercial passenger ***rail schedules are predictable and announced in advance to the general public*** in many forms. Paper and electronic route maps, schedules, and timetables could aid terrorists in the planning, rehearsal, and execution of an attack.

(U//FOUO) Rail industry ***vehicles and equipment are exposed to the public,*** making them vulnerable to tampering or sabotage.

(U//FOUO) Many ***commuter trains share rail lines with freight carriers,*** making them vulnerable if an attack occurred against a freight train carrying hazardous or flammable material. Some rail systems run along or near streets, highways, and other critical infrastructure, making them vulnerable to attack from these vantage points. Additionally, rail assets could suffer collateral damage if these other infrastructure elements were attacked.

(U) Consequences Overview

(U//FOUO) High Potential Consequences of an Attack Against Commercial Passenger or Freight Rail

(U//FOUO) Along with the casualties that could result from an attack on U.S. rail systems, the resulting loss or disruption of services could have escalating economic and social consequences. Loss of passenger rail services could also substantially reduce a region's evacuation capability.

(U//FOUO) U.S. commercial passenger and freight rail lines are often collocated and interdependent with other key infrastructures and resources such as electricity, water, telecommunications, and commercial facilities. A strike against the rail infrastructure could damage other sectors by cutting cabling, pipes, and other critical infrastructures that share common tunnels, bridges, and rights-of-way.

(U//FOUO) Commercial passenger and mass transit systems also provide service to critical infrastructures such as government facilities, the defense industrial base, and monuments and icons, enabling a terrorist attack to have cross-sector economic impact. The shutdown of such rail systems could reduce business and government operations in the systems' service area.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF) and the Homeland Security Operations Center (HSOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the HSOC can be reached by telephone at 202-282-8101 or by email at HSOC.Common@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached by telephone at 202-282-9201 or by email at NICC@dhs.gov. Each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, when this information is available, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document, please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) Tracked by:

(U) HSEC-010000-01-05
(U) HSEC-010200-01-05
(U) HSEC-020300-01-05
(U) TERR-010000-01-05
(U) TERR-010200-01-05
(U) TERR-020000-01-05
(U) TERR-020500-01-05
(U) TERR-020600-01-05
(U) TERR-040900-01-05
(U) TERR-050000-01-05
(U) TERR-050300-01-05
(U) TERR-060000-01-05
(U) TERR-060200-01-05