United States Government Accountability Office

GAO

Report to Congressional Committees

July 2010

TECHNOLOGY ASSESSMENT

Explosives Detection Technologies to Protect Passenger Rail

GAO
Accountability * Integrity * Reliability

GAO-10-898

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-898, a report to congressional committees

July 2010

TECHNOLOGY ASSESSMENT

Explosives Detection Technologies to Protect Passenger Rail

Why GAO Did This Study

Passenger rail systems are vital to the nation's transportation infrastructure, providing approximately 14 million passenger trips each weekday. Recent terrorist attacks on these systems around the world—such as in Moscow, Russia in 2010—highlight the vulnerability of these systems. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary federal entity responsible for securing passenger rail systems.

In response to the Legislative Branch Appropriations Act for fiscal year 2008, GAO conducted a technology assessment that reviews 1) the availability of explosives detection technologies and their ability to help secure the passenger rail environment, and 2) key operational and policy factors that impact the role of explosives detection technologies in the passenger rail environment. GAO analyzed test reports on various explosives detection technologies and convened a panel of experts comprised of a broad mix of federal, technology, and passenger rail industry officials. GAO also interviewed officials from DHS and the Departments of Defense, Energy, Transportation, and Justice to discuss the effectiveness of these technologies and their applicability to passenger rail. GAO provided a draft of this report these departments for comment. Four departments provided technical comments, which we incorporated as appropriate.

View GAO-10-898 or key components.
For more information, contact Nabajyoti Barkakati at (202) 512-4499 or BarkakatiN@gao.gov or David Maurer at (202) 512-9627 or MaurerD@gao.gov.

What GAO Found

A variety of explosives detection technologies are available or in development that could help secure passenger rail systems. While these technologies show promise in certain environments, their potential limitations in the rail environment need to be considered and their use tailored to individual rail systems. The established technologies, such as handheld, desktop, and kit-based trace detection systems, and x-ray imaging systems, as well as canines, have demonstrated good detection capability with many conventional explosive threats and some are in use in passenger rail today. Newer technologies, such as explosive trace portals, advanced imaging technology, and standoff detection systems, while available, are in various stages of maturity and more operational experience would be required to determine their likely performance if deployed in passenger rail. When deploying any of these technologies to secure passenger rail, it is important to take into account the inherent limitations of the underlying technologies as well as other considerations such as screening throughput, mobility, and durability, and physical space limitations in stations.

GAO is not making recommendations, but is raising various policy considerations. For example, in addition to how well technologies detect explosives, GAO's work, in consultation with rail and technology experts, identified several key operational and policy considerations impacting the role that these technologies can play in securing the passenger rail environment. Specifically, while there is a shared responsibility for securing the passenger rail environment, the federal government, including TSA, and passenger rail operators have differing roles, which could complicate decisions to fund and implement explosives detection technologies. For example, TSA provides guidance and some funding for passenger rail security, but rail operators themselves provide day-to-day-security of their systems. In addition, risk management principles could be used to guide decision-making related to technology and other security measures and target limited resources to those areas at greatest risk. Moreover, securing passenger rail involves multiple security measures, with explosives detection technologies just one of several components that policymakers can consider as part of the overall security environment. Furthermore, developing a concept of operations for using these technologies and responding to threats that they may identify would help balance security with the need to maintain the efficient and free flowing movement of people. A concept of operations could include a response plan for how rail employees should react to an alarm when a particular technology detects an explosive. Lastly, in determining whether and how to implement these technologies, federal agencies and rail operators will likely be confronted with challenges related to the costs and potential privacy and legal implications of using explosives detection technologies.

Contents

Abbreviations

AFP	amplifying fluorescent polymer
AIT	Advanced Imaging Technology
ANFO	ammonium nitrate/fuel oil
APTA	American Public Transportation Association
AT	Advanced Technology
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
ATSA	Aviation and Transportation Security Act of 2001
CCTV	closed circuit television
CONOPS	concept of operations
CT	computed tomography
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EDC	explosives detection canine
ETP	explosive trace portal
FEMA	Federal Emergency Management Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GHz	gigahertz
HME	homemade explosives
HMTD	hexamethylene triperoxide diamine
HMX	octahydrotetranitrotetrazine
HSIN	Homeland Security Information Network
IED	improvised explosive device
IMS	ion mobility spectrometry
JIEDDO	Joint Improvised Explosive Device Defeat Organization
LANL	Los Alamos National Laboratory
MARC	Maryland Area Regional Commuter
MS	mass spectrometry
NEDCTP	National Explosives Detection Canine Team Program
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
NRC	National Research Council
NSTS	National Strategy for Transportation Security
PATH	Port Authority Trans-Hudson
PETN	pentaerythritol tetranitrate
QPL	Qualified Products List
RDX	cyclotrimethylene trinitramine
S&T	Science and Technology Directorate

SEMTAP	Security and Emergency Management Technical Assistance Program
SNL	Sandia National Laboratories
TATP	Triacetone triperoxide
THz	terahertz
TNT	trinitrotoluene
TSA	Transportation Security Administration
TS-SSP	Transportation Systems-Sector Specific Plan
TSGP	Transit Security Grant Program
TSWG	Technical Support Working Group
VIPR	Visible Intermodal Prevention and Response

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 28, 2010

The Honorable Ben Nelson
Chairman
The Honorable Lisa Murkowski
Ranking Member
Subcommittee on Legislative Branch
Committee on Appropriations
United States Senate

The Honorable Debbie Wasserman Schultz
Chairman
The Honorable Robert B. Aderholt
Ranking Member
Subcommittee on Legislative Branch
Committee on Appropriations
House of Representatives

Passenger rail systems are vital components of the nation's transportation infrastructure, encompassing rail transit (heavy rail, commuter rail, and light rail), and intercity rail.[1] In the United States, passenger rail systems provide approximately 14 million passenger trips each weekday, and commuters rely on these systems to provide efficient, reliable, and safe transportation.[2] Terrorist attacks on passenger rail systems around the world—such as the March 2010 Moscow, Russia subway bombings, and the July 2006 passenger train bombing in Mumbai, India that resulted in

[1]Passenger rail systems consist of various passenger rail transit systems. Transit rail is comprised of heavy, commuter, and light rail systems. Heavy rail is an electric railway that can carry a heavy volume of traffic, and is characterized by high speed and rapid acceleration, passenger rail cars operating singly or in multi-car trains on fixed rails, separate rights of way from which all other vehicular and foot traffic is excluded, sophisticated signaling, and high-platform loading. Most subway systems are considered heavy rail. Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service, such as between a central city and its adjacent suburbs. Light rail systems typically operate passenger rail cars singly (or in short, usually two-car trains) and are driven electrically with power being drawn from an overhead electric line.

[2]The American Public Transportation Association compiled this ridership data from the Federal Transit Administration's National Transit Database. Ridership on rail transit systems in the District of Columbia and Puerto Rico are included in these statistics. A passenger trip is defined as the number of passengers who board public transportation vehicles. Passengers are counted each time they board vehicles no matter how many vehicles they use to travel from their origin to their destination.

209 fatalities—highlight the vulnerability of these systems. Additionally, the administration's Transborder Security Interagency Policy Committee, Surface Transportation Subcommittee's recently issued Surface Transportation Security Priority Assessment stated that the nation's transportation network was at an elevated risk of attack and that recent plots against passenger rail highlight the lengths terrorists will go to defeat security measures put in place after September 11, 2001.[3] Another threat facing passenger rail systems are chemical and biological weapons. While there have been no terrorist attacks against U.S. passenger rail systems to date, the systems are vulnerable to attack in part because they rely on an open architecture that is difficult to monitor and secure due to its multiple access points, hubs serving multiple carriers, and, in some cases, no barriers to access. Further, an attack on these systems could potentially lead to casualties due to the high number of daily passengers, especially during peak commuting hours, and result in serious economic disruption and psychological impact.

Day-to-day responsibility for securing passenger rail systems falls on passenger rail operators, local law enforcement, and state and local governments that own portions of the infrastructure. While several entities play a role in helping to fund and secure U.S. passenger rail systems, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary federal agency responsible for overseeing security for these systems and for developing a national strategy and implementing programs to enhance their security. The Department of Transportation's (DOT) Federal Transit Administration (FTA) and Federal Railroad Administration (FRA) also provide support to rail operators by providing technical assistance in conducting threat and vulnerability assessments and developing and providing training courses for rail operators. Additionally, several other DHS components conduct threat and vulnerability assessments of passenger rail systems, research and develop security technologies for these systems, and develop security training programs for passenger rail employees. We have previously reported, most recently in June 2009, on federal and industry efforts to secure passenger rail systems and have made recommendations for

[3]The White House Transborder Security Interagency Policy Committee Surface Transportation Subcommittee, *Surface Transportation Security Priority Assessment* (March 2010). In making its recommendations, the subcommittee gathered input from surface-transportation owners and operators, the Department of Homeland Security and the Department of Transportation, as well as state and local government representatives.

strengthening these efforts.[4] DHS generally agreed with these recommendations and is taking action to implement them.

A variety of security measures, including technological measures, have been and are being considered by federal policymakers and rail operators as part of a layered approach to strengthening the security of passenger rail systems, particularly in the area of protecting against the threat of explosives. Explosives detection technologies have been tested and implemented for screening passengers and baggage in aviation and building security. Further, the U.S. military uses some of these technologies to, among other things, detect the presence of improvised explosive devices (IED) in Iraq and Afghanistan.[5] However, these technologies have been tested and implemented less frequently in passenger rail systems. This is due in part to the open nature of passenger rail systems, which does not lend itself to people and baggage screening. Also, there is relatively less funding available to support the purchase and maintenance of such equipment compared to the funding available for commercial aviation security in which the federal government plays a larger role. Because of the potential impact of implementation of explosives detection technology on the open nature of passenger rail systems, weighing rail operator needs and technological effectiveness of explosives detection technology against the relative costs and impact on rail operations is important. Additionally, because these explosives detection technologies tend to be expensive, rail operators may look to other funding sources, such as the federal government, to assist in implementing these technologies.

In the Senate report accompanying the proposed bill for the legislative branch fiscal year 2008 appropriation, the Senate Committee on Appropriations recommended the establishment of a permanent technology assessment function within GAO.[6] In the 2008 Consolidated

[4] GAO, *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, But Opportunities Exist to Strengthen Federal Strategy and Programs*, GAO-09-678 (Washington, D.C: June 2009) and *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington, D.C.: September 2005).

[5] An IED is a device fabricated in an improvised manner that incorporates in its design explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals. It can be carried by an individual or deposited in an unnoticed location for detonation by a timer or remote control.

[6] S. Rep. No. 110-89, at 42-43 (2007).

Appropriations Act, Congress authorized GAO to use up to $2.5 million of amounts appropriated for salaries and expenses for technology assessment studies.[7] After consultation with congressional committees, GAO agreed to conduct a technology assessment on the use of explosives detection technologies to secure passenger rail systems. Specifically, this report addresses the following questions:

1. What is the availability of explosives detection technologies and what is their ability to help secure the passenger rail environment?
2. What key operational and policy factors could have an impact on the role of explosives detection technologies in the passenger rail environment?

This report is a public version of the restricted report (GAO-10-590SU) that we provided to you on May 28, 2010. DHS deemed some of the information in the restricted report as sensitive security information, which must be protected from public disclosure. Therefore, this report omits this information. Although the information provided in this report is more limited in scope, it addresses the same questions as the restricted report. Also, the overall methodology used for both reports is the same.

To determine what explosives detection technologies are available and their ability to help secure the passenger rail environment, we met with experts and officials on explosives detection research, development, and testing, and reviewed test, evaluation, and pilot reports and other documentation from DHS's Science and Technology Directorate, including the Transportation Security Laboratory; TSA; several Department of Defense (DOD) components, including the Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV), the Technical Support Working Group (TSWG), and the Joint Improvised Explosive Device Defeat Organization (JIEDDO); several Department of Energy (DOE) National Laboratories involved in explosives detection testing, research, and development including Los Alamos National Laboratory (LANL), Sandia National Laboratories (SNL), and Oak Ridge National Laboratory (ORNL); and the Department of Justice (DOJ) because of its expertise in explosives detection. We also observed a TSA pilot test of a standoff explosives detection system at a rail station within the Port Authority Trans-Hudson passenger rail system. In addition, we interviewed several

[7] Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, div. H, tit. I, 121 Stat. 1844, 2249 (Dec. 26, 2007).

manufacturers of explosives detection technologies and attended government-sponsored demonstrations, a conference, and an academic workshop on explosives detection technologies. We also interviewed government officials involved with securing passenger rail in the United Kingdom. We visited six domestic passenger rail locations, two of which were involved in testing various types of explosives detection technologies to either observe the testing or discuss the results of these tests with operators. The specific locations we visited are listed in appendix I.

In determining which explosives detection technologies were available and able to secure the passenger rail environment, we considered those technologies available today or deployable within 5 years, technologies which could be used to screen either passengers or their carry-on items, and technologies which were safe to use when deployed in public areas. In determining the capabilities and limitations of explosives detection technologies we evaluated their detection and screening throughput performance, reliability, availability, cost, operational specifications, and possible use in passenger rail. We also restricted our evaluation to those technologies which have been demonstrated to detect explosives when tested against performance parameters as established by government and military users of the technologies.

We also obtained the views of various experts and stakeholders during a panel discussion we convened with the assistance of the National Research Council (NRC) in August 2009 (hereafter referred to as the expert panel). Panel attendees included 23 experts and officials from academia, the federal government, domestic and foreign passenger rail industry organizations, technology manufacturers, national laboratories, and passenger rail industry stakeholders such as local law enforcement officials and domestic and foreign passenger rail operators. During this meeting, we discussed the availability and applicability of explosives detection technologies for the passenger rail environment and the operational and policy impacts associated with implementing these technologies in the rail environment. While the views expressed during this panel are not generalizable across all fields represented by officials in attendance, they did provide an overall summary of the current availability and effectiveness of explosives detection technologies and industry views on their applicability to passenger rail.

To determine what key operational and policy factors could have an impact in determining the role of explosives detection technologies in the passenger rail environment, we reviewed documentation related to the federal strategy for securing passenger rail, including TSA's Mass Transit

Modal Annex to the Transportation Systems Sector Specific Plan, and other documentation, including DHS reports summarizing explosives detection technology tests conducted in passenger rail to better understand the role and impact that these technologies have in the passenger rail environment.[8] We reviewed relevant laws and regulations governing the security of the transportation sector as a whole and passenger rail specifically, including the Implementing Recommendations of the 9/11 Commission Act.[9] We also reviewed our prior reports on passenger rail security and studies and reports conducted by outside organizations related to passenger rail or the use of technology to secure passenger rail, such as the National Academies, Congressional Research Service, and others to better understand the existing security measures used in passenger rail and operational and policy issues. During our interviews and expert panel mentioned above, we also discussed and identified officials' views related to the key operational and policy issues of using explosives detection technologies to secure passenger rail. While these views are not generalizeable to all industries represented by these officials, they provided a snapshot of the key operational and policy views.

During our visits to 6 rail operator locations involved in explosives detection testing, we interviewed officials regarding operational and policy issues related to technology and observed passenger rail operations. We selected these locations because they had completed or were currently conducting testing of the use of explosives detection technology in the rail environment and to provide the views of a cross-section of heavy rail, commuter rail, and light rail operators. While these locations and officials' views are not generalizeable to the entire passenger rail industry, they provided us with a general understanding of the operational and policy issues associated with using such technologies in the rail environment. In addition, we utilized information obtained and presented in our June 2009 report on passenger rail security.[10] For that work, we conducted site visits, or interviewed security and management officials from 30 passenger rail agencies across the United States and met with officials from two regional transit authorities and Amtrak. The passenger rail operators we visited or interviewed for our June 2009 report represented 75 percent of the

[8]The Transportation Systems Sector Specific Plan documents the processes to be used in carrying out the national strategic priorities related to securing the U.S. transportation system.

[9]Pub. L. No. 110-53, 121 Stat. 266 (Aug. 3, 2007).

[10]GAO-09-678.

nation's total passenger rail ridership based on the information we obtained from the FTA's National Transit Database and the American Public Transportation Association. For additional information on our scope and methodology please see appendix I.

We conducted our work from August 2008 through July 2010 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to Technology Assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

Background

Overview of the U.S. Passenger Rail System

Passenger rail systems provided 10.7 billion passenger trips in the United States in 2008.[11] The nation's passenger rail systems include all services designed to transport customers on local and regional routes, such as heavy rail, commuter rail, and light rail services. Heavy rail systems—subway systems like New York City's transit system and Washington, D.C.'s Metro—typically operate on fixed rail lines within a metropolitan area and have the capacity for a heavy volume of traffic. Commuter rail systems typically operate on railroad tracks and provide regional service (e.g., between a central city and adjacent suburbs). Light rail systems are typically characterized by lightweight passenger rail cars that operate on track that is not separated from vehicular traffic for much of the way. All types of passenger rail systems in the United States are typically owned and operated by public sector entities, such as state and regional transportation authorities.

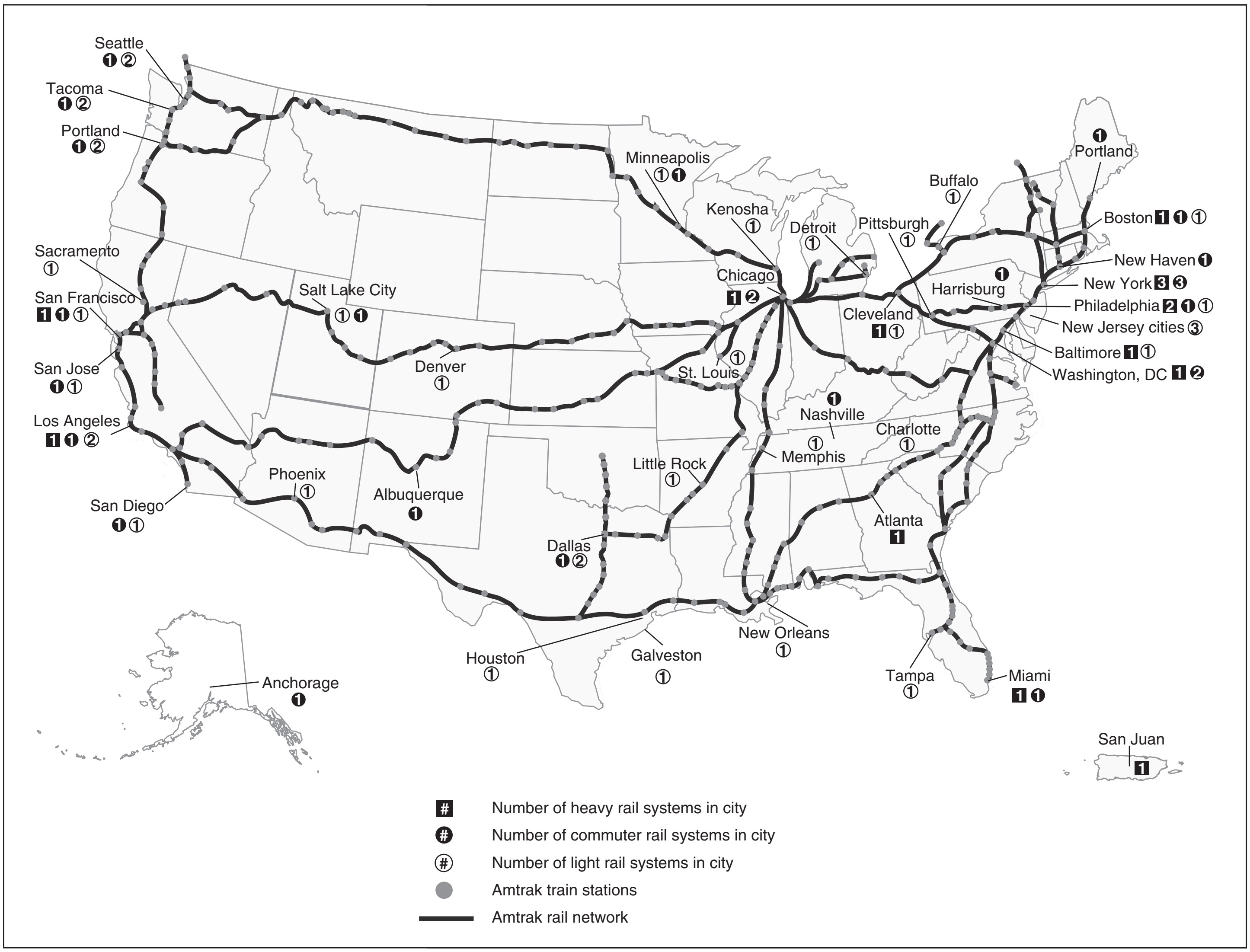
Amtrak, which provided more than 27 million passenger trips in fiscal year 2009, operates the nation's primary intercity passenger rail and serves more than 500 stations in 46 states and the District of Columbia.[12] Amtrak operates a more than 22,000 mile network, primarily over leased freight

[11]Ridership data reported by the American Public Transportation Association for 2008.

[12]The Alaska Railroad Corporation also operates intercity passenger rail service. Amtrak's ridership data comes from the 2007 Amtrak Environmental Health and Safety Report.

railroad tracks. In addition to leased tracks, Amtrak owns about 650 miles of track, primarily on the “Northeast Corridor” between Boston and Washington D.C., which carries about two-thirds of Amtrak’s total ridership. Stations are owned by Amtrak, freight carriers, municipalities, and private entities. Amtrak also operates commuter rail services in certain jurisdictions on behalf of state and regional transportation authorities. Figure 1 identifies the geographic location of passenger rail systems and Amtrak within the United States as of January 1, 2010.

Figure 1: Geographic Distribution of Passenger Rail Systems and Amtrak in the United States

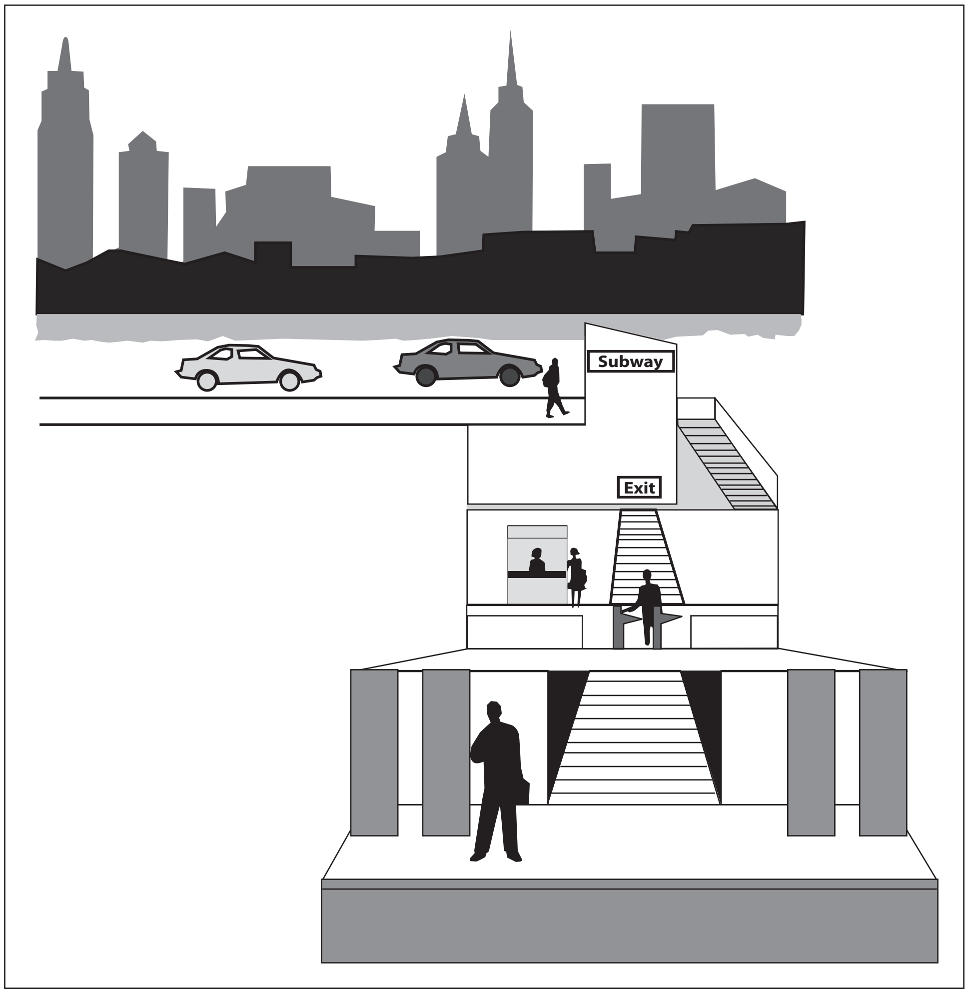


Source: Amtrak, National Transit Database, and APTA; Map Resources (map).

Passenger rail operators that we spoke to and that attended our expert panel indicated that rail stations in the United States generally fall into one of three categories:

- Heavy rail station. These stations are generally heavily traveled—serving thousands of passengers during rush hours—and are located in major metropolitan areas. They are usually space constrained and located either underground or on an elevated platform and serviced by heavy rail. Entry to the stations is usually controlled by turnstiles and other chokepoints. Many of the subway stations in New York City and elevated stations in Chicago are examples of these types of stations. See figure 2 for an example of a typical heavy rail station.

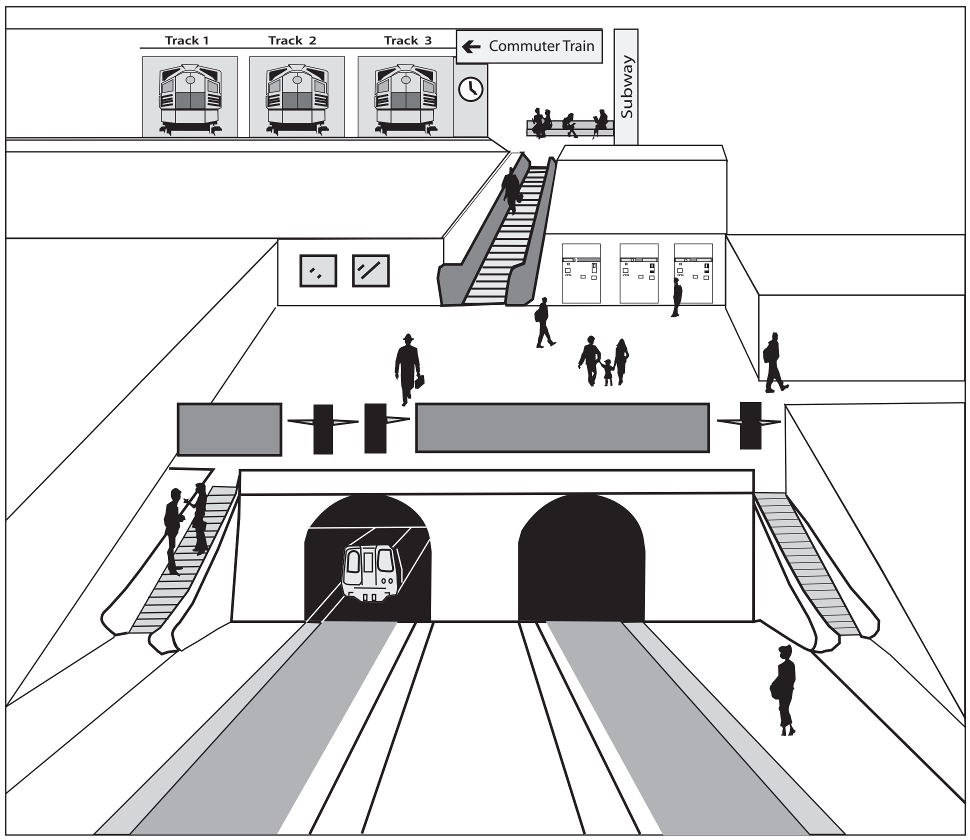
Figure 2: Example of Typical Metropolitan Heavy Rail Station



Source: GAO.

- Large intermodal station. These stations are also heavily traveled and service multiple types of rail including heavy rail, commuter rail, and intercity passenger rail (such as Amtrak). These stations are usually not as space constrained and access is usually restricted either by turnstiles or naturally occurring chokepoints, such as escalators or doorways leading to rail platforms. Examples of these types of stations include Union Station in Washington, D.C. See figure 3 for an example of a typical large intermodal station.

Figure 3: Typical Large Intermodal Passenger Rail Station

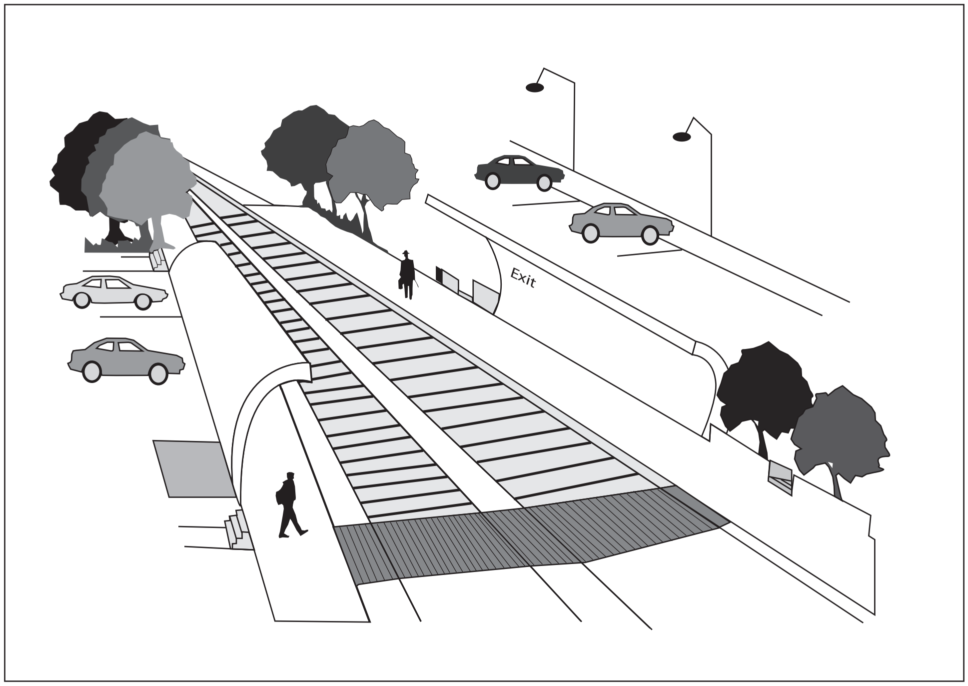


Source: GAO.

- Commuter or light rail station. These stations are open and access is generally not constrained by turnstiles and other chokepoints. These stations are usually served by commuter rail systems in suburban or rural areas outside of a metropolitan area or in the case of light rail may be located physically on the city's streets with no access barriers between the city and the station stop. The stations are easily accessible, not usually space constrained, and are often located outdoors. Examples of this type of station include Virginia Railway Express commuter stations in suburban

Virginia and the Maryland Area Regional Commuter (MARC) stations in Maryland. See figure 4 for an example of a commuter or light rail station.

Figure 4: Example of a Typical Outdoor Commuter or Light Rail Station



Source: GAO.

Passenger Rail Systems Are Inherently Difficult to Secure and Vulnerable to Terrorist Attacks, Particularly Against the Threat From Explosives

To date, U.S. passenger rail systems have not been attacked by terrorists. However, according to DHS, terrorists' effective use of IEDs in rail attacks elsewhere in the world suggests that IEDs pose the greatest threat to U.S. rail systems. Rail systems in the United States have also received heightened attention as several alleged terrorists' plots have been uncovered, including multiple plots against systems in the New York City area. Worldwide, passenger rail systems have been the frequent target of terrorist attacks. According to the Worldwide Incidents Tracking System maintained by the National Counter Terrorism Center, from January 2004 through July 2008 there were 530 terrorist attacks worldwide against passenger rail targets, resulting in more than 2,000 deaths and more than 9,000 injuries. Terrorist attacks include a 2007 attack on a passenger train in India (68 fatalities and more than 13 injuries); 2005 attack on London's underground rail and bus systems (52 fatalities and more than 700 injuries); and 2004 attack on commuter rail trains in Madrid, Spain (191 fatalities and more than 1,800 injuries). More recently, in January 2008, Spanish authorities arrested 14 suspected terrorists who were allegedly connected to a plot to conduct terrorist attacks in Spain, Portugal, Germany, and the United Kingdom, including an attack on the Barcelona metro. The most common means of attack against passenger rail targets has been through the use of IEDs, including attacks delivered by suicide bombers.

According to passenger rail operators, the openness of passenger rail systems can leave them vulnerable to terrorist attack. Further, other characteristics of passenger rail systems—high ridership, expensive infrastructure, economic importance, and location in large metropolitan areas or tourist destinations—make them attractive targets for terrorists because of the potential for mass casualties, economic damage, and disruption. Moreover, these characteristics make passenger rail systems difficult to secure. In addition, the multiple access points along extended routes make the costs of securing each location prohibitive. Balancing the potential economic impacts of security enhancements with the benefits of such measures is a difficult challenge.

Multiple Stakeholders Share Responsibility for Securing Passenger Rail Systems

Securing the nation's passenger rail systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and passengers who ride these systems. Since the September 11, 2001, terrorist attacks, the role of the federal government in securing the nation's transportation systems has evolved. In response to attacks, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and conferred to the agency broad responsibility for overseeing the security of all modes of transportation, including passenger rail.[13] Congress passed the Homeland Security Act of 2002, which established DHS, transferred TSA from DOT to DHS, and assigned DHS responsibility for protecting the nation from terrorism, including securing the nation's transportation systems.[14] TSA is supported in its efforts to secure passenger rail by other DHS entities such as the National Protection and Programs Directorate (NPPD) and Federal Emergency Management Administration's (FEMA) Grant Programs Directorate and Planning and Assistance Branch. NPPD is responsible for coordinating efforts to protect the nation's most critical assets across all

[13]Pub. L. No. 107-71, 115 Stat. 597 (Nov. 19, 2001).

[14]Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).

18 industry sectors, including transportation.[15] FEMA's Grant Programs Directorate is responsible for managing DHS grants for mass transit. FEMA's Planning and Assistance Branch is responsible for assisting transit agencies with conducting risk assessments.

While TSA is the lead federal agency for overseeing the security of all transportation modes, DOT continues to play a supporting role in securing passenger rail systems. In a 2004 Memorandum of Understanding and a 2005 annex to the Memorandum, TSA, and FTA agreed that the two agencies would coordinate their programs and services, with FTA providing technical assistance and assisting DHS with implementation of its security policies, including collaborating in developing regulations affecting transportation security. In addition to FTA, Federal Railroad Administration (FRA) also has regulatory authority over commuter rail operators and Amtrak and employs over 400 inspectors who periodically monitor the implementation of safety and security plans at these systems. FRA regulations require railroads that operate intercity or commuter passenger train service or that host the operation of that service adopt and comply with a written emergency preparedness plan approved by FRA.[16]

In August 2007, the Implementing Recommendations of the 9/11 Commission Act was signed into law, which included provisions that require TSA to take certain actions to secure passenger rail systems.[17] Among other items, these provisions include mandates for developing and issuing reports on TSA's strategy for securing public transportation, conducting and updating security assessments of mass transit systems, and establishing a program for conducting security exercises for rail operators. The 9/11 Commission Act includes requirements for TSA to increase the number of explosives detection canine teams and required

[15]The 18 industry sectors include agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear, postal and shipping, public health and healthcare, transportation, and water.

[16]FRA regulations define emergency to include a security-related incident, such as a bomb threat, among other things. Each plan must address, for example, employee training and qualification and coordination with emergency responders. Also, each covered railroad must conduct full-scale passenger train emergency simulations in order to determine its capability to execute the emergency preparedness plan.

[17] Pub. L. No. 110-53, 121 Stat. 266 (Aug. 3, 2007).

DHS to carry out a research and development program to secure passenger rail systems.

State and local governments, passenger rail operators, and private industry are also stakeholders in the nation's passenger rail security efforts. State and local governments might own or operate portions of passenger rail systems. Consequently, the responsibility for responding to emergencies involving systems that run through their jurisdictions often falls to state and local governments. Although all levels of government are involved in passenger rail security, the primary responsibility for securing the systems rests with the passenger rail operators. These operators, which can be public or private entities, are responsible for administering and managing system activities and services, including security. Operators can directly operate the security service provided or contract for all or part of the total service. For example, the Washington Metropolitan Area Transit Authority operates its own police force.

Federal and Industry Stakeholders Have Taken Actions to Secure Passenger Rail Systems

Federal stakeholders have taken actions to help secure passenger rail. For example, in November 2008, TSA published a final rule that requires passenger rail systems to appoint a security coordinator and report potential threats and significant security concerns to TSA.[18] In addition, TSA developed the Transportation Systems-Sector Specific Plan (TS-SSP) in 2007 to document the process to be used in carrying out the national strategic priorities outlined in the National Infrastructure Protection Plan (NIPP) and the National Strategy for Transportation Security (NSTS).[19] The TS-SSP contains supporting modal implementation plans for each transportation mode, including mass transit and passenger rail. The Mass Transit Modal Annex provides TSA's overall strategy and goals for securing passenger rail and mass transit, and identifies specific efforts TSA is taking to strengthen security in this area.[20]

DHS also provides funding to passenger rail operators for security, including purchasing and installing security technologies, through the

[18] 73 Fed. Reg. 72,130 (Nov. 26, 2008).

[19] The NSTS, mandated in the Intelligence Reform and Terrorism Prevention Act of 2004, outlines the federal government approach—in partnership with state, local, and tribal governments and private industry—to secure the U.S. transportation system from terrorist threats and attacks.

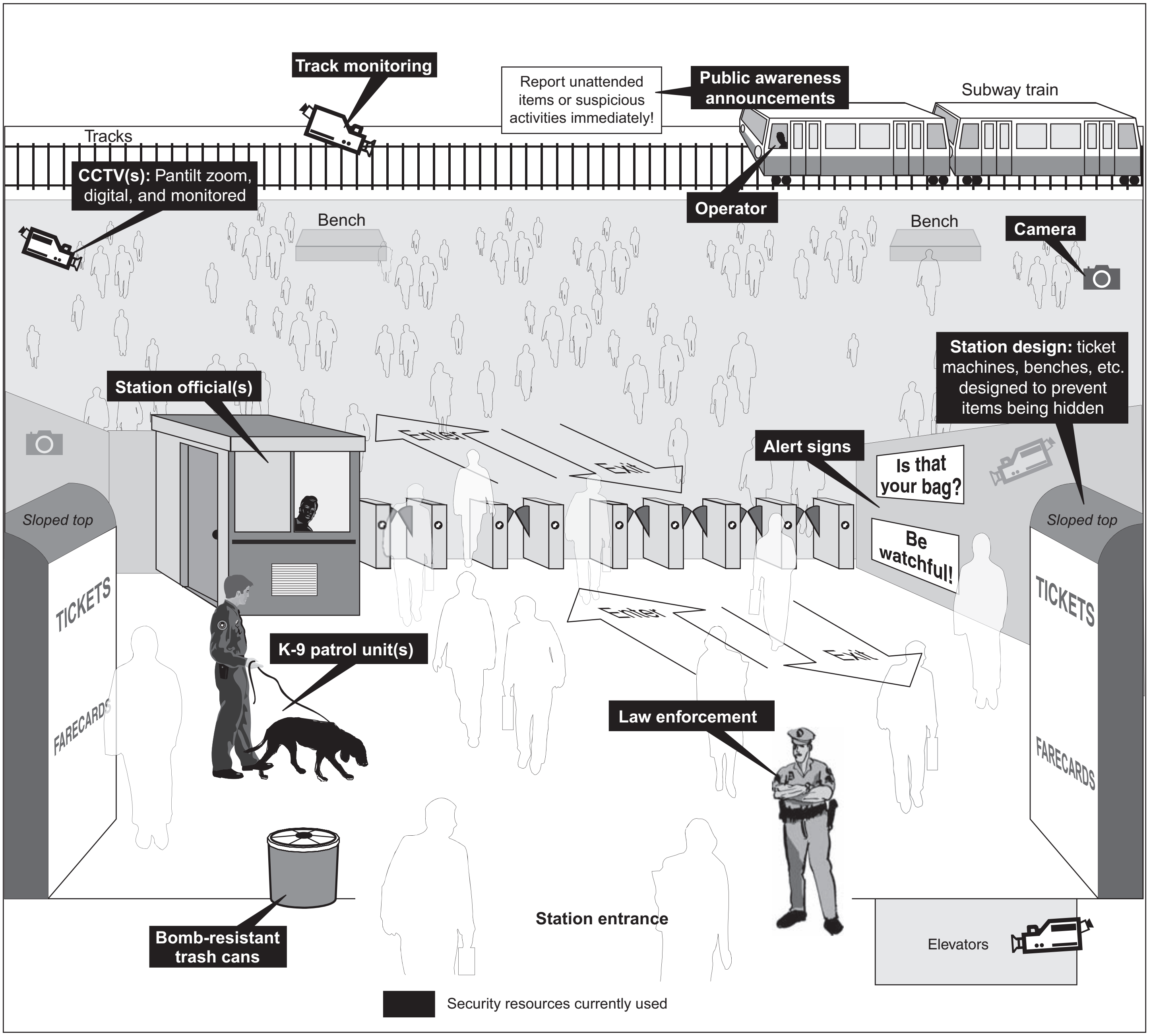
[20] DHS updated the NIPP in 2009.

Transit Security Grant Program (TSGP). We reported in June 2009 that from fiscal years 2006 through 2008, DHS provided about $755 million dollars to mass transit and passenger rail operators through the TSGP to protect these systems and the public from terrorist attacks.[21] Passenger rail operators with whom we spoke and that attended our expert panel said that they used these funds to acquire security assets including explosives detection canines, handheld explosives detectors, closed circuit television (CCTV) systems, and other security measures.

Passenger rail operators have also taken actions to secure their systems. In September 2005, we reported that all 32 U.S. rail operators that we interviewed or visited had taken actions to improve the security and safety of their rail systems by, among other things, conducting customer awareness campaigns; increasing the number and visibility of security personnel; increasing the use of canine teams, employee training, passenger and baggage screening practices, and CCTV and video analytics; and strengthening rail system design and configuration. Passenger rail operators stated that security-related spending by rail operators was based in part on budgetary considerations, as well as other practices used by other rail operators that were identified through direct contact or during industry association meetings. According to the American Public Transportation Association (APTA), in 2005, 54 percent of passenger rail operators faced increasing deficits, and no operator covered expenses with fare revenue; thus, balancing operational and capital improvements with security-related investments has been an ongoing challenge for these operators. Figure 5 provides a composite of selected security practices used in the passenger rail environment.

[21] GAO, *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO-09-491 (Washington, D.C.: June 8, 2009).

Figure 5: Selected Security Practices in the Passenger Rail Environment



Source: GAO and NOVA Development Corporation.

Types and Characteristics of Explosives and IEDs

Countering the explosives threat to passenger rail is a difficult challenge as there are many types of explosives and different forms of bombs. The many different types of explosives are loosely categorized as military, commercial, and a third category called homemade explosives (HME) because they can be constructed with unsophisticated techniques from everyday materials. The military explosives include, among others, the high explosives PETN and RDX, and the plastic explosives C-4 and Semtex.[22] The military uses these materials for a variety of purposes, such as the explosive component of land mines, shells, or warheads. They also have commercial uses such as for demolition, oil well perforation, and as the explosive filler of detonation cords. Military explosives can only be purchased domestically by legitimate buyers[23] through explosives distributors and typically terrorists have to resort to stealing or smuggling to acquire them. RDX was used in the Mumbai passenger rail bombings of July 2006. PETN was used by Richard Reid, the “shoe bomber” in his 2001 attempt to blow up an aircraft over the Atlantic Ocean, and was also a component involved in the attempted bombing incident on board Northwest Airline Flight 253 over Detroit on Christmas Day 2009.

Commercial explosives, with the exception of black and smokeless powders, also can only be purchased domestically by legitimate buyers through explosives distributors. These are often used in construction or mining activities and include, among others, trinitrotoluene (TNT), ammonium nitrate and aluminum powder, ammonium nitrate and fuel oil (ANFO), black powder,[24] dynamite, nitroglycerin, smokeless powder,[25] and urea nitrate. Dynamite was likely used in the 2004 Madrid train station bombings, as well as the Sandy Springs, Georgia abortion clinic bombing in January, 1997. ANFO was the explosive used in the Oklahoma City, Oklahoma bombings in 1995.

[22]PETN is pentaerythritol tetranitrate. RDX is the explosive cyclotrimethylene trinitramine, also known as cyclonite. These can be used separately or combined with binders and other agents to form, for example, the hand-moldable plastic explosives, C-4 and Semtex. RDX is the main ingredient of C-4. Semtex contains both PETN and RDX.

[23]Legitimate buyers are licensed or permitted possessors of explosives.

[24]Black powder, also called gunpowder, is a mixture of sulfur, charcoal, and potassium nitrate. It is the main ingredient found in fireworks. In the past it was used as a propellant powder in ammunition.

[25]Smokeless powder is not an explosive but rather a flammable solid that burns very rapidly and is mainly used as a propellant in modern ammunitions.

The common commercial and military explosives contain various forms of nitrogen. The presence of nitrogen is often exploited by detection technologies some of which look specifically for nitrogen (nitro or nitrate groups) in determining if a threat object is an explosive.

HMEs, on the other hand, can be created using household equipment and ingredients readily available at common stores and do not necessarily contain the familiar components of conventional explosives. On February 22, 2010, Najibullah Zazi pleaded guilty to, among other things, planning to use TATP[26] to attack the New York City subway system. Also, HMEs using TATP and concentrated hydrogen peroxide, for example, were used in the July 2005 London railway bombing. TATP can be synthesized from hydrogen peroxide, a strong acid such as sulfuric acid, and acetone, a chemical available in hardware stores and found in nail polish remover, and HMTD[27] can be synthesized from hydrogen peroxide, a weak acid such as citric acid, and hexamine solid fuel tablets such as those used to fuel some types of camp stoves and that can be purchased in many outdoor recreational stores. ANFO is sometimes misrepresented as a homemade explosive since both of its constituent parts—ammonium nitrate, a fertilizer, and fuel oil—are commonly available.

When used, for example, in terrorist bombings, explosives are only one component of an IED. Explosive systems are typically composed of a control system, a detonator, a booster, and a main charge. The control system is usually more mechanical or electrical in nature. The detonator usually contains a small quantity of a primary or extremely sensitive explosive. The booster and main charges are usually secondary explosives which will not detonate without a strong shock, for example from a detonator. IEDs will also have some type of packaging or, in the case of suicide bombers, some type of harness or belt to attach the IED to the body. Often, an IED will also contain packs of metal—such as nails, bolts, or screws—or nonmetallic material which are intended to act as shrapnel or fragmentation, increasing the IED's lethality. The various components of an IED—and not just the explosive itself—can also be the object of detection.

The initiation hardware, which may be composed of wires, switches, and batteries, sets off the primary charge in the detonator which, in turn,

[26]TATP is triacetone triperoxide and its usual form is a white powder.

[27]HMTD is hexamethylene tripreoxide diamine and its usual form is a white powder.

provides the shock necessary to detonate the main charge. The primary charge and the main charge are often different types and categories of explosives. For example, in the attempted shoe bombing incident in 2001, the detonator was a common fuse and paper-wrapped TATP, while PETN was the main charge. While in the past the initiation hardware of many IEDs contained power supplies, switches, and detonators, certain of the newer HMEs do not require an electrical detonator but can be initiated by an open flame.

A Variety of Explosives Detection Technologies Are Available or in Development That Could Help Secure Passenger Rail Systems—If Tailored to the Needs of Individual Rail Systems—but Limitations Exist

Several different types of explosives detection technologies could be applied to help secure passenger rail, although operational constraints of rail exist that would be important considerations. For example, handheld, desktop, and kit explosives detection systems are portable and already in use in the passenger rail environment. Carry-on item explosives detection technologies are mature and can be effective in detecting some explosive devices. Explosive Trace Portals generally use the same underlying technology as handheld and desktop systems, and have been deployed in aviation with limited success. Advanced Imaging Technology (AIT) portals are becoming available but, as with trace portals, will likely have only limited applicability in passenger rail. Standoff detection technologies promise a detection capability without impeding the flow of passengers, but have several limitations. Canines are currently used in passenger rail systems, generally accepted by the public, and effective at detecting many types of explosives. Limitations in these technologies restrict their more widespread or more effective use in passenger rail and include limited screening throughput and mobility, potential issues with environmental conditions, and the openness and physical space restrictions of many rail stations.[28]

[28] Certain details regarding the ability of particular technologies to detect explosives and any limitations in their ability to detect certain types of explosives were deleted because DHS considered them to be Sensitive Security Information.

Various Explosives Detection Technologies Could be Applied to Help Secure Passenger Rail Systems If Operational Constraints of Rail are Effectively Considered

In the passenger rail environment detection of explosives involves the screening of people and their carry-on baggage. The different types of explosives detection technology available to address these screening needs can be divided into two basic categories. There are those based on imaging methods, sometimes called bulk detection, and those that are based on trace detection methods. The goal in bulk detection is to identify any suspicious indication—an anomaly—in a bag or on a person that might potentially be a bomb. These systems, while they may be used to detect explosive material, are also often used to detect other parts of a bomb. Although some automated detection assistance is usually included, imaging based detection systems currently depend heavily on trained operators in identifying the anomalies indicative of a bomb.

Trace detection technologies, on the other hand, involve taking a physical sample from a likely source and then analyzing it with any one of several different techniques for the presence of trace particles of explosive material.[29] Importantly, a positive detection does not necessarily indicate the presence of a bomb because the trace particles may just be contamination from someone having handled or having been near explosives material. Explosives trace detection systems can often identify the individual type of explosives trace particles present.

Bulk and trace detection technology generally serve different functions and can sometimes be paired to provide a more complete screening of a person and their belongings. Typically that screening occurs in two stages. First, an initial screening is done to separate suspicious persons or carry-on baggage from the rest of the passenger flow quickly. In almost all cases, any anomalies detected in initial screening will trigger the need for a person or baggage to undergo a secondary inspection, via different methods, and typically aside from the main screening flow to confirm or dismiss the anomaly as a threat.[30] Technology need not be used in either inspection stage. For example, behavioral assessment is sometimes used to provide an initial screening. In addition, secondary inspection can be a physical pat-down of a person or hand inspection of carry-on baggage although explosives detection technology can also be used. Screening can

[29]Trace particles are microscopic particles not visible to the naked eye. Existing explosives trace detectors can detect on the order of 10 nanograms of explosive trace material, which is 1,000 times smaller than what is typically considered to be the least visible amount.

[30]A familiar implementation of this two stage process is the primary and secondary inspection layers used in airport security checkpoints.

be done on 100 percent of passengers or on a subset of passengers chosen at random or by some selection method.

Different types of bulk and trace explosives detection technology have been developed over the years to handle both the screening of people and the screening of carry-on baggage. Generally, equipment falls into certain typical configurations—handheld, desktop, kit-based systems, carry-on baggage inspection systems, explosive trace portals, AIT portals, standoff detection systems, and explosives detection canines.[31] Certain equipment has been designed for the screening of people, some for the screening of carry-on baggage, and some equipment can be used for both. (See figure 6.)

[31]While canines are not a technology per se, they have been included in this assessment because of their widespread use for explosives detection.

Figure 6: Explosives Detection Technologies Used to Screen People and Their Carry-On Baggage

Configuration		Can be used to check for explosives on people	Can be used to check for explosives in carry-on baggage	Description
Handheld explosives detectors Source: Naval Explosive Ordnance Disposal Technology Division.		✓	✓	Portable devices for detecting traces of explosives
Desktop explosives detectors Source: Naval Explosive Ordnance Disposal Technology Division.		✓	✓	Desktop devices for detecting traces of explosives
Kit based explosives detectors Source: American Innovations, Inc., XD-2i Explosives Detector.		✓	✓	Portable devices for detecting traces of explosives
Carry-on baggage detection systems Source: Department of Transportation.			✓	X-ray based devices that look inside carry-on items to help the operator identify the presence of suspect items, such as explosives
Explosive trace portals Source: GAO.		✓		Walk-through devices for detecting traces of explosives on people

Figure 6: continued.

Configuration		Can be used to check for explosives on people	Can be used to check for explosives in carry-on baggage	Description
Advanced imaging technology portals Source: DHS Science and Technology Directorate.		✓		Walk-through devices that are used to look for hidden objects on people
Standoff detection systems Source: GAO.		✓		Detection systems that can be used to look for hidden objects on people
Explosives detection canines Source: DHS Science and Technology Directorate.		✓	✓	Dogs which have been trained to detect certain explosives

To be effective, equipment in each of these configurations is generally evaluated across several different technical characteristics. The first important technical characteristic of an explosives detection system is how good it is at detecting a threat. Several different parameters are considered to fully express a system's ability to detect a threat. They are used to express how often the system gets the detection right, and how often—and in which ways—it gets the detection wrong. The system can get the detection right when it alarms in the presence of a threat and the percentage of times it does under a given set of conditions is called the probability of detection.

However, other important parameters measure the percentage of times the system gets the detection wrong. This can occur in two ways. First, the system can alarm even though a threat is not present. This is called a false positive and the percentage of times it occurs in a given number of trials is called the false positive rate. It is also called the false alarm rate or probability of false alarm. Second, the system can fail to alarm even though a threat is present. This is called a false negative and the percentage of times it occurs in a given number of trials is called the false negative rate.

A second key technical characteristic for explosives detection systems is screening throughput, which is a measure of how fast a person or item can be processed through the system before the system is ready to accept another person or item. Screening throughput is an important characteristic to know because it directly impacts passenger delay, an important consideration when using technology in passenger rail. The higher the throughput, the less delay is imposed on passenger flow.

Other important technical characteristics to consider when assessing applicability of explosives detection systems for use in passenger rail are the system's size and weight, which will impact its mobility, the physical space needed to operate the system, and the system's susceptibility to harsh environmental conditions. Understanding the system's cost is also important.

Handheld, Desktop, and Kit Explosives Detection Systems

Handheld, desktop, and kit explosives detection systems are portable systems that are designed to detect traces of explosive particles. They have been shown to detect many explosive substances and are already used in passenger rail environments today, generally in support of secondary screening or in a confirmatory role when the presence of explosives or their trace particles are suspected.

In a typical usage with handheld and desktop systems, a sample of trace particles is collected by wiping a surface with a swab or other collection device designed for use with the system.[32] The sample is transferred into the system and typically heated to vaporize the trace particles, which are then drawn into the detector where they are analyzed for the presence of

[32]In addition to trace particles, there may also be minute amounts of explosive substances naturally vaporized and aloft in the atmosphere near the compound. However, most conventional explosives have very low vapor pressures and, hence, do not produce much vaporized particles at their surface and therefore, the primary sampling source is trace particles. For sample collection, some handheld detectors also have a vacuum collection system.

substances indicative of explosives. The results of sample analysis are typically displayed on a readout screen.

Handheld and desktop systems encompass a variety of detection techniques to analyze the sample and determine if it contains particles of explosive compounds. The various underlying techniques include ion mobility spectrometry (IMS), amplifying fluorescent polymer (AFP), chemiluminescence, and colorimetric. Many handheld and desktop systems are generally based on IMS technology, a mature and well-understood method of chemical analysis. This technique consists of ionizing the sample vapors and then measuring the mobility of the ions as they drift in an electric field. Each sample ion possesses a unique mobility—based on its mass, size, and shape—which allows for its identification.[33]

The AFP technique utilizes compounds that fluoresce when exposed to ultraviolet light. However, the fluorescence intensity decreases in the presence of vapors of certain nitrogen-containing explosives, such as TNT. Detection methods based on this principle look for a decrease in intensity that is indicative of specific explosives. AFP has been shown to have a high level of sensitivity to TNT. The chemiluminiscence principle is based on the detection of light emissions coming from nitro[34] groups that are found in many conventional military and commercial explosives such as TNT, RDX, PETN, black powder, and smokeless powder. However, chemiluminiscence by itself cannot identify any specific explosives because these nitro compounds are present not only in a number of commercial and military explosives, but also in many nonexplosive substances such as fertilizers and some perfumes. Therefore, this technique is often used in conjunction with other techniques, such as gas chromatography,[35] to positively identify specific explosives.

[33] Details regarding the ability of IMS technologies to detect explosives were deleted because DHS considered them to be Sensitive Security Information.

[34] Many conventional explosive compounds contain either nitro (NO2) or nitrate (NO3) groups.

[35] Gas chromatography (GC) is a technique used to separate various molecular species in a gaseous mixture. It consists of a hollow tube or column that is usually packed with beads. The gaseous mixture is made to pass through this column where various molecules interact differently with the beads causing them to exit the GC column at various times thereby resulting in the separation of individual gaseous species. A GC is used at the front end of an IMS or mass spectrometry trace detector to improve its detection effectiveness.

Kit-based explosives detection systems generally use colorimetric techniques. In this method, the detection is based on the fact that a specific compound, when treated by an appropriate color reagent,[36] produces a color that is characteristic of this compound. The sample is taken by swiping the target object, typically with a paper, and then the colorimetric reagents are applied by spraying or dropping them on the paper. The operator deposits chemical reagents in a series and observes color changes with each reagent added. This process of adding reagents is stopped when a visible color change is observed by the operator. The operator decides whether there are any trace explosives present by visually matching the color change observed to a standardized sheet of colors.

Table 1 describes some of the trace explosives detection methods described above.

Table 1: Some Trace Explosives Detection Methods

Trace explosives detection method	Operating principles
Ion mobility spectrometry	Based on ionizing the sample and measuring its mobility. In general heavier ions move slowly and lighter ones move relatively fast.
Amplifying fluorescent polymer	Detection is based on a reduction in fluorescent intensity of AFP in the presence of certain explosives.
Chemiluminescence	Based on detection of light emissions coming from nitro groups that are found in many conventional explosives.
Colorimetric Techniques	Various colorimetric reagents are applied to a sample in a predetermined sequence. The operator observes color changes with each reagent added that is indicative of an explosive.

Source: GAO analysis of Naval Explosive Ordnance Disposal Technology Division and other data.

In comparative studies over the last 8 years, the Naval Explosive Ordinance Disposal Technology Division showed that IMS-based handheld and desktop systems are capable of detecting many conventional military and commercial explosives that are nitrogen-based, such as TNT, PETN, and RDX. Non-IMS based techniques such as amplifying fluorescent polymer and chemiluminescence based techniques are able to additionally

[36]A reagent is a chemical agent or a substance or compound that is added to a system in order to bring about a chemical reaction or is added to see if a reaction occurs. Such a reaction is used to confirm the presence of another substance.

detect ANFO, smokeless powder, and urea nitrate. However, a report sponsored by DOD's Technical Support Working Group shows that most of these systems had difficulty in detecting certain other types of explosives.[37]

Preliminary results from an ongoing comparative study of kit-based detection systems sponsored by the Transportation Security Laboratory have shown that these systems can detect the presence of nitrogen when there is sufficient quantity of explosive sample (in small-bulk[38] or visible amounts) available for analysis. For example, kit-based systems were able to correctly identify the presence of nitrogen in a variety of different threat materials.[39] Additionally, kit-based systems have been shown to be susceptible to false alarms when challenged with substances such as soaps and perfumes, among others.

The open and often dirty air environment of passenger rail presents certain operational issues for trace detection. However, durable versions of handheld and desktop detectors are starting to appear for use in the open and rugged field environment. This is meant to improve the instruments' reliability, availability, and performance in an environment that has varying degrees of temperature, pressure, and humidity. In 2008 and 2009, both the Technical Support Working Group and the Joint Improvised Explosive Device Defeat Organization [40] sponsored evaluations of commercial 'hardened mobile' trace detectors, during which these systems demonstrated the capability to detect certain types of explosives

[37] Details regarding the difficulty these systems face in detecting certain types of explosives were deleted because DHS considered them to be Sensitive Security Information.

[38] Small-bulk amount is defined by the Naval Explosive Ordnance Disposal Technology Division as the minimum amount that is visible to the eye.

[39] Certain details regarding the ability of kit-based detection systems to detect explosives and any limitations regarding these technologies were deleted because DHS considered them to be Sensitive Security Information.

[40] The Joint Improvised Explosive Device Defeat Organization is a jointly manned activity of DOD, established to reduce or eliminate the effects of all forms of IEDs used against U.S. and Coalition Forces. Its leadership teams include representatives from the office of the secretary of all five branches of the U.S. military, plus legal, advisory and expert representatives from throughout the DOD and the intelligence community.

in an open environment over a range of external temperature, pressure, and humidity conditions.[41]

A survey by the Transportation Security Laboratory in 2009 showed a large number of manufacturers of handheld, desktop, and portable kit-based devices available on the commercial market. [42] Although costs are a consideration—for example, in addition to initial costs, there are routine maintenance costs and the cost of consumables such as the swabs used for sampling—for determining whether to make future deployments of handheld, desktop, and kit explosives detection systems, these technologies are already being used in the passenger rail environment and are expected to continue to play a role there.

Carry-on Baggage Explosive Detection Systems

Carry-on baggage explosive detection systems are based on x-ray imaging, a technology that has been in use for more than a century. Screening systems incorporating the technology have been used in commercial aviation for more than 30 years, in part, because they serve a dual purpose; images are analyzed for guns and other weapons at the same time they are analyzed for the presence of materials that may be explosives. Because these images do not uniquely identify explosive materials, secondary screening is required to positively identify the materials as explosives.

Single-energy x-ray systems are useful for detecting some bomb components. They are, however, not as useful for the detection of explosive material itself. Advanced techniques add multiple views, dual x-ray energies, backscatter, and computed tomography (CT) features (see Table 2) to provide the screener with additional information to help identify IEDs. Systems with one or more advanced techniques, multiple views; dual energies, and backscatter, but not CT, are called advanced technology (AT) systems to distinguish them from CT. AT systems enable more accurate identification of explosives without the additional expense of CT. Further, the additional information can be used to automatically detect explosive materials. Carry-on baggage explosive detection technology used in commercial aviation is a mature technology.[43] The

[41] The specific types of explosives that these technologies were able to detect were deleted because DHS considered them to be Sensitive Security Information.

[42]The Transportation Security Laboratory survey showed there were 11 manufacturers of handheld, 10 of desktops, and 9 of portable kits.

[43]The Transportation Security Laboratory gives carry-on baggage a technology readiness level of 9 for use in commercial aviation. Technology at this level has been proven through successful mission operations.

Transportation Security Laboratory has qualified[44] several different models of carry-on baggage explosive detection systems manufactured by several vendors for use in commercial aviation. Many of these systems are in use every day at airports in the United States.

Table 2: Description of Advanced Techniques for Carry-on Baggage Explosive Systems

Technology	Key feature	Characteristics
Multiple view	Records images from different directions.	Aids in thickness reconstruction.
Dual energy	Two x-ray energies or x-ray detectors sensitive to different x-ray energies.	Material discrimination based on shape.
Backscatter	Records images from backscattered x-rays as well as transmitted x-rays.	Distinguishes atomic characteristics of materials such as explosives from other materials.
Computed tomography	3-dimensional images.	Allows the most accurate estimate of material properties. Hidden objects are identified.

Source: GAO and Sandia National Laboratories.

Carry-on baggage explosive detection systems are effective in detecting IEDs that use conventional explosives when screeners interpret the images as was demonstrated in a Transportation Security Laboratory air cargo screening experiment where five different models of currently fielded AT baggage explosives detection systems were used to screen all eight categories of TSA-defined cargo.

In addition, DHS Science and Technology (S&T) Directorate provided another comparison of screener performance to automatic detection performance in a 2006 pilot program at the Exchange Place Station in the Port Authority Trans-Hudson (PATH)[45] heavy rail system. Phase I of this pilot evaluated the effectiveness of off-the-shelf explosives detection capabilities that were adapted from current airport checkpoint screening technologies and procedures. The carry-on baggage explosive detection equipment was operated in the automated threat detection mode to

[44] •Qualified carry-on baggage explosive detection systems have been tested to verify that they meet requirements as specified in a TSA-initiated Technical Requirements Document.

[45] PATH is a subsidiary of the Port Authority of New York and New Jersey, and is the eighth largest heavy rail transit authority in the United States.

minimize passenger delay. System effectiveness was tested by the use of a red team, an adversary team that attempted to circumvent the security measures. While the results were highly sensitive and not discussed in the pilot program report, the false alarm rate was found to be low.

Carry-on baggage explosive detection technologies have operational issues that limit their usefulness in passenger rail security. These systems are used in checkpoints and their acceptability will depend upon the tolerance for passenger delay. At checkpoints, 100 percent screening is possible up to the throughput capacity of the screening equipment; beyond that rate, additional screening equipment and personnel or selective (less than 100 percent) screening is required. During S&T's screening in the PATH system passenger rail pilot, a maximum single system throughput of 400 bags per hour was measured with carry-on baggage explosive detection systems operating in automatic explosive detection mode at threat levels appropriate to passenger rail, as described above. The 400 bags per hour single system throughput had a corresponding passenger throughput of 2336 passengers per hour. With this throughput, the pilot was able to perform 100 percent screening of large bags and computer bags (see below) during the peak rush hour using two carry-on baggage explosive detection systems.

Another closely related challenge associated with checkpoint screening is passenger delay. The S&T pilot in the PATH system measured median passenger delays of 17 seconds and 47.5 seconds respectively depending on whether or not a passenger's bags set off automated explosive detection alarms. These delays can be compared to the 13 second median time for an unscreened passenger to walk through the screening area. The longer delay, when bags set off alarms, was caused by secondary screening required to confirm or deny the presence of explosives. Maximum passenger throughput was achieved when screening only bags large enough and heavy enough to contain sufficient explosives to damage passenger rail infrastructure. When 100 percent screening exceeded the capacity of the system, the pilot used queue-based selection to maximize throughput. In queue-based selection, a traffic director selects passengers for screening as long as there is room in the queue for the screening process. Using this procedure, the pilot was able to accommodate PATH's desire to keep queue lengths below five passengers.

Acquisition costs range from $25,000 to $50,000 for AT systems to more than $500,000 for CT systems. The primary operating cost is manpower. Operating manpower typically includes a traffic director (someone to select passengers for screening [if required], direct passengers to the carry-on baggage explosive detection system, and provide instructions as required), a secondary screener, and a maintenance person.

Structures would be needed to protect existing carry-on baggage explosive detection systems from the challenging passenger rail environments, which include outdoor stations that are exposed to dust and precipitation. This is because typical carry-on baggage explosive detection systems have hazardous parts that are not protected from foreign objects up to 1 inch in diameter and have no protection from water intrusion.

Explosive Trace Portals

Explosive trace portals (ETP) are used in screening for access to buildings and, to a limited extent, airport checkpoint screening. The operation of these systems generally involves a screener directing an individual to the ETP and the ETP sensing his presence and, when ready, instructing the individual to enter. The portal then blows short puffs of air onto the individual being screened to help displace particles and attempts to collect these particles with a vacuum system. The particle sample is then preconcentrated and fed into the detector for analysis. The results are displayed to the operator as either positive or negative for the detection of explosives. Positive results can display the detected explosives and trigger an audible alarm.

Currently tested and deployed ETPs use IMS analytical techniques for chemical analysis to detect traces of explosives, similar to those used for handheld and desktop detectors. These techniques are relatively mature but the operation of IMS-based ETPs in an open air environment, such as that of passenger rail, is subject to interference from ambient agents, such as moisture and contaminants, that can impact a detector's performance by interfering with its internal analysis process resulting in false readings.[46]

Regardless of the detection technique used, sampling is a major issue for trace detection. Generally, factors such as the explosives' vapor pressure and packaging, as well as how much contamination is present on an individual from handling the explosive, affect the amount of material available for sampling. Particular to trace portals, factors such as the systems' puffer jets and timing, clothing, the location of explosive contamination on the body, and human variability impact the effectiveness of sampling. For example, if the puffer jets produce too little pressure,

[46] Certain details regarding the limitations of IMS screening technology in portals were deleted because DHS considered them to be Sensitive Security Information.

they have little impact in improving the trace explosive signal, while too much pressure results in trace explosive particles becoming lost in a large volume of air that is difficult to sample effectively. In addition, clothing material and layering can reduce the available trace explosive signal. The location of the explosive trace on the body also impacts the amount of trace explosives that the system will collect.

In laboratory testing of ETPs in 2004, the Naval Explosive Ordnance Disposal Technology Division tested three ETP systems' basic ability to detect trace amounts of certain explosives within the required detection threshold when deposited on the systems' collection sites.[47] While the systems consistently detected some of these explosives, they were unable to detect others. [48]

In addition, during laboratory testing on systems from three manufacturers performed by the Naval Explosive Ordnance Disposal Technology Division in 2004 and the Transportation Security Laboratory from 2004 through 2007, the systems did not meet current Naval Explosive Ordnance Disposal Technology Division or TSA requirements.

In 10 laboratory and airport pilot tests of ETPs from three manufacturers from 2004 through 2005, the Naval Explosive Ordnance Disposal Technology Division and TSA also measured the systems' throughput. In laboratory testing, the average throughput without alarms ranged from 2.56 to 5 people per minute. During pilot testing in airports, the operational mean throughput, which included alarms, ranged from 0.3 to 1.4 people per minute and the operational mean screening time ranged from 15.4 seconds to 22.2 seconds. Although, they may have some applicability for checkpoint screening in lower volume rail environments that require passengers to queue up, the throughput and screening time of ETPs make them impractical to use for 100 percent screening in high volume rail stations.

An ETP system using a different analytical technique, mass spectrometry (MS), for chemical analysis has the potential of significantly improving the

[47]The Naval Explosive Ordnance Disposal Technology Division performance requirements are established by military security personnel, various government agencies with similar requirements, and commercial industry.

[48] Certain details regarding the ability of ETPs to detect explosives were deleted because DHS considered them to be Sensitive Security Information.

ability to distinguish explosives from environmental contaminants, although its use in a portal configuration has not been tested in the rail environment.[49] DHS has, however, performed laboratory testing of two versions of an MS-based ETP.[50]

Other operational issues may limit their applicability in the rail environment. GAO found that during the pilot testing in airports, for example, the systems did not meet TSA's reliability requirements due to environmental conditions.[51] This resulted in higher than expected maintenance costs and lower than expected operational readiness time. ETPs may have some applicability for checkpoint screening in lower volume rail environments that require passengers to queue up such as Amtrak, but the low throughput and long screening time of ETPs make them impractical to use for 100 percent screening in high volume rail stations. In addition, the large size and weight of ETPs make them difficult to transport and deploy in stations with limited space and also impractical for use in any random way.

Advanced Imaging Technology Portals

Advanced Imaging Technology (AIT) portals are used for screening people for building access and, to an increasing extent, airport access. The operation of these systems generally involves the individual undergoing screening entering the AIT portal and raise his hands above his head. The AIT portal then takes images of the individual, which are displayed to another officer who inspects the images. The inspecting officer views the image to determine if there are threats present. If a threat is detected, the individual must go through further inspection to determine if the he or she is carrying explosives.

---

[49] MS-based systems can provide about 10,000 times greater specificity than an IMS-based system; that is they have a much greater ability to distinguish explosive molecules from interfering molecules in a sample, resulting in a significantly lower alarm rate. The greater specificity also makes MS-based systems capable of better distinguishing a broader range of explosives from other similar chemical compounds.

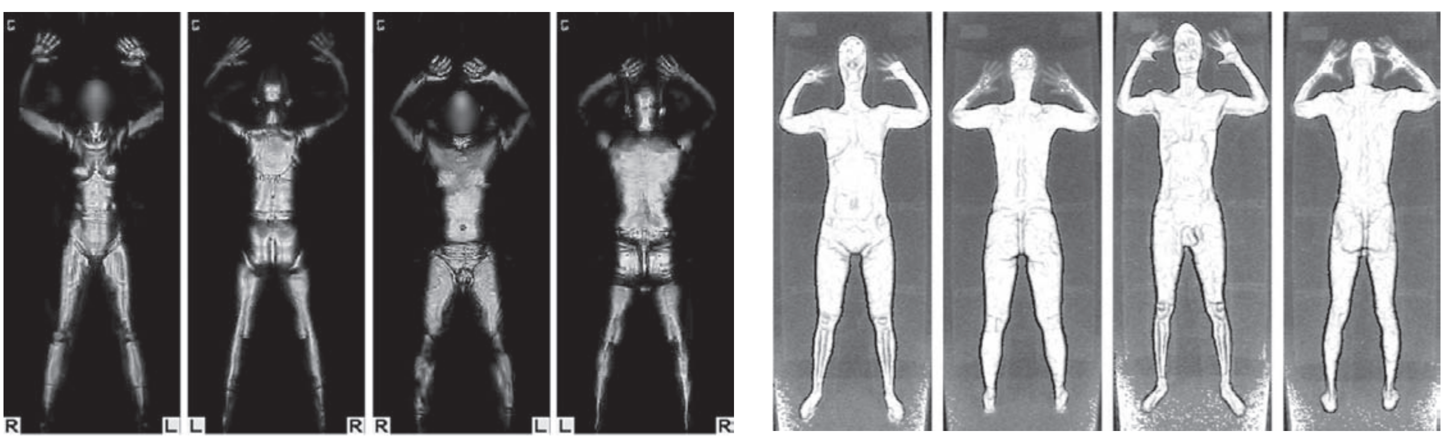
[50] Details concerning the ability of MS-based ETPS to detect explosives in DHS laboratory tests were deleted because DHS considered them to be Sensitive Security Information.

[51] GAO, *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*, GAO-09-21SU (Washington, D.C.: Apr. 17, 2009).

Currently deployed AIT portals in the aviation environment use either millimeter wave[52] or backscatter x-ray techniques to generate an image of a person through their clothing. While both systems generate images of similar quality, millimeter wave has the advantage that it does not produce ionizing radiation. Although, according to one manufacturer, its backscatter x-ray system meets all applicable federal regulations and standards for public exposure to ionizing radiation, systems that don't use ionizing radiation will likely raise fewer concerns.

An issue of particular concern to the public with AIT portals is privacy, due to the ability of the systems to image underneath clothing (see figure 7). In order to protect passengers' privacy, TSA policy for these systems specifies that the officer directing passengers into the system never sees the images. In addition, some systems offer privacy algorithms that can be configured to blur out the face and other areas of the body or present the image as a chalk outline. Efforts are currently underway to develop algorithms to automate the detection of threat objects, which has the potential to increase privacy if it eliminates the need for a human to inspect the images.

Figure 7: Examples of AIT portal images



Millimeter wave images

Backscatter x-ray images

Source: Transportation Security Administration.

[52]The millimeter wave region of the electromagnetic spectrum encompasses frequencies generally between 30 GHz and 300 GHz.

In testing done prior to October 2009, TSA tested AIT portals from two vendors—one using millimeter wave and the other backscatter x-ray—against detection, safety, throughput, and availability requirements for airport checkpoint screening. Both systems met these requirements.[53] In addition, in 2006, TSA pilot tested an AIT portal in the rail environment to determine the usefulness and maturity of these systems.

In 2007 and 2008, the Transportation Security Laboratory tested the performance of AIT systems in a laboratory environment for DHS S&T. TSA also began an operational evaluation of AIT systems in airports in 2007, which, due to privacy concerns, includes the use of privacy algorithms. Laboratory testing included a comparison of the performance of AIT systems against enhanced metal detectors and pat-downs; determining the detection effectiveness of the systems for different body concealment locations and threat types, including liquids, metallic and nonmetallic weapons, and explosives; and measuring the systems' throughput. The detailed results of this testing are classified so will not be outlined in this technology assessment.

However, generally, the testing showed that there are a number of factors that affect the performance of AIT systems, including the individual inspecting the images for potential threats, the use and settings of privacy algorithms, and other factors. For example, the detection performance varied by screener. In addition, the use of privacy algorithms generally impacts the decision time for screeners, and has other operational considerations. The throughput of one of the AIT systems was measured to be 40 people per hour, which was significantly lower than the S&T requirement of 60 people per hour.

As with ETPs, AIT portals may have some applicability for checkpoint screening in lower volume rail environments, but the low throughput, long screening time, and other factors make them impractical to use for 100 percent screening in high volume rail stations. Another operational issue that may limit their applicability in the rail environment is their large size and weight that makes them difficult to transport and deploy in stations with limited space.

[53] Details from the TSA's October 2009 test regarding the probability of detection and probability of false alarm for AIT systems were deleted because DHS considered them to be Sensitive Security Information.

Standoff Explosives Detection Systems

Standoff explosives detection systems are primarily differentiated from other types of explosives detection devices by the significant physical separation of detection equipment from the person or target being scanned.[54] Several different technologies have been incorporated into standoff explosives detection systems, but those suitable for use today in a public setting such as passenger rail are passive or active imaging systems using typically either the millimeter wave or terahertz (THz)[55] portion of the electromagnetic spectrum. Radiation in these portions of the spectrum are naturally emitted or reflected from everyday objects, including the human body, and have the added feature that clothing is often transparent to them. Therefore, they can be used to safely screen people for hidden threat objects. Systems available on the market today claim to detect person-borne objects across a range of distances.

In several laboratory and field studies since 2006 looking at passive standoff imaging systems, organizations including Naval Explosive Ordnance Disposal Technology Division, Transportation Security Laboratory, S&T, and TSA have demonstrated the technology's basic ability, under the right conditions, to detect hidden person-borne threat objects. Because the detection technique relies on a temperature differential between the warmer human body and the colder threat object next to it and not on the metallic content of the object, it also has the potential to detect non-metallic threats. This capability gives these standoff imaging systems a distinct advantage over walk-through metal detectors—the conventional person screening tool—which can only detect objects with sufficient metallic content.

DHS has also evaluated several standoff detection systems in operational rail environments. For example, as part of Phase II of the 2006 Rail Security Pilot looking at advanced imaging technologies, S&T found that such systems, in general, had some ability to detect threat objects indicative of suicide bombs on passengers and, overall, were developing into potentially useful technologies for passenger rail. Follow-on tests in 2007 and 2009 conducted by TSA at operational passenger rail or other

[54] There is no standard definition of standoff detection and separation distances can be less than a meter to tens of meters and beyond depending on concept of operations and goals. When applied to passenger rail, their distinguishing feature is they attempt to screen passengers with minimal to no impact on normal passenger flow.

[55] The THz region of the electromagnetic spectrum encompasses frequencies generally between 1000 GHz and 10,000 GHz.

mass transit locations provided further support for the technologies potential in addressing the screening needs of these systems.[56] In the July 2009 pilot, for instance, screening throughput for a passive millimeter wave system was tested by TSA during rush hour at the PATH Exchange Place subway station in New Jersey, a key entry point for commuters entering lower Manhattan. Two systems were used with each positioned 8 to 10 meters from a group of passenger turnstiles which provided a chokepoint for commuters entering the station. At several periods during rush hour, the systems demonstrated the ability to scan at or near 100 percent screening—in one case, more than 900 people per hour—without disrupting the flow of passengers.

Those pilots also demonstrated another attractive feature of these systems important for their use in passenger rail; they can be built to be relatively portable. For the PATH pilot, TSA broke down, moved and re-configured multiple standoff devices four times a day. The ability for screening systems to be deployed and easily re-deployed to another location encourages their use for random deployment, a recommended protective measure for mass transit systems.[57] In addition, this allows rail operators a way to provide screening to a much wider percentage of their system with fewer units than it would if they had to use fixed systems, which might prove cost prohibitive for the larger rail systems.[58]

While promising, several factors limit the more widespread use of current standoff detection technologies to just detection of objects carried on a person's body. They cannot provide a complete screening of a passenger and their belongings. They could, however, be used in tandem with other technologies or methods to handle accompanying articles.

Another limiting factor of current standoff technologies is the inability to discriminate between a potential threat object and a real one. Because the current state of the technology is based on imaging alone, explosives material identification is generally not possible. Use of radiation in the weaker, nonionizing millimeter wave and THz bands is attractive because

[56]Tests were run, for example, in New Jersey's PATH system, Washington D.C.'s Amtrak station at Union Station, and at the Staten Island Ferry Line in New York.

[57]DHS and DOJ/FBI Office of Intelligence and Analysis, *Terrorist Tactics Against Mass Transit and Passenger Rail*,,September 18, 2009.

[58]TSA has told us that they are encouraged enough by the technology that at least one commercial standoff system is on the path to be qualified.

it presents no danger to humans, but it also means that there is not enough information in the energy received by the sensor to more positively identify the threat as explosives material, as is routinely done, for example, by the higher energy CT systems used to screen checked baggage in aviation. Therefore, secondary screening will often be needed to completely resolve an alarm. In a standoff configuration, this raises logistical and manpower issues. At a minimum, for example, since the system is operating at a distance and passengers are not queuing up, it is not obvious how a person showing up as a potential threat could be easily intercepted and directed out from the normal flow of passengers.

In addition, although recent TSA testing in 2009 on an advanced standoff system showed good performance detecting hidden threat objects—including nonmetallic objects—on moving people in controlled situations, consistent detection under actual operating conditions in heavy passenger volume scenarios will be challenging. The TSA tests showed good probability of detection rates and low false alarm rates for indoors and outdoors screening.[59] Unlike the use of similar technology in a portal configuration (such as AIT) where a passenger can be asked to pause, turn around, or, for example, lift their arms to provide the sensor a better view, in a standoff configuration passenger, movement is uncontrolled. Although some systems allow tracking, the length of time a person can be maintained within the required line of sight is minimal in a fast-moving, large density crowd.

Finally, at up to several hundred thousand dollars per unit, a deployment of standoff technology in passenger rail could be costly and manpower intensive. Based on their operational pilots over the last several years, TSA told us that a likely implementation for a standoff detection system at a rail site would consist of multiple detectors, and a 3 to 4 person team including one operator per system, an assistant, and probably two Behavioral Detection Officers[60] to focus special attention on persons of interest. A good implementation would also have a canine team ready to inspect the passenger or accompanying articles, if the system detected an anomaly. Also, since some of the systems produce images susceptible to

[59] Certain details regarding the limitations of stand-off technologies were deleted because DHS considered them to be Sensitive Security Information.

[60] A Behavior Detection Officer is a TSA Transportation Security Officer specially trained to detect suspicious behavior in individuals.

the same privacy concerns as the recent deployment of AIT in airports, a remote imaging station might also need to be configured and staffed.

Explosives Detection Canines

Explosives detection canines (EDC) are currently used in passenger rail systems for both random screening of passengers and their belongings and as a deterrent to criminal and terrorist activity. EDCs are considered a mature technology and are being used by all of the passenger rail operators with whom we spoke or that attended our expert panel. These operators also viewed canines as the most effective method currently available for detecting explosives in the rail environment because of their detection capability as well as the deterrent effect that they provide. More specifically, operators noted EDCs' ability to rapidly move to various locations throughout a rail system, their minimum impact on passenger flow and rail operations, and their ability to detect explosives they are trained to detect. Operators and experts on our panel also noted that canines are generally accepted by members of the public that use these systems. In addition to passenger rail operators, canines have been deployed by federal agencies such as the U.S. Secret Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); and U.S. Customs and Border Protection. While the use of canines is mature, both the government, through DHS S&T, as well as academia, are conducting ongoing research on the limits of canine detection.

While the mechanism of how canines detect explosives through their sense of smell is not well understood, there are several certification programs to validate the canines' ability to detect explosives, which include specifying standards for explosives detection. These standards vary based on which entity is certifying the canine. A guiding document on the training of canines is the Scientific Working Group on Dog and Orthogonal Detectors Guidelines that specifies recommended best practices for canine explosives detection. These standards call for an EDC to detect explosives a certain percent of the time and a probability of false alarms less than a certain rate. Certifying entities, however, may have more stringent standards. For example, ATF requires that its canines detect all explosives that are presented to them, and have limited false alarms in its tests. TSA requires that their certified canines find a specified percent of explosives in a variety of scenarios, such as onboard an aircraft, mass transit rail, and mass transit buses. Homeland Security Presidential Directive-19 tasks the Attorney General, in coordination with DHS and other agencies, with assessing the effectiveness of, and, as necessary, making recommendations for improving federal government training and education initiatives related to explosive attack detection, including canine training and performance standards. According to ATF officials, TSA, in coordination with ATF, is developing standards for EDCs, which are nearly complete and are similar to the standards that ATF uses.

EDCs have a limited period of endurance at which they can maintain effective detection capabilities. According to ATF officials and other experts that attended our panel, canines can typically operate between 20 and 45 minutes before requiring a break with a total of 3 to 4 hours of time spent detecting per day. Additionally, members of our expert panel told us that aspects of the rail environment such as dirt, cleaning chemicals, and metal fragments from trains, may reduce canines' optimum operating time in this environment. As a result, one rail operator told us that their EDCs are stored in the back of police cars throughout the day unless they are needed and are not available for use as a deterrent. TSA advocates using explosive detection canines on patrols as visible deterrents in an effort to reduce crime and prevent the introduction of explosives into the rail environment.

Canines have a history of being trained to detect items and in recent years have been trained to detect, among other things, explosives, fire accelerants used in arson investigations, and drugs. While training methods differ among canine training schools, these methods typically train canines by rewarding them for locating certain items. Rewards include toys, a food treat, or the canine's food itself. In turn, these canines are trained to alert their handlers if they detect an item of interest, usually by sitting down next to the item. EDCs used in rail are generally deployed to screen passenger baggage, either on a primary basis by inspecting baggage as passengers enter a system or on a secondary basis to screen an item of interest, such as an unattended package. Additionally, EDCs are to receive training on a regular basis to ensure that they are capable of detecting explosives. Recurrent training requirements vary based on the training method used with the canine. For instance, one training regime we reviewed calls for 4 hours per week of recurrent training for EDCs, while other training regimes, such as those used by ATF, require daily training. The amount of recurrent training necessary for EDCs has not been determined according to the experts we spoke with, but they agree that the training is necessary to ensure the canine accurately detects explosives. As such, passenger rail operators who employ EDCs are to incorporate the training regime specified by the training method used to produce the EDC to ensure the canine operates effectively. Additionally, TSA and ATF both require their trained EDCs to be recertified on an annual basis whereby the canine and handler must demonstrate that they can detect explosives and meet required performance standards.

The quality of an EDC's search for explosives is dependent on the handler correctly interpreting behavioral changes of the canine. As the canine is capable of giving a positive or negative response as to the presence of an explosive odor emanating from an item, the handler must interpret the canine's response and respond appropriately in keeping with a pre-determined concept of operations because the canine cannot indicate the type of explosive it has detected. Moreover, according to ATF officials, a canine is only capable of detecting the explosives it has been trained to detect and there are tens of thousands of explosive compounds. To address this issue, ATF separates explosives into six categories with similar characteristics that the canines are trained and required to identify.

According to TSA, the total initial cost to acquire and train an EDC and handler is about $31,000. In addition, there are also ongoing maintenance costs including food, veterinary services, and other maintenance expenses, as well as the ongoing expense of the handler's salary. TSGP grant funding can often be used to offset the initial acquisition cost of the canine, but cannot typically be used to pay for ongoing maintenance throughout the canines' duty life.[61] According to ATF officials, an EDC typically has an operational life of about 7 years, having completed training around age 2 and entering retirement at age 9.

Vapor Wake Canines are an emerging use of EDCs that may be applicable to the passenger rail environment. Vapor Wake Canines differ from more traditional EDCs in that the canine does not directly sniff individual passengers and their belongings and instead the canine may remain in a stationary location sniffing multiple passengers as they pass by the canine, thus allowing more passengers and their belongings to be screened. These canines are trained to alert if they detect any explosives in the air and follow the explosive to its source. Vapor Wake Canines were piloted by DHS S&T in 2006 in the Metropolitan Atlanta Rapid Transit Authority with generally positive results. Specifically, these canines were able to detect explosives under the concept of operations developed by DHS S&T.[62] DHS S&T officials told us that they will soon begin additional research on Vapor Wake Canines to determine their probability of detection and to better understand factors behind their performance.

[61] Generally, TSGP funding for each EDC lasts 36 months.

[62] Details regarding the limitations of vapor wake canines were deleted because DHS considered them to be sensitive security information.

Limitations in Available Explosives Detection Technologies Restrict Their More Widespread or More Effective Use in Passenger Rail

The ability of explosives detection technologies to help protect the passenger rail environment depends both upon their detection performance and how effectively the technologies can be deployed in that environment. Detection performance varies across the different technologies with more established technologies such as handheld, desktop, kit-based trace detection systems, x-ray imaging systems, and canines having demonstrated good performance against many conventional explosives threats while newer technologies such as ETPs, AIT, and standoff detection systems are in various stages of maturity. However, all of the technologies face key challenges, and most will struggle in passenger rail stations to screen passengers without undue delays. Important characteristics of the technologies such as screening throughput, mobility, and durability, as well as physical space constraints in rail stations may limit deployment options for explosives detection technologies in passenger rail.

Detection Performance Varies Across the Different Explosives Detection Technologies and Challenges Exist in Detection of HMEs

Certain explosives detection technologies have demonstrated good detection performance against conventional explosives. Explosives detection canines, for example, are certified by several organizations as being able to detect a wide variety of conventional explosives for which they have been trained. In addition, some of the analytical trace detection methods are mature laboratory techniques that—within their individual design constraints—have been shown to be capable of consistent detection of many conventional explosives and their components when used in handheld, desktop, and kit-based systems. In many cases, this is because they have been designed specifically to focus on specific characteristics of nitro-based conventional explosives. Similarly, the more mature bulk detection techniques—carry-on baggage x-ray systems, for example—have been widely used for many years and, when used by trained operators, have shown good detection performance.

However, some of the newer detection technologies—ETPs, AIT, and standoff detection systems, for example—are in varying stages of maturity and more extensive testing would be required to determine their likely performance if deployed in passenger rail. For example, ETPs performed poorly in laboratory testing even though those devices incorporated mature analytical detection techniques. In this case, the variation in performance might be the result of how those techniques are integrated by specific manufacturers into a portal configuration. AIT is currently being deployed in airports nationwide, and laboratory testing has shown it has some ability to detect explosives.[63] While standoff detection systems have demonstrated good performance detecting hidden threat objects on people in controlled testing, consistent detection under actual operating conditions in heavy passenger volume scenarios will be challenging.

With all the technologies, certain factors underlie their ability to achieve adequate performance and often these depend on the human operator. For example, in a trace detection system the human operator plays a key part in preparing the sample and delivering it to the trace detection machine. In addition, trace detection is an indirect method of detection, relying on the presence of trace signatures that may, in fact, not exist or exist in insufficient quantities to be detected even though the threat object is present, or are present in the absence of a threat object.

Similarly, image based detection schemes are all dependent on successful image interpretation. Human operator image interpretation is a difficult task and performance is largely a function of adequate and persistent training. To help address this issue, DHS has initiated efforts looking at enhancing automated image processing algorithms to provide for better detection and lower false alarm rates. As part of this, DHS is creating a database of raw image data from commercially available systems—for example, x-ray and millimeter wave image data—which can be made available to researchers to help them develop better automated detection algorithms to improve processing across a range of imaging technologies including carry-on baggage x-ray technologies such as AT-based systems, AIT, and some of the standoff detection technologies. With the goal of increasing the probability of detection and reducing the number of false alarms these systems generate when operating in automated mode, such enhancements could help with the challenge of screening large volumes of people by increasing system throughput. While an outgrowth of research and development to support aviation security, this could benefit the use of imaging technologies in passenger rail settings as well.

Finally, adequate detection performance of explosives detection technologies can depend on other factors, such as maintenance, system calibration, and proper setup. For example, performance can be affected by the operator's preferences regarding sensitivity of the equipment. With many of the technologies there are tradeoffs that can be made between the

[63] Certain details regarding the limitations of AIT systems were deleted because DHS considered them to be Sensitive Security Information.

sensitivity of the device and the operator's tolerance for false alarms. In cases where a trace detector is highly sensitive to contaminants in the air, for instance, decreasing the sensitivity may reduce the number of false alarms but will also increase the possibility for missed detections.

One of the issues in implementing explosives detection technologies effectively in passenger rail is in identifying the explosive materials and amounts that constitute the threat to that environment. While requirements and standards for explosives threat amounts and detection levels, for example, have been defined for the aviation environment and for DOD's counter IED mission, threat amounts have not been determined for rail for either the conventional explosives threat or the threat from HMEs. As a result, in general, detection performance has been measured against threats levels defined for other environments.

Screening Throughput, Mobility, and Other Characteristics of Explosives Detection Technologies Could Limit Deployment Options in Passenger Rail

Because passenger volumes and timeliness expectations vary across the different rail systems including heavy rail and commuter or light rail, different methods of selecting and screening passengers are possible. Although passenger volumes in the heavier trafficked rail stations may preclude 100 percent screening of passengers in an overly intrusive way, lighter volume stations may allow for such intrusive screening if an adequate screening throughput speed can be maintained. Decisions regarding screening modes will vary by systems, stations, and the tolerance for passenger delay.

Two important system characteristics when considering the use of explosives detection technologies in passenger rail are screening throughput and system mobility. The higher the throughput, the less delay is imposed on passenger flow. The more portable a detection system is, the more it lends itself for use in random deployment, a known deterrent and cost effective option for rail operators.

Screening throughput and system mobility varied across the different explosives detection technologies we examined, but many had screening times that would be difficult to accommodate in situations with heavy passenger volume. In airport security checkpoints, for example, using similar equipment and working toward a goal of 10 minute or less wait times, the TSA staffing allocation model for screening operations requires individual screening lanes to be able to process 200 passengers per hour. [64] However, during the 2006 S&T pilot testing in PATH, passenger flow rates on the order of 4,000 passengers per hour was measured during the afternoon rush at just the main entrance turnstiles at one station. Even under TSA's aviation wait time goal this would require the purchase, staffing, and physical space for 20 screening lanes.

These technologies, however, might be considered for use in lower volume rail stations, for example, or in other areas of passenger rail where passenger queues could be supported without unduly impacting passenger flow. However, they are generally large, bulky and not easily moved from place to place and therefore impractical for use in any highly mobile way.

In general, most passenger rail operators that have deployed explosives detection technologies have done so on a less intrusive basis, using, for example, mobile explosives detection canine teams as a deterrent in stations or, alternatively, setting up temporary, portable stations for the screening of selected passengers who are pulled out of the normal passenger flow randomly, via some selection method, or as a result of behavioral cues. In this mode, for example, they have used handheld detectors for primary screening.

Standoff detection systems, which minimize the impact of screening on passenger flow, are the only explosives detection technology that currently could be considered for helping to address the 100 percent screening scenario at heavy volume stations, generally, for passenger rail. As noted, some of these systems demonstrated the ability to scan at or near 100 percent of passengers even in heavy rail stations for periods of time. In addition, many are portable and are designed so that system installations could be shifted from site to site. However, while attractive from a throughput point of view, standoff systems are developing in terms of their detection performance and general concept of operations.

In addition to limitations imposed by the technologies, rail stations themselves have constraints that will influence the applicability of certain technology for certain purposes. These include environmental issues, such

[64] GAO, *Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed,* GAO-07-299 (Washington, D.C.: Feb. 28, 2007). The model is used to guide Transportation Security Officer (TSO) staffing requirements for screening operations at the nation's airports using assumptions on a representative week during each airports' busiest month.

as the relatively high level of contaminants found in passenger rail environments like steel dust and soot that can disrupt the operation of sensitive equipment, and raise the potential for false alarms, and the lack of controlled temperature and humidity levels in many stations and the potential for extremes of those levels in outdoor stations. Some DOD research and development efforts are looking at hardened versions of some explosives detection technologies.[65]

The general openness of many rail stations is another important consideration in deciding on the use of explosives detection technologies in rail. In commuter or light rail systems, for example, many stations may be unmanned, outdoor platforms without barriers between pubic areas and the train and with few natural locations to place technologies to be able to screen passengers. With limited existing chokepoints, implementation of certain technologies may require station infrastructure modifications to aid in funneling passengers for screening.

Finally, physical space constraints in many stations are an important consideration. For example, many rail stations have limited space in which to install large equipment, accommodate any passenger queues that might build up, or add multiple screening lanes as a way of dealing with long lines. Further, while standoff detection technologies are more able to deal with heavy passenger volumes and do not necessarily have a large physical footprint, they do require several to tens of meters of open, line of sight spacing between sensor and passengers for effective operation.

[65] Both DOD's Technical Support Working Group and the Joint Improvised Explosive Device Defeat Organization have sponsored research and development efforts to test emerging hardened handheld trace detectors, and the Technical Support Working Group is developing a hardened portal.

Several Overarching Operational and Policy Factors Could Impact the Role of Explosives Detection Technologies in the Passenger Rail Environment

In addition to how well technologies work in detecting explosives and their applicability in the passenger rail environment, there are several overarching operational and policy considerations impacting the role that these technologies can play in securing the passenger rail environment, such as who is paying for them and what to do when they apparently detect explosives. Even if a technology works in the passenger rail environment, our work, in consultation with rail experts, identified several critical operational and policy factors that arise when these technologies are being considered for deployment. Specifically, 1) the roles and responsibilities of multiple federal and local stakeholders could impact how explosives detection technologies are funded and implemented in passenger rail; 2) implementation of technology or any security investment could be undertaken in accordance with risk management principles, to ensure limited security funding is allocated to those areas at greatest risk; 3) explosives detection technologies are one component of a layered approach to security, where multiple security measures combine to form the overall security environment; 4) a well-defined and designed concept of operations for the use of these technologies is important to ensure that they work effectively in the rail environment; and 5) cost and potential legal implications are important policy considerations when determining whether and how to use these technologies.

The Roles and Responsibilities of Multiple Federal and Local Stakeholders Could Impact How Explosives Detection Technologies are Funded and Implemented in Passenger Rail

Although there is a shared responsibility for securing the passenger rail environment, the federal government and rail operators have differing roles, which could complicate decisions to fund and implement technologies. More specifically, while passenger rail operators are responsible for the day to day security measures in their stations, including funding them, they utilize federal grant funding to supplement their security budgets. While federal grant funding for security has increased in recent years, decision making for funding these measures, including technology, is likely to continue to be shared between the rail operators and the federal government moving forward. In addition, as federal agencies implement their own rail security measures and operations, which could include the use of explosives detection technology, decisions of how to implement and coordinate these measures will likely be shared with operators.

Regarding the federal role, TSA defines and implements federal policies and actions for securing passenger rail systems in their role as the lead federal agency responsible for transportation security. TSA's strategy for securing passenger rail is identified in the Mass Transit Modal Annex to the Transportation Systems- Sector Specific Plan, including its role in developing and procuring technologies for securing rail systems. To date, TSA's primary approach to securing passenger rail, defined in the Modal Annex, has been to assess the risk facing rail systems, develop security guidance for rail operators, and to provide funding to operators to make security improvements to their systems, including the purchase of security technologies. Specifically, TSA's stated objectives for using technology in passenger rail is to bolster the use of technologies to screen passengers and their bags on a random basis in partnership with rail operators. According to the Modal Annex, these objectives are to be achieved through the use of explosives detection technology to screen passengers during TSA Visible Intermodal Prevention and Response (VIPR) operations and screening programs introduced by passenger rail operators themselves.[66] In addition, through its National Explosives Detection Canine Team Program (NEDCTP), TSA procures, trains, and certifies explosives detection canine teams and provides training and the canines to passenger rail operators.[67]

TSA also supports the use of technology by providing funding to rail operators to purchase screening technologies and train their employees through TSGP.[68] To date, TSGP has provided funding for various security-

[66]Since late 2005, TSA has reported deploying VIPR teams consisting of various TSA personnel to augment the security of passenger rail systems and promote the visibility of TSA. Working alongside local security and law enforcement officials, VIPR teams conduct a variety of security tactics to introduce unpredictability and deter potential terrorist actions, including random high visibility patrols at passenger rail stations and conducting passenger and baggage screening operations using specially trained behavior detection officers and a varying combination of explosives detection canine teams and explosives detection technology.

[67]In 2005, TSA expanded the NEDCTP from aviation into mass transit. TSA has worked in partnership with mass transit systems to procure, train, certify, and deploy canine teams to mass transit systems nationwide to provide mobile and flexible deterrence and explosives detection capabilities. TSA provides the canine training for the handler and the dogs and also allocates funds to cover costs associated with continued training and maintenance of the team, while the transit system commits a handler to attend the TSA training and receive program certification.

[68]Since fiscal year 2008, TSA has approved transit agency projects and then forwarded them to FEMA's Grant Programs Directorate (GPD) for review. GPD is responsible for ensuring that all grant projects adhere to federal grant requirements, including all environmental and historical preservation (EHP) requirements. FEMA's Office of Environmental and Historical Preservation (OEHP) assists with the EHP reviews. GPD reviews projects identified as having limited EHP impacts, while OEHP reviews projects needing a more extensive environmental and historical review. Until FEMA is satisfied that all requirements have been met, no grant funding can be released to transit agencies to begin projects. However, once funds are awarded, transit agencies must complete the grant project within the designated performance period for the grant year.

related technologies; including handheld explosive trace detection equipment, closed-circuit television, intrusion detection devices, and others. In June 2009, we reported that the TSGP faces a number of challenges, such as lack of clear roles and responsibilities in the program and delays in approving projects and making funds available to operators, and as of February 2009, of the $755 million that had been awarded by TSGP for fiscal years 2006 through 2008, approximately $334 million had been made available to transit agencies, and transit agencies had spent about $21 million.[69] We further reported that these delays were caused largely by TSA's lengthy cooperative agreement process with transit agencies, a backlog in required environmental reviews, and delays in receiving disbursement approvals from FEMA. As such, rail operators have spent a small percentage of the resources available to fund security investments. We recommended that DHS establish and communicate to rail operators time frames for releasing funds after the projects receive approval from TSA. DHS agreed with this recommendation and indicated that it would establish and communicate timeframes for releasing funds to TSGP grantees and try to release funds shortly after they have received all required documentation from grant recipients.[70]

Additionally, in a March 2010 report, the administration's Surface Transportation Security Priority Assessment recommended that TSA adopt a multi-year, multi-phase approach for grant funding based on a long-term strategy for transportation security. This approach calls for segmenting larger projects into smaller components to both complete the projects quicker and also to provide strategic planning for future grant funding needs and provide closer alignment of federal and stakeholder long-term priorities. Moreover, during our expert panel, rail operators stated that they would prefer the federal government to procure and provide security technologies to them, instead of providing cash awards to directly procure the technologies by the operators. These operators indicated that their local procurement regulations can often make the process of procuring security technologies slow and cumbersome.

In addition to providing funding for technology, the Modal Annex also identifies TSA's role in providing resources for research, development, testing, and evaluation of technology. TSA, like other DHS components, is responsible for articulating the technology needs of all transportation

[69] GAO-09-491.

[70] GAO-09-491.

sector stakeholders—including passenger rail operators—to DHS S&T for development.[71] Although TSA and DHS have worked to develop some security technologies specific to passenger rail systems, technologies that it has pursued could work across different transportation modes, including aviation, maritime, mass transit, and passenger rail. TSA officials told us that they look for opportunities to take advantage of technologies in transportation modes other than those for which they were originally developed. However, the TSA officials indicated that certain characteristics of passenger rail may not allow the deployment of technologies developed for other modes such as aviation.

In addition to its work with S&T, TSA has commissioned its own research efforts, including pilot programs designed to test existing explosives detection equipment in the rail environment and the use of standoff technologies in the passenger rail environment. Additionally, the administration recommended in its March 2010 report that TSA, DHS S&T, and other agencies directly involve rail operators in setting surface transportation research and development priorities.[72]

TSA also provides technological information to rail operators through the Public Transit Portal of the Homeland Security Information Network (HSIN) and maintains a Qualified Products List (QPL)[73] of technologies that have been qualified for use in aviation.[74] As we reported in June 2009[75], the information on HSIN is in an early state of development and contains limited information that would be useful to rail operators. For example, for a given security technology, TSA's list of technologies provides a

[71]To carry out this process, DHS S&T brings together agency representatives into Integrated Product Teams (IPT) to collaboratively set research and spending priorities to the individual project level. IPTs do not include technology end-users—such as transit bus and rail system security operators—because DHS has assumed that its component agencies would represent end-user interests.

[72]The White House Transborder Security Interagency Policy Committee Surface Transportation Subcommittee, *Surface Transportation Security Priority Assessment* (March 2010). In making its recommendations, the subcommittee gathered input from surface-transportation owners and operators, DHS and DOT, as well as state and local government representatives.

[73] See FAR § 9.203.

[74]Technologies that successfully pass independent and operational evaluation are added to a list of qualified products.

[75] GAO-09-678.

categorical definition (such as video motion analysis), a subcategory (such as day or night camera), and the names of products within those categories. We also reported that the list on HSIN neither provides nor indicates how rail operators can obtain information beyond the product's name and function and does not provide information on the product's capabilities, maintenance, ease of use, and suitability in a rail environment. We recommended that TSA explore the feasibility of expanding the security technology information in HSIN, including adding information on cost, maintenance, and other information to support passenger rail agencies' purchases and deployment of these technologies. TSA concurred with this recommendation and stated that it would provide information on HSIN about specifications, performance criteria, and evaluations of security technologies used in or adaptable to the passenger rail environment. In January 2010, TSA officials told us that they were still planning to provide this information on the HSIN some time in 2010, but had not done so yet.

TSA officials told us that in addition to the QPL for aviation there is another list that is administered by FEMA called the Authorized Equipment List, which provides a list of technologies for which TSGP grant recipients can use grant funding. According to TSA officials, the Authorized Equipment List is available on HSIN and there is one explosives detection technology on the list—a handheld explosive trace detector. Passenger rail operators that attended our expert panel stated that they would like TSA to pursue research more directly related to rail and provide additional information on which technologies are best for use in rail, including a list of "approved" or recommended technologies.[76] TSA officials told us that they are currently developing minimum standards for technologies for modes of transportation other than aviation, but did not provide a time frame for completing this effort. Once these standards are developed they envision adding categories for other modes of transportation-—such as rail-—to the QPL. Additionally, the administration's Surface Transportation Security Priority Assessment report from this year recommended that TSA along with DHS S&T establish a fee-based, centrally managed "clearing house" to validate new privately developed security technologies that meet federal standards.

[76] In our June 2009 report, we recommended that to help ensure that DHS security technology research and development efforts reflect the security technology needs of the nation's mass transit and passenger rail systems, TSA should expand its outreach to the mass transit and passenger rail industry in the planning and selection of related security technology research and development projects. See GAO-09-678.

In contrast to the federal role, passenger rail operators and local government stakeholders are responsible for the day-to-day security of rail systems, including the purchase, installation, and operation of any explosives detection technologies. As such, operators consider their own unique security and operational needs when deciding whether and to what extent to use these technologies. While the operators have responsibility for securing their systems, the operators that attended our panel expressed to us that their limited resources often limit their ability to directly invest in security, including technology, and instead they look to the federal government to provide financial assistance. For example, rail operators that we spoke to and that attended our expert panel noted that they often do not collect sufficient revenue from their fares to cover operational expenses.

In June 2009, we reported that while the majority of rail operator actions to secure passenger rail have been taken on a voluntary basis, the pending 9/11 Commission Act regulations outline a new approach that sets forth mandatory requirements, such as, among others, requirements for employee training, vulnerability assessments, and security plans, the implementation of which may create challenges for TSA and industry stakeholders.[77] In general, TSA has a collaborative approach in encouraging passenger rail systems to voluntarily participate and address security gaps. We also reported that with TSA's pending issuance of regulations required by the 9/11 Commission Act, TSA will fundamentally shift this approach, and establish new regulatory requirements for passenger rail security. TSA officials stated that they do not see the 9/11 Commission Act requirements impacting TSA's current role as it relates to technologies in the passenger rail environments. Because of the unique characteristics of the rail environment and the fact that the 9/11 Commission Act does not impose specific requirements related to technologies, TSA officials stated that the agency's role will continue to be to assist rail operators in conducting random deployments of explosives detection technologies and inspections, as stated in the Modal Annex.

[77] GAO-09-678.

Risk Management Could be Used to Effectively Guide the Decision to Fund or Implement Explosives Detection Technologies

As passenger rail operators consider the use of explosives detection technologies, it is not only important to select technologies capable of detecting explosives and that can be used in the passenger rail environment, but it is also important to select technologies that will address identified risks. We have recommended that a risk management approach be used to guide the investment of security funding, particularly for passenger rail systems, where security funding and rail operator budgets are limited.[78] As such, the decision as to whether or not to deploy explosives detection technologies should be made consistent with a risk management framework to ensure that limited security budgets are expended to address the greatest risks. We reported in June 2009 that officials from 26 of 30 transit and passenger rail systems we visited stated that they had conducted their own assessments of their systems, including risk assessments. Additionally, Amtrak officials stated that they conducted a risk assessment of all of their systems. As part of the assessment, Amtrak contracted with a private consulting firm to provide a scientific basis for identifying critical points at stations that might be vulnerable to IED attacks or that are structurally weak.[79] We also reported that other transit agencies indicated that they have received assistance in the form of either guidance or risk assessments from federal and industry stakeholders. For example, FTA provided on-site technical assistance to the nation's 50 largest transit agencies (i.e., those transit agencies with the highest ridership) on how to conduct threat and vulnerability assessments, among other technical assistance needs, through its Security and Emergency Management Technical Assistance Program (SEMTAP). According to FTA officials, although FTA continues providing technical assistance to transit agencies, the on-site SEMTAP program concluded in July 2006. Furthermore, FTA officials stated that on-site technical assistance was transferred to TSA when TSA became the lead agency on security matters for passenger rail.

In addition, multiple federal agencies recommend the use of risk based principles in assessing risk and making investment decisions. DHS's National Infrastructure Protection Plan states that implementing protective programs based on risk assessment and prioritization enables DHS, sector-specific agencies, and other security partners to enhance

[78]GAO-09-678.

[79]Another rail operator with whom we spoke, indicated that they had performed a risk assessment in which they identified their most critical assets and had identified likely threats to their system, including terrorism attacks by IEDs.

current critical infrastructure and key resources protection programs and develop new programs where they will offer the greatest benefit. Further, TSA's Modal Annex advocates using risk-based principles to secure passenger rail systems and we have previously reported that TSA has used various threat, vulnerability, and consequence assessments to inform its security strategy for passenger rail. In June 2009, we reported that TSA had not completed a risk assessment of the entire passenger rail system and recommended that, by doing so, TSA would be able to better prioritize risks as well as more confidently assure that its programs are directed toward the highest priority risks.[80] TSA concurred with this recommendation and stated that it is developing a Transportation Systems Security Risk Assessment that aims to provide TSA with a comprehensive risk assessment for use in passenger rail. To this end, TSA told us that it has developed a Transportation Systems Sector Risk Assessment report, which is to evaluate threat, vulnerability, and consequence in more than 200 terrorist attack scenarios on passenger rail. Moreover, TSA also indicated that they are developing and fielding a risk assessment capability focused on individual passenger rail agencies. This effort includes, among other things, a Baseline Assessment for Security Enhancement for rail operators, a Mass Transit Risk Assessment, and an Under Water Tunnel Assessment. Rail operators with whom we spoke or who attended our expert panel noted the importance of using risk management practices to allocate limited resources.

Explosives Detection Technologies are One Component of a Layered Approach to Security

TSA's Modal Annex calls for a flexible, layered, and unpredictable approach to securing passenger rail, while maintaining an efficient flow of passengers and encouraging the expanded use of the nations' rail systems. Expanding the use of explosives detection technology is one of the layers of security identified by the Modal Annex. When considering whether to fund or implement explosives detection technologies, it will be important for policymakers to consider how explosives detection technology would complement other layers of security, the impacts on other layers of security, and the security benefits that would be achieved. For example, one rail operator who attended our expert panel told us that they used deployments of explosives detection technologies along with customer awareness campaigns and CCTV as layers of security in their security

[80]A risk assessment, as required by the National Infrastructure Protection Plan, involves assessing each of the three elements of risk—threat, vulnerability, and consequence—and then combining them together into a single analysis.

posture. In addition to explosives detection technology, other layers of security that rail operators have used or are considering using to secure passenger rail include:

- Customer awareness campaigns. Rail operators use signage and announcements to encourage riders to alert train staff if they observe suspicious packages, persons, or behavior. We have previously reported that of the 32 rail operators we interviewed, 30 had implemented a customer awareness program or made enhancements to an existing program.[81]
- Increased number and visibility of security personnel. Of the 32 rail operators we previously interviewed, 23 had increased the number of security personnel they utilized since September 11, 2001, to provide security throughout their system or had taken steps to increase the visibility of their security personnel. Further, these operators stated that increasing the visibility of security is as important as increasing the number of personnel. For example, several U.S. rail operators we spoke with had instituted policies such as requiring their security staff, wearing brightly colored vests, to patrol trains or stations more frequently, so they are more visible to customers and potential terrorists or criminals. These policies make it easier for customers to contact security personnel in an emergency or potential emergency.
- Employee training. All 32 of the rail operators we previously interviewed had provided security training to their staff, which largely consisted of ways to identify suspicious items and persons and how to respond to events.
- CCTV and video analytics. As we previously reported, 29 of 32 U.S. rail operators had implemented some form of CCTV to monitor their stations, yards, or trains. Some rail operators have installed “smart” cameras which make use of video analytics to alert security personnel when suspicious activity occurs, such as if a passenger left a bag in a certain location or if a person entered a restricted area. According to one passenger rail operator we spoke with, this technology was relatively inexpensive and not difficult to implement. Several other operators stated they were interested in exploring this technology.
- Rail system design and configuration. In an effort to reduce vulnerabilities to terrorist attack and increase overall security, passenger rail operators are incorporating security features into the design of new and existing rail infrastructure, primarily rail stations. For example, of the 32 rail operators we previously interviewed, 22 of them had removed their conventional

[81] GAO-05-851.

trash bins entirely, or replaced them with transparent or bomb-resistant trash bins. Of 32 rail operators we previously interviewed, 22 had stated they were incorporating security into the design of new or existing rail infrastructure.

A Concept of Operations For Explosives Detection Technologies Could Enable Passenger Rail Operators to Better Balance Security with the Movement of Passengers

In deploying explosives detection technologies, it is important to develop a concept of operations (CONOPS) for both using these technologies to screen passengers and their belongings and for responding to identified threats. This CONOPS for passenger rail would include specific plans to respond to threats without unacceptable impacts on the flow of passengers through the system. There are multiple components of a CONOPS. First, operators identify likely threats to rail systems and choose layers of security to mitigate these threats. Since each rail system in the United States faces different risks, rail systems perform their own risk assessment in consultation with federal partners to identify their risks. Using the results of the risk assessment, each system crafts a strategy to respond to the threat and to mitigate the risks by acquiring different layers of security. Rail systems typically make use of multiple security layers—which may or may not include the use of an explosives detection technology component—based on the risks each system faces.

The CONOPS is a plan to respond to threats identified by one of the layers of security. Developing a CONOPS for responding to explosives detection technology is challenging because of the potential for false alarms. For example, two rail operators with whom we spoke and that were using explosives detection technologies to screen passengers and their belongings stated that a CONOPS was critical for ensuring that actions taken in response to an alarm are appropriate and are followed correctly. For example, should the person be questioned or searched further or should the person be moved to another location on the chance that the threat is real. These are questions that would be answered in developing a CONOPS and before implementing explosives detection technology in the passenger rail environment. Two of the rail operators and one of the experts that attended our panel also expressed concern about the potential for false alarms when using explosives detection technologies and the potential impacts on rail operations. For example, operators were concerned about a false alarm stopping service. As a result, it is important to carefully consider the CONOPS of using a particular technology, such as how to respond to false alarms, in addition to the security benefits before implementation. For instance, one major rail operator's CONOPS involves using handheld explosives detection technology to screen passengers' baggage randomly by a law enforcement officer. The frequency in which bags are selected is determined in advance by someone other than the law enforcement officer—such as a supervisor—based on a number of factors such as the number of passengers entering a station and resources available for screening. The baggage is then screened by the officer with the explosives detection equipment; if there is no alarm, the passenger is free to continue. Should the bag alarm, the officer then questions the passenger to determine the source of the alarm and, if necessary, takes action to respond to a threat.

Costs, Potential Legal Implications, and Policy Concerns, such as Privacy and Health, Are Important Considerations When Making Decisions about Explosives Detection Technologies in the Passenger Rail Environment

Cost is an important consideration for rail system security investments, as all operators have limited resources to devote to security. For example, all of the rail operators that we spoke with and that attended our expert panel expressed the view that obtaining funds for security priorities is challenging. Nearly all domestic rail systems operate at a deficit in which their revenues from operations do not cover their total cost of operations. An official from the industry association representing passenger rail and mass transit systems that attended our expert panel stated that when it comes to security investments, security often becomes less of a priority than operational investments as they often operate with budgets deficits. In addition, another rail operator that attended our expert panel raised concern that TSGP often will not provide funding for ongoing maintenance of capital purchases, additional staff needed to deploy these technologies, and disposable items required to operate the technology, such as swabs for explosive trace detection devices. For example, while rail operators can use TSGP grant funds to purchase explosives detection equipment, funding for the operation and maintenance of this technology is only provided for a 36 month period. One major rail operator that attended our expert panel stated that the cost of deploying a random baggage check with a handheld explosive trace detector costs between $700 and $1,000 per hour, including the costs of staffs' salaries and disposable items. Given the cost of operating and maintaining these security technologies, it would be important for policymakers to consider all associated costs of these technologies before implementing new security measures or encouraging their use.

Legal implications with regard to constitutional and tort law would also be important for passenger rail operators to consider when determining whether and how explosives detection technologies are applied in the passenger rail environment.[82] The Fourth Amendment of the U.S. Constitution protects individuals against unreasonable governmental searches, and state constitutional law may provide additional protections against searches. In recent years, federal courts have heard several challenges to new passenger inspection programs implemented in passenger rail environments.[83] In these cases, in order to assess the constitutionality of the programs, the courts considered factors such as the intrusiveness of the searches, the government interest in the program, and the effectiveness of the program. In addition to constitutional concerns, taking actions to mitigate potential tort liability is another important consideration for rail operators. For example, state law may allow individuals to bring tort claims against transit agencies, such as claims related to invasion of privacy and health hazards posed by scanning equipment. Also, operators using explosives detection canines should be conscious of potential claims related to dog bites.

There are also privacy considerations associated with subjecting passengers to certain types of screening technologies. Because explosives detection technologies generally do not collect personally identifiable information, they pose fewer privacy concerns than other screening techniques may. However, a number of advocacy groups have raised concerns about the use of AITs which produce an image of a person

[82]For a detailed discussion of legal implications of performing passenger security inspections, see Jenks, Christopher W. Transportation Research Board of the National Academies *TCRP Report 86: Public Transportation Security—Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers* (Washington, D.C.: 2007).

[83]Three passenger inspection programs have been challenged in different judicial districts. Based on the specific facts and circumstances of each case, each of the challenges was denied. See, e.g., Cassidy v. Chertoff, 471 F. 3d 67 (2d Cir. 2006) (holding that random inspections of ferry passengers' automobiles and baggage did not violate the Fourth Amendment because the intrusions on privacy interests are minimal and the measures are reasonably effective in serving an important governmental special need to protect ferry passengers and crew from terrorist acts); McWade v. Kelly, 2005 WL 3338573 (S.D.N.Y. 2005) (holding that New York City's random passenger inspection program did not violate the Fourth Amendment because the governmental interest in preventing a terrorist act on the subway is vitally important, that the inspection program is effective in deterring such an act, and the minimal intrusion entailed by subway searches is justified); American-Arab Anti-Discrimination Committee et al. v. Massachusetts Bay Transportation Authority, 2004 WL 1682859 (D. Mass. 2004) (holding that a policy permitting security searches of handbags, briefcases, and other items carried onto trains and buses was likely constitutional because there is a substantial governmental need or public interest served by the regime and the privacy intrusion is reasonable in its scope and effect, given the nature and dimension of the public interest to be served).

without clothing. To protect passengers' privacy, however, ways have been introduced to blur the passengers' images with privacy settings.

Concerns also exist about the impact that certain technologies could have on the health of passengers. For example, certain types of explosives detection screening equipment may expose individuals to mild radiation. Specifically, technologies such as backscatter x-ray AIT expose the passenger to minute amounts of radiation. While this radiation exposure is smaller than the radiation a person receives by a normal medical x-ray, the public may have concerns about being exposed to any radiation or may misjudge the amount of radiation they receive. For example, according to TSA, a person would require more than 1,000 backscatter scans in a year to reach the effective dose equal to one standard chest x-ray. Additionally, some forms of IMS technology make use of radiation in their operation and some people may be concerned with having any radiation source in a rail network.

Finally, some passenger rail systems operate across multiple city, county, and other jurisdictions and must coordinate with local governments and law enforcement across these areas. For example, the Washington Metropolitan Area Transit Authority was established by an interstate compact between Maryland, Virginia, and the District of Columbia. The authority has its own police force and must coordinate with not only the police force of the District of Columbia, but also the surrounding communities through which its trains pass. This pattern is common across the country where public transportation systems cross state and local boundaries. As such, the use of explosives detection equipment throughout these networks involves coordination across many levels of government and may potentially invoke the laws of multiple jurisdictions and come under the scrutiny of different governments.

Concluding Observations

Securing passenger rail systems is a daunting challenge for several reasons, including the open nature of these systems and the relative ease and the number of locations in which these systems can be accessed by those wishing to cause harm. While there are some explosives detection technologies available or currently in development that could be used to help secure passenger rail, there are several technical, operational, and policy factors that are important to consider when determining the role that these technologies can play in passenger rail security. There are various stakeholders responsible for securing passenger rail systems and all may need to be involved when making decisions to fund, implement, and operate explosives detection technologies. It is also important that the need for explosives detection technologies be based on a consideration of the risks posed by the threat of an explosives attack on passenger rail systems. Such a risk assessment would help define the detection needs, including what explosives materials need to be detected and in what quantities.

Explosives detection technologies are just one of many layers of security and cannot, by themselves, secure passenger rail systems. While explosives detection technologies can play a role in securing passenger rail systems, certain aspects of these technologies will likely limit their immediate use. All of the technologies face key challenges, including the ability to screen passengers without undue delays. In some cases, the ability to detect more conventional explosives is also limited. The ability of these technologies to effectively detect explosives on people and their belongings, as well as the expectations of the public for openness and speed when using rail, will likely be key drivers in decisions about which technologies should be applied, and in what capacity. Other important characteristics of the technologies, including the mobility, durability, and the size of the equipment, may limit deployment options for explosives detection technologies in passenger rail. The ability of these technologies to effectively detect explosives often depends on a human operator and the development of a strong concept of operations that defines the processes used to screen passengers and their belongings and the roles that people and technology play in that process will be critical.

When considering the options for securing passenger rail, it is important that policymakers also take into account the cost and legal implications of securing systems that are so open and widely used by the public. The lack of funding from passenger rail operator budgets means that the purchase and maintenance of explosives detection technologies would likely originate from or be highly subsidized by the federal government. Moreover, the wide scale use and reliance on these systems by the public means that individuals and advocacy groups may raise concerns about any technology that screens passengers or their belongings. An effective risk management process that continuously examines the risks posed by explosives to the passenger rail environment and considers the various technical, operational, and policy considerations when determining alternative solutions to address the explosives risk should result in an effective identification of the role that explosives detection technologies can play in securing passenger rail.

Agency Comments and Our Evaluation

We provided draft copies of this report to the Secretaries of Homeland Security, Defense, Transportation, Justice, and Energy for review and comment. DHS's TSA and the Department of Transportation provided technical comments which we have incorporated as appropriate. The National Nuclear Security Administration of the Department of Energy agreed with our report and also provided technical comments which we incorporated, as appropriate. The Department of Defense provided technical comments which we have incorporated as appropriate. The Department of Justice stated they had no comments on the draft report.

We will send copies of this report to the Secretaries of Homeland Security, Defense, Transportation, Justice, and Energy, and appropriate congressional committees. The report will also be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff has any questions about this report, please contact Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov or David Maurer at (202) 512-9627 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff that made major contributions to this report are listed in appendix II.

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Chief Technologist
Director, Center for Science, Technology, and Engineering

David C. Maurer

David C. Maurer
Director, Homeland Security and Justice Issues

Appendix I: Scope and Methodology

To determine what explosives detection technologies are available and their ability to help secure the passenger rail environment, we met with experts and officials on explosives detection research, development, and testing, and reviewed test, evaluation, and pilot reports and other documentation from several components within the Department of Homeland Security including the Science and Technology Directorate, the Transportation Security Laboratory; the Transportation Security Administration (TSA); the Office of Bombing Prevention; and the United States Secret Service; several Department of Defense (DOD) components including the Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV), the Technical Support Working Group (TSWG), and the Joint Improvised Explosive Device Defeat Organization (JIEDDO); several Department of Energy (DOE) National Laboratories involved in explosives detection testing, research and development including Los Alamos National Laboratory (LANL), Sandia National Laboratories (SNL), Oak Ridge National Laboratory (ORNL), and Idaho National Laboratory (INL); and the Department of Justice (DOJ) including the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), because of its expertise in explosives detection. We also observed explosives detection canine testing at the ATF's National Canine Training and Operations Center in Front Royal, Virginia. We also observed a TSA pilot test of a standoff explosives detection system at a rail station within the Port Authority Trans-Hudson passenger rail system (PATH). In addition, we made site visits to LANL and SNL to observe the research and development work being done and to interview experts on explosives detection technologies. We also interviewed several manufacturers of explosives detection technologies and attended an industry-wide exhibition and demonstration of explosives detection equipment products. In addition, we attended a symposium and workshop on explosives detection organized by DOD's Combating Terrorism Technical Support Office, the 2009 DOD Explosive Detection Equipment Program Review at NAVEODTECHDIV, and an academic workshop on explosive detection at DHS's Center of Excellence for Explosives Detection, Mitigation, and Response at the University of Rhode Island. We also interviewed government officials involved with securing passenger rail in the United Kingdom. Finally, we visited six domestic passenger rail locations that were involved in testing various types of explosives detection technologies to either observe the testing or discuss the results of these tests with operators. Table 3 is a listing of the passenger rail locations we visited.

Table 3: Passenger Rail Operators Interviewed During This Engagement

Passenger rail system	Urban area served
Chicago Transit Authority (CTA)	Chicago, Illinois
Maryland Transit Administration (MTA)	Greater Washington, D.C., and Maryland
METRA Commuter Rail	Chicago, Illinois
Port Authority Trans Hudson (PATH)	New York, New York and New Jersey
Virginia Railway Express (VRE)	Northern Virginia, greater Washington, D.C.
Washington Metropolitan Area Transit Authority (WMATA)	Washington, D.C.

Source: GAO.

In determining which explosives detection technologies were available and able to secure the passenger rail environment, we considered those technologies available today or deployable within 5 years, technologies which could be used to screen either passengers or their carry-on items, and technologies which were safe to use when deployed in public areas. In determining the capabilities and limitations of explosives detection technologies we evaluated their detection and screening throughput performance, reliability, availability, cost, operational specifications, and possible use in passenger rail. We also restricted our evaluation to those technologies which have been demonstrated through tests, evaluations, and operational pilots, to detect explosives when tested against performance parameters as established by government and military users of the technologies.[1]

We also obtained the views of various experts and stakeholders during a panel discussion we convened with the assistance of the National Research Council on August 11-12, 2009.[2] Panel attendees included 23 experts and officials from academia, the federal government, domestic and

[1] Specific performance parameters included, for example, the ability to successfully determine the presence of a variety of explosives and not falsely indicate the presence of nor falsely confirm the absence of explosives.

[2] We have a standing contract with the National Research Council (NRC) under which the NRC provides assistance in convening groups of experts to provide information and expertise in our engagements. The NRC uses its scientific network to identify participants and uses its facilities and processes to arrange the meetings. Recording and using the information in a report is our responsibility.

foreign passenger rail industry organizations, technology manufacturers, national laboratories, and passenger rail industry stakeholders such as local law enforcement officials and domestic and foreign passenger rail operators. During this meeting, we discussed the availability and applicability of explosives detection technologies for the passenger rail environment and the operational and policy impacts associated with implementing these technologies in the rail environment. While the views expressed during this panel are not generalizable across all fields represented by officials in attendance, they did provide an overall summary of the current availability and effectiveness of explosives detection and industry views on their applicability to passenger rail.

To determine what key operational and policy factors could have an impact in determining the role of explosives detection technologies in the passenger rail environment, we reviewed documentation related to the federal strategy for securing passenger rail, including TSA's Mass Transit Modal Annex to the Transportation Systems Sector Specific Plan, and other documentation including DHS reports summarizing explosives detection technology tests conducted in passenger rail to better understand the role and impact that these technologies have in the passenger rail environment. We reviewed relevant laws and regulations governing the security of the transportation sector as a whole and passenger rail specifically, including the Implementing Recommendations of the 9/11 Commission Act. We also reviewed our prior reports on passenger rail security and studies and reports conducted by outside organizations related to passenger rail or the use of technology to secure passenger rail, such as the National Academies, Congressional Research Service, and others to better understand the existing security measures used in passenger rail and operational and policy issues. During our interviews and expert panel mentioned above, we also discussed and identified officials' views related to the key operational and policy issues of using explosives detection technologies to secure passenger rail. While these views are not generalizeable to all industries represented by these officials, they provided a snapshot of the key operational and policy views.

During our visits to six rail operator locations involved in explosives detection testing, we interviewed officials regarding operational and policy issues related to technology and observed passenger rail operations. We selected these locations because they had completed or were currently conducting testing of the use of explosives detection technology in the rail environment and to provide the views of a cross-section of heavy rail, commuter rail, and light rail operators. While these locations and officials' views are not generalizeable to the entire passenger rail industry, they provided us with a general understanding of the operational and policy issues associated with using such technologies in the rail environment. In addition, we utilized information obtained and presented in our June 2009 report on passenger rail security.[3] For that work, we conducted site visits, or interviewed security and management officials from 30 passenger rail agencies across the United States and met with officials from two regional transit authorities and Amtrak. The passenger rail operators we visited or interviewed for our June 2009 report represented 75 percent of the nation's total passenger rail ridership based on the information we obtained from the Federal Transit Administration's National Transit Database and the American Public Transportation Association.

We conducted our work from August 2008 through July 2010 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to Technology Assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

[3]GAO-09-678.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Dr. Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

David Maurer, (202) 512-9627 or maurerd@gao.gov

Staff Acknowledgments

In addition to the contacts named above, contributors to this report include Amy Bowser, William Carrigg, Nirmal Chaudhary, Frederick K. Childers, Christopher Currie, Andrew Curry, Richard Hung, Lara Kaskie, Leyla Kazaz, Tracey King, Robert Lowthian, and Maria Stattel.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548