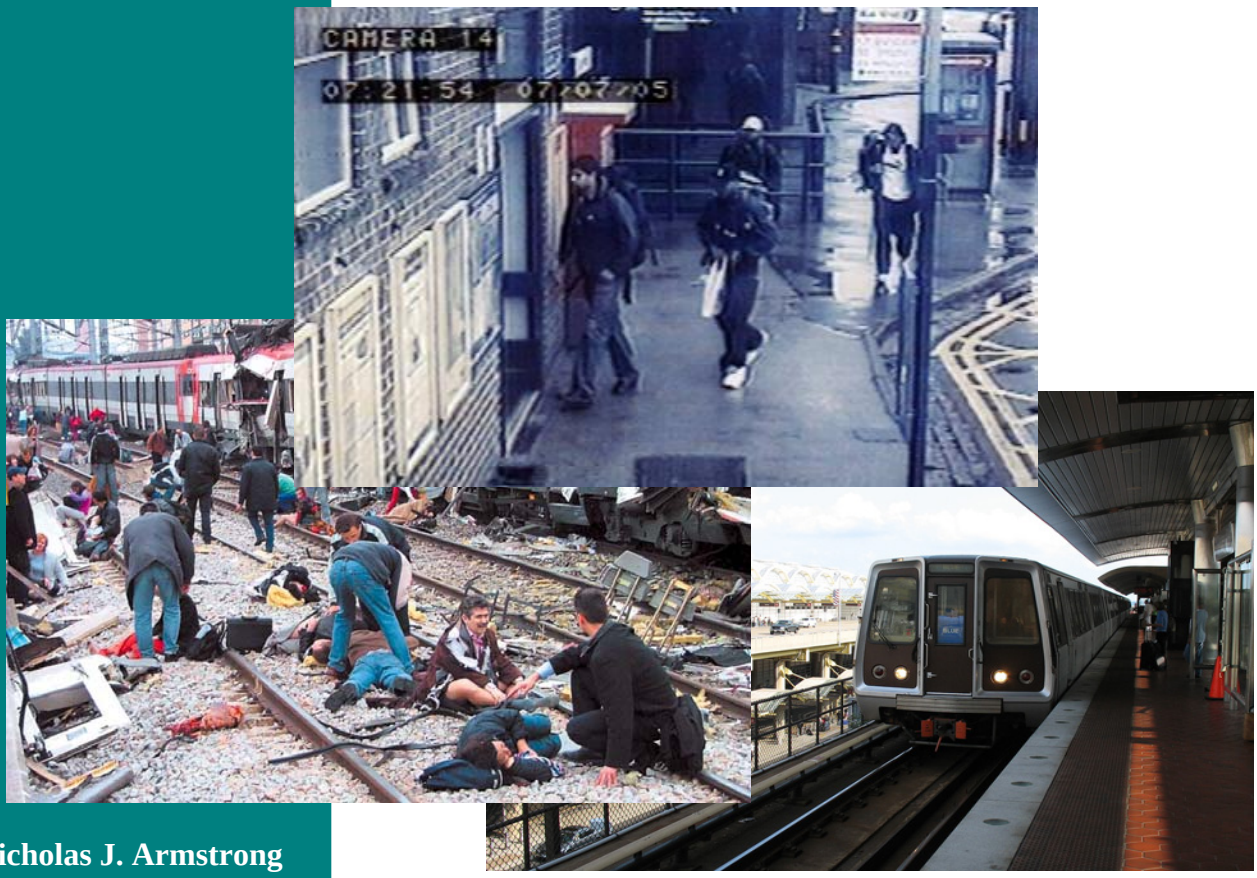
SECURING AMERICA'S PASSENGER RAILS:

ANALYZING CURRENT CHALLENGES AND FUTURE SOLUTIONS



Nicholas J. Armstrong
Drew Bland
Edward Cox
Eric Oddo
Dan Wears
P.C. Zai

June 4, 2008

Maxwell School
OF CITIZENSHIP AND PUBLIC AFFAIRS
SYRACUSE UNIVERSITY

This page intentionally left blank.

Executive Summary

Homeland security research and recent transnational terrorist trends lend credibility to the prediction that the next major terrorist attack on the U.S. homeland could be on a mass transit transportation system. Mass transit systems remain an easy target even for the terrorists with modest levels of reconnaissance and surveillance training. London, Madrid, Mumbai, Tokyo and other cities have experienced terrorist attacks on their public transportation systems. For the United States, it is only a matter of time.

Mass transit security requires a different approach than airport security. Unlike airports, mass transit systems are open with flexible schedules and multiple points of entry for a much larger number of daily passengers (3.8 ***billion*** passenger trips in 2007[1]). Consequently, mass transit security often comes at the expense of operational efficiency. For example, implementing single-entry choke points for 100 percent passenger screening at Grand Central Station during rush hour – as employed by airports – would cause crippling operational delays. Furthermore, mass transit authorities receive a sub-optimal allocation of homeland security funding with respect to risk, leaving vulnerable systems open to an attack.

The purpose of this report is to provide an analysis of domestic and international mass transit screening strategies, current and future screening technologies, and governmental challenges to and cost-benefits of enhancing rail security while maintaining as open a system as possible. In addition to discussing these critical topics and providing recommendations in the following section, this report highlights the following themes:

- A layered, system-of-systems approach to screening is most effective in a mass transit environment. The principal challenge of quick and efficient screening is in screening carry-on baggage, not passengers.
- Current technologies such as biometrics and intelligent video offer the ability to enhance current security systems in the short-term, while the advent of new technologies like Portable Explosive Detection Devices and Passive Millimeter Wave Screening will provide additional layers of security as they become more cost-effective and efficient over time.
- Federal grant funding for rail security has increased substantially, particularly in the FY 2008 Transit Security Grant Program; however, allocation of those funds are somewhat less than proportional to the risk among the recipient agencies.
- Coordination is both the problem and solution to effective rail security implementation. Local, regional, and state governments are the implementing authorities for rail security projects; it is the responsibility of the federal government to foster coordination through incentives, best practices, and supportive policies.
- A centralized clearinghouse for transit security research and best practices does not exist and U.S. government representation within international clearinghouses is weak.

Recommendations for U.S. Transit Systems

The recommendations of this report address three main categories of rail security: Rail Security Strategies, Screening Technology, and Funding & Best Practices.

Rail Security Strategies

Continue to support the implementation of an integrated systems approach to rail security. The domestic portion of this report shows that many U.S. transit systems already apply many of these methods. U.S. transit systems incorporate CPTED (Crime Prevention Through Environmental Design) into the design of new stations, develop and practice incident response programs, and seek to leverage technological solutions.

Emphasize public awareness campaigns. U.S. operators should emphasize public awareness campaigns similar to those in London and Tokyo rather than follow Madrid's policy of de-emphasizing such campaigns. As noted below, the London Underground responds to 10,000 reports of unattended bags every month. While the majority of those reports are undoubtedly not a threat to public safety, the high volume suggests an alert and proactive ridership, which increases security for the overall system.

Promote coordination between regulatory agencies and transit operators. U.S. agencies such as DHS and TSA should follow the Japanese model of consulting with transit operators to ensure new regulations and policies are feasible for implementation.

Increase security for long-distance rail service. Cities like New York and Boston have transit stations that serve as transfer points to long-distance rail service. These cities should consider following the Madrid model of establishing a passenger-only area for screening and boarding Amtrak long-distance service.

Increase international coordination. The International Association of Public Transport (UITP) is a network of over 3,000 public transportation operators, industry representatives, government agencies, and research institutes. The UITP seeks to be an international clearinghouse for best practices and a resource for the public transport industry. Although several major U.S. transit systems are members, such as New York's MTA, Boston's MBCR, and Washington, D.C.'s MTA, no U.S. government agency or transit system operators are represented on the UITP's Commission on Security. In contrast, each of the four international cities studied for this report has one or more representatives on the UITP's Commission on Security.[2]

Consider a program similar to the Registered Traveler program in the aviation transportation industry. As the Registered Traveler program continues to evolve in the aviation industry, it may be feasible to implement a similar program for mass rail transit. This could expedite security screening for regular commuters, and increase the ability of security personnel to focus on other individuals.

Screening Technologies

Congress and the Department of Homeland Security should liaise with the Millimeter Wave market's major competitors, such as Brijot, Millivision, QinetiQ, Thruvision and Trex, in order to monitor their technological progress and effectively communicate the crucial need to maintain throughput and reduce investment costs.

Implement biometrics technology to increase security of transportation personnel. By adding a layer of biometric technology, physical security of sensitive areas, such as control panels, can be greatly increased. With the additional layer of security, it will become more difficult for unauthorized individuals to interrupt transportation services.

Add biometric sensors to ticket turnstiles. Adding this sensor provides the capability to scan transit users' information against information of known terrorists. Scanning individuals against lists of known terrorists will increase security and reduce the likelihood of attack from known terrorists.

Continue investing in DHS Future Attribute Screening Technology. If DHS is able to produce such technology, significant security gaps can be closed. Having the capacity to screen the future intent of individuals would remove the need to have information on previously known terrorists, and enhance the ability to screen all passengers.

Add intelligent video software to existing CCTV networks to enhance the capabilities, effectiveness and efficiency of security cameras. Coupling of these two technologies will shift the focus of CCTV from a response and deterrent security measure to a preventative measure.

Refrain from investing in Passive Millimeter Wave Screening immediately, due to the relatively exorbitant costs and projected inefficiencies in baggage screening. This technology has the potential to be a formidable and reliable primary or supplemental resource for screening passengers in heavy rail systems throughout the United States because it provides security while maintaining privacy. However, current costs and throughput efficiencies are prohibitive.

Refrain from investing in Portable Explosive Detection Devices until a vapor-based system, which would sample the air surrounding the package without touching it, is perfected. While the current technology is reliable, affordable and mobile, its major flaw is the prerequisite that all suspicious packages have to be manually swabbed prior to inspection. This necessity would be eliminated by the development of a vapor-based detection system. While EDDs could not function as the primary screening technology in urban mass transit systems, they could be a valuable tool for security personnel in applying discretionary searches of suspicious luggage/passengers.

Funding and Best Practices

Congress should do everything in its power to sustain the total upward trend in rail security funding. Transit authorities are still short their required funding to sustain their long-term security-related investments despite significant Transit Security Grant Program (TSGP) increases in recent years. Even after the substantial FY08 TSGP increase, several of our most at-risk urban areas still do not have funding commensurate with their share of the total national risk from terrorist attacks.

Increase funding for training. Evidence suggests domestic transit agencies are willing to increase their training, but lack of funding is a prohibitive obstacle. Although training is but one security option among many, it is broad enough to increase the effectiveness of almost every other option, including technology-based improvements.

DHS must improve upon its risk-based funding methodology to ensure its funding priorities are aligned with strategic goals and nationwide target capabilities for transit security. This step will not only more effectively improve the nation's overall preparedness level through projects targeting national capability gaps, it will help to further reduce any opportunity for unnecessary 'pork-barrel' security spending better allocated to an area of higher risk.

DHS should develop a more detailed and comprehensive list of project priority groups. Considering the range of operational and capital strategies and technologies available discussed throughout this report, grouping project types into four possible priority categories seems rudimentary. Even with other variables in the project scoring function, the suggestion that a public awareness campaign and employee training are equally effective in reducing risk is doubtful.

Centralize existing best practices research clearinghouses into one body. While evidence suggests that transit agencies share information, they often receive too much information to process efficiently due in part to the variety of existing research centers.

Strike a balance between standardization and experimentation when using best practices research. Although best practices should be integrated to the fullest extent possible, new security approaches should be encouraged in order to further the development of best practices.

Acknowledgements

We would like to thank everyone who helped to make this report a success. Studying how to improve security for public transportation systems in the United States was a fulfilling and challenging assignment for all involved. We could not have completed this report without the assistance of several individuals whom we would like to thank.

- William Banks, Director, Institute for National Security and Counterterrorism (INSCT) at Syracuse University
- Veronique Pluviose-Fenton, House Committee on Homeland Security
- Erin Daste, House Committee on Homeland Security
- Leon Chlimper, Vice President of Global Sales and Marketing, Brijot Imaging Systems, Inc.
- Marlene Diamond, Administrative Assistant, Institute for National Security and Counterterrorism (INSCT) at Syracuse University

Thank you to everyone who took the time to speak with us about this project.

Author Contact Information

Professor William Banks, Project Advisor
Phone: (315) 443-3678
Email: wcbanks@law.syr.edu

Marlene Diamond, INSCT Administrative Assistant
Phone: (315) 443-2284
Email: mhdiamon@law.syr.edu

Nicholas J. Armstrong
Phone: (315) 443-2284
Email: narmstro@maxwell.syr.edu

Drew Bland
Phone: (330) 207-0013
Email: ddbland@maxwell.syr.edu

Edward Cox
Phone: (254) 291-2147
Email: wp54916@west-point.org

Eric Oddo
Phone: (315) 657-3562
Email: ericoddo@gmail.com

Dan Wears
Phone: (315) 323-1758
Email: wearsdh@gmail.com

P.C. Zai
Phone: (925) 200-3657
Email: pamzai@gmail.com

This page intentionally left blank.

Table of Contents

List of Figures

List of Acronyms

BIS-WDS	Brijot Imaging Systems, Inc. – Weapons Detection System
BFD	Boston Fire Department
BTP	British Transport Police
CBRNE	Chemical / Biological / Radiological / Nuclear / Explosive
CCTV	Closed Circuit Television
CERTU	French Ministry of Transportation
CPTED	Crime Prevention Through Environmental Design
DHS	U.S. Department of Homeland Security
EDD	Explosive Detection Device
EDS	Electronic Data Systems, Corp.
ETA	Basque Nationalist Separatist Organization
FAST M^2	Future Attribute Screening Technology Mobile Module
FTA	Federal Transit Administration
GAO	U.S. Government Accountability Office
ICS	Incident Command System
INSCT	Institute for National Security & Counterterrorism, Syracuse University
LLIS	Lessons Learned Information Sharing
LU	London Underground
MBCR	Massachusetts Bay Commuter Railroad Company
MBTA	Massachusetts Bay Transportation Authority
MTA	Metropolitan Transit Authority
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NYPD	New York Police Department
RATP	*Regie Autonome des Transports Parisiens* (Autonomous Transit Operator of Paris)
RENFE	*La Red de los Ferrocarriles Españoles* (Spanish National Rail)
RTSWG	Regional Transit Security Working Group
SAA	State Administrative Agency
SCADA	Supervisory Control and Data Acquisition System
SNCF	*Société Nationale des Chemins de fer Français* (French National Railway Company)
SPOT	Screening Passengers By Operation Techniques
TCL	Target Capabilities List
TCLDR-GCC	Transit, Commuter and Long-Distance Rail Government Coordinating Council
T-DAR	Tailgating Detection, Alarm and Recording System
TfL	Transport for London
TSA	Transportation Security Agency
TSGP	Transit Security Grant Program

List of Acronyms (cont.)

TWIC	Transportation Worker Identification Credential
UITP	International Association of Public Transport
VIGIPIRATE	French National Alert System
VIPR	Visible Intermodal Protection Response Team
WMATA	Washington Metropolitan Area Transit Authority

Introduction

On July 7, 2005, Islamic extremists attacked three London Underground locations and one bus, killing 37 people and injuring 700 others. This attack is only one example of terrorists targeting public transportation systems; there have been over 800 such attacks since 1970.[3] The fact that the United States has not suffered a terrorist attack on a public transit system is not because the U.S. is not targeted. In 1993, Islamic extremists planned attacks on New York City's tunnels and bridges. In 1997, Islamic terrorists planned suicide bombings targeting New York City's subway system. There have been at least six attempted terrorist attacks thwarted in New York City since September 11, 2001, some involving rail and mass transit.[4] It is not a question of whether terrorists will target public transit systems in the U.S. but rather when they will do so and succeed.

When an attack is attempted, failure to detect and stop the attack could have catastrophic consequences in terms of human lives, economic losses, and psychological damage to Americans' sense of security. The size and prominence of the target will affect the number of possible lives lost. The number of people who travel through New York's Penn Station every morning, for example, is equivalent to the number of passengers who pass through Chicago's O'Hare airport every two and a half days.[5] An attack that targets subway stations near major financial centers such as the New York Stock Exchange or the Chicago Stock Exchange could also have major economic impacts. In the week following the terrorist attacks of September 11, 2001, U.S. stocks lost $1.4 trillion in value.[6] While an attack on a subway system is not likely to result in four days of lost trading as the attacks on the World Trade Center did, any attack will cause death, injury, damage to infrastructure, and widespread disruption in a major urban center.

In recent years terrorists have targeted public transportation systems in London, Paris, Tokyo, Madrid, Moscow, and Mumbai. In 1991, public transportation systems were the target of 20% of all violent terrorist attacks. By 1998 that figure had increased to 40% of all violent attacks. Additionally, "the largest percentage (46%) of terrorist attacks against public surface transportation systems [were] carried out on subways and trains, subway and train stations, and rail."[7] These figures indicate that public mass transit systems are more vulnerable to terrorist attacks than aviation transportation. Brian Jenkins wrote that,

> "For those determined to kill in quantity and willing to kill indiscriminately, public transportation is an ideal target. Precisely because it is public and used by millions of people daily, there is little security, with no obvious checkpoints like those at airports to inspect passengers and parcels. Passengers are strangers, promising attackers anonymity and easy escape. Concentrations of people in contained environments are especially vulnerable to conventional explosives and unconventional weapons. Attacks on public transportation, the circulatory systems

of urban environments, cause great disruption and alarm, which are the traditional goals of terrorism."[8]

Many of the security measures implemented at airports cannot be fully implemented at all stations in a mass transit system because of a vast difference in the volume, duration, and nature of mass transit service. New York City's subway system has approximately as many subway stations as the number of commercial airports in the entire United States.[9] Over 10 billion passengers used mass transit systems in the United States in 2006. "To put the 10.1 billion public transportation trips in perspective, transit trips outnumber domestic airline trips by 15 to one."[10]

Attempts to employ airport security measures in mass transit systems would be cost-prohibitive and impractical. Boarding stations for subway and rail systems range from small and accessible platforms to vast hubs like New York's Penn Station, and unlike the aviation industry the links between stations (the rails themselves) are often open and undefended as well. Security measures common at airports, such as searching each individual and their bags using x-ray machines, metal detectors, and security personnel are infeasible for public transit systems designed to be rapid and efficient. Thus the security challenge for public transit systems is to strike a balance between security and efficiency. No security system can completely eliminate the risk of a terrorist attack on a public transportation system, but "good security measures can make terrorist operations more difficult, increase the terrorists' likelihood of being detected and identified, keep casualties and disruptions to a minimum, reduce panic, and reassure alarmed passengers in a crisis."[11]

Assessing risk is an important aspect of designing security systems and public transportation mass transit systems are no exception. It is a fair question to ask whether mass transit systems are at risk of a terrorist attack before committing additional resources towards preventing such attacks. This paper concludes that mass transit systems are at risk, especially in large urban centers. This risk can never be completely eliminated, but much more can be done in terms of both prevention and response measures.

Current Strategies in U.S. Rail Transit Security

This section provides an overview of current domestic passenger rail security practices and addresses GAO recommendations on how to incorporate foreign practices into domestic security operations.

Overview of Current Strategies

Domestic mass transit agencies have used similar security strategies since 2001 without significantly reducing operational efficiency.[12] These actions can be grouped into three categories: process-based improvements, technology-based improvements and facility improvements.[13] No single category provides complete security. Rather, agencies use strategies from each category in combination to comprise a multi-layered security strategy as recommended by DHS.[14]

Agencies have also cooperated to form security plans. Each of the 50 largest transit agencies have developed emergency response plans and have had those plans audited by FTA.[15] This coordination may have positive spillover effects for information sharing for best practices.

Process-based Improvements

Process-based improvements have been the most common type since 2001. They have less impact on the operational efficiency of a given transit system. They are also visible to transit system users, simultaneously providing a sense of security and a deterrent to terrorists and criminals. A good example is Visible Intermodal Protection Response (VIPR) Teams, which use canines, inspectors and marshals, among others, to provide a surge of deterrent presence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities.[16]

Federal support has been a catalyst for the growth of the use of canine units. Section 1309 of Implementing Recommendations of 9/11 Commission Act (P.L. 110-53) requires an increase in use of canine units. At the federal level, this is facilitated primarily through TSA's National Explosives Detection Canine Team Training Center. As of February, 2007, TSA has trained and provided 53 units to 13 major transit agencies[17]. In a 2006 report, GAO found 21 of 32 cities it surveyed used canine units.[18]

In addition to increasing the quantity and visibility patrols, many cities have increased training. This can take many forms. Training can focus on prevention and detection of attacks before they occur, improve overall response capacity, and enable security officers to make better use of available technology.

One specific type of training focused on prevention and detection is behavior recognition training. Many variations exist, but the most widely implemented is TSA's Screening Passengers by Operation Techniques (SPOT) program. Under SPOT, security officers are trained to identify involuntary physical and physiological reactions that people exhibit in response to a fear of being discovered.[19] SPOT is currently in use in 40 airports nationwide and has also been used in Boston subways. A lawsuit has been filed in U.S. district court challenging the constitutionality of behavior recognition training in Boston on the grounds that such training is tantamount to racial profiling.[20]

Establishing and sustaining effective, comprehensive security training is costly. This is particularly true for frontline employees given the need to backfill these positions and provide overtime pay for actual training.[21] According to a 2007 FTA report, most domestic agencies can only afford to train new employees during orientation.[22] MBTA estimated $750,000 annual spending for its security training center.[23] This is an area where the federal government can help local agencies by providing funding.

Background checks and access control are another popular process-based improvement. Of the 32 cities analyzed by GAO in 2006, 23 implemented some type of access control. This often involved installing a system requiring employees to swipe an access card to enter control rooms, repair facilities, and other key locations.[24] Access control can be integrated with background checks very easily. For example, TSA's Transportation Worker Identification Credential (TWIC) program for airport screeners and maritime transportation workers investigates current and prospective rail-operation and security personnel. Those that do not meet screening requirements are either not hired or given restricted access.

Technology-based Improvements

The use of technology in securing passenger rail systems is growing. Closed circuit television (CCTV) surveillance cameras and chemical/biological/radiological (CBR) detectors have received the most attention. There is substantial debate about the limitations of CBR detectors and the manpower required to operate a comprehensive CCTV system. However, CCTV has become a staple of American mass transit security due in part its applicability to fighting general crime.

Almost all domestic transit agencies have implemented CCTV surveillance systems.[25] Many agencies used CCTV even before 2001 because it is also effective in fighting general crime. However, this has led to the use of outdated technology that is systematically difficult to integrate into a post-2001 security strategy. A 2007 FTA report cited these reasons as primary causes of the varied effects of CCTV systems across the 50 largest transit agencies.[26] Indeed,

GAO reported many rail operators often use CCTV as a deterrent due to the staff resources needed to monitor video feeds.[27]

New CCTV technologies are being developed to increase the security and reduce staffing needs. New Jersey Transit has installed a system of "smart" cameras that can detect abnormal movements and objects and alert officials.[28] New cameras are being developed that have thermal imaging technology to detect suspicious objects, although they are costly.[29]

Domestic agencies have been exploring CBR detectors since the Tokyo subway attack, but implementation has been limited due to cost. The Washington Metropolitan Area Transit Authority (WMATA) has been the most active. WMATA was the first domestic agency to install chemical detectors in 1999 under the PROTECT program and now has chemical detectors in at least 12 subway stations. Boston has also used chemical and biological detectors in its stations, but details of the program are classified.[30] CBR detectors can also be used in post-blast analysis of blast residue to collect evidence.[31]

WMATA's PROTECT program is the only systems-based approach[32] to integrating chemical detectors into a security strategy. WMATA's partnership with the FTA, the National Institute of Justice and the Department of Energy enabled greater federal funding to ameliorate the cost issue. When PROTECT is triggered, video cameras verify the attack, alarms sound at the subway operation command center, and operators are directed through a set of optimized responses shown on computer screens. In this example, the effectiveness of a multi-layered security strategy is clear. The chemical sensors work better when augmented by smart cameras, which, in turn, are more effective when used by trained human agents.

CBR detectors have their limitations. They can detect the presence of a CBR substance, but often cannot identify a precise source as a canine could. Portable detectors ameliorate this problem. For example, WMATA recently purchased hand-held portable detectors for its agents.[33] Ultimately, detectors are most effective when used in combination with canine units and camera systems.

Facility Improvements

The physical design and inventory of a transit station can improve the security of that station. This is commonly known as Crime Prevention Through Environmental Design (CPTED). It is more feasible to incorporate these into new buildings than retrofit them.

Domestic agencies have instituted variations of this approach. The GAO reported in 2006 that 22 of the 32 domestic agencies it surveyed were incorporating security design into new or existing structures. These included increasing visibility for onboard staff and cameras,

reducing the areas where someone could hide an explosive device, and enhancing emergency exits in transit stations.[34] For example, in 2004, FTA directed domestic agencies to use clear and bomb-resistant trash bins. Another innovation is installing vending machines without holes and with sloped, rather than flat, tops to eliminate hiding places for explosives. Visibility can also be increased by reducing columns inside stations and improving lighting. Figure 6 is taken from a FTA report and lists various design options for rail stations.

Figure 1. Transit Design Considerations
(Source: Table 6-2, FTA. "Transit Design Considerations." Nov. 2004.)

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Structures set back from roads and parking areas, if applicable	Deter/Minimize	
Physical barriers such as bollards, road spikes, and fencing to enforce setbacks and/or prevent ramming	Deter/Minimize	X
Minimum number of vehicle entrances	Deter/Detect	X
Unobstructed sightlines surrounding the station	Deter/Detect	X
Interior Layout		
Interior station layout provides unobstructed sightlines, minimizing hidden areas or remote passageways	Deter/Detect	
Kiosks, ads, and information positioned to not disrupt sightlines	Deter/Detect	X
Minimum use of columns and blind corners	Deter/Detect	
Security mirrors on columns and corners	Deter/Detect	X
Operator booth positioned for maximum presence and visibility within station	Deter/Detect	
Critical assets buffered from public or vulnerable areas	Deter	
Non-public facilities hidden and not identified	Deter	X
ADA-complaint emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Critical equipment secured with gates, locks, or other access control measures	Deter/Detect	X

Figure 1. Transit Design Considerations (continued)

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Dimensions of station entrances limit permissible vehicle size	Deter	X
"No Trespassing" signage	Deter	X
Posted or broadcasted instructions on how to report suspicious activity	Deter/Detect	X
Bright paint colors to increase ambient lighting	Deter/Detect	X
Vulnerable features designed to channel blasts	Minimize	
Shatter-proof glazing	Minimize	X
Façade materials that resist explosive blasts	Minimize	
Materials that do not absorb toxic substances when exposed	Minimize	Maybe
Fire-retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		
Appropriate surveillance at entrances, at access points to non-public areas, and throughout the station	Deter/Detect	X
Sufficient lighting for nighttime surveillance	Detect	X
Motion detectors or intrusion alarms on vehicle entrances	Detect	X
Intrusion alarms at access points to non-public areas	Detect	X
Communication links from remote station areas to station personnel (such as call boxes and a public address system)	Detect/Deter	X
Communication links to administrative and emergency response centers	Detect/Deter/ Minimize	X
Backup emergency lighting	Minimize	
Fire detection and suppression system	Minimize	X

Addressing GAO Recommendations

In a 2006 report, the GAO identified three foreign practices that were not in use domestically: random screening, a national research clearinghouse and covert testing. Information on the extent to which domestic transit agencies use covert testing was largely unavailable due to its classified nature. As of 2008, multiple research clearinghouses exist[35] within DHS, but they are designed for different audiences. There is a need for centralization of these bodies to reduce information overload.

The Next Frontier: Passenger Screening

The strategies outlined in the preceding overview do not impose significant delays on the operation of a transit system. However, transit agencies and DHS are working toward developing ways to screen passengers in mass transit settings as they do in airports. There is widespread agreement within the field that screening every passenger with existing technology is

infeasible because of the inherently open and dynamic nature of urban mass transit.[36] Thus, effective screening techniques will strike a balance between security and efficiency.

One attempt to strike this security/efficiency balance is to conduct random bag screens. Boston randomly screened bags during the 2004 Democratic National Convention.[37] New York City began a permanent random screening policy shortly after the July 2005, London subway bombings.

The constitutionality of these random searches was upheld by the United States Court of Appeals, Second Circuit in *MacWade v. Kelly*, 460 F.3d 260 (2006). The court ruled the government's interest in preventing a terrorist attack in New York City's subway system was "vitally important" and outweighed the minimal invasion of passengers' privacy.[38] The court also noted that subway users had a walk-away option. Posted signs alerted them to the prospect of the search and users had the option to walk away from the station to use other means of transport and avoid the search. Upon entering the station, they consented to the search.

The security benefit of random screening is unknown. The randomness of the searches provides a deterrent. The presence of the searching and the officers is designed, in part, to make the public feel safer.[39] However, the number of officers conducting the screening is sometimes perceived as too small. In 2005, a Washington Post reporter described a "handful of officers" overwhelmed by "a river of commuters" at a New York City station.[40]

Random bag screening does provide an increased level of security with minimal operational delays, but delays increase with the number of screens. Technology can be used to narrow down which passengers to screen, but this is a systematic passenger screening system rather than a random one. For example, smart cameras could identify a passenger as a potential threat that could then be pulled aside and screened by an existing random screening unit already in the station.

Research Clearinghouses

National research clearinghouses also exist, but there does not appear to be a single central clearinghouse. This has contributed to an information overload that burdens transit agencies. Evidence suggests many agencies do not have the resources to digest the information they need to make informed decisions about their security policies.[41]

DHS operates Lessons Learned Information Sharing (LLIS.gov), a national online network of Lessons Learned and Best Practices for emergency response providers and homeland security officials that is peer-validated by homeland security professionals. DHS also operates

the Homeland Security Digital Library, which provides policy and strategy documents for academics and practitioners.

The federal government should be aware of the limitations of implementing best practices. Local agencies have authority over their own security practices. The federal government cannot force local agencies to implement a particular practice, but they do control the purse strings. In the past, this has been used to push through particular policies the federal government supported but could not mandate (55 mph speed limits, 21 year-old drinking age). A similar approach could be taken in the security realm. Discussed in further detail in the following section, DHS now requires all transit authorities to have a current and validated emergency response plan to be eligible to receive transit security grants.

A careful balance should be struck between standardization and variation in security practices. Variation in security methods could be a positive because it fosters creativity and best practices. In addition, agencies vary in terms of their level of security and sophistication, which diminishes the feasibility of standardization.

International Efforts to Secure Rail Transit

This section provides an assessment of implemented rail security strategies and common features among major foreign cities facing similar threats from terrorist attacks. The common features of these cities are a good reference for future planning in U.S. systems.

Paris, France[42]

Background

The French government increased security following a series of bombing attacks carried out by Algerian Islamic extremists in 1995 and 1996.[43]

Overlapping Jurisdictions

The Office of the Prime Minister and the Ministries of Interior, Defense, and Transportation are now involved in a hierarchical system of interlocking security plans. RATP and SNCF are transit operators in Paris and each maintains a security office that coordinates closely with the government security offices. "Comprehensiveness, coordination, communication, and the adoption of a systemic approach" are the keywords used by French officials in describing their security planning priorities.[44]

Security Systems

The French national alert system, known as VIGIPIRATE, calls for patrols by both civil police and French military forces of symbolic monuments and subway metro stations in Paris.[45] Like most transit authorities around the world, Parisian planners divide their time between attack prevention and response planning. The Paris Metro employs human detection and prevention measures such as uniformed and plain-clothes attendants equipped with two-way radios. They also use technologies like CCTV cameras and locks on trains and platforms that can be remotely activated to prevent terrorists or criminals from escaping. Construction of new subway stations relies heavily on crime prevention through environmental design (CPTED) measures. For example, new stations lack the byzantine labyrinth-like passages and tunnels of the old stations. Instead, engineers planning new stations seek to optimize fields of observation for station attendants and use shatterproof transparent fiberglass for windows instead of glass. Train doors are transparent to allow visibility of both tracks.

In October 2003, CERTU staged a nerve gas attack simulation. The French government developed a security plan for responding to chemical attacks known as "Piratox" in 2003 and also has a plan for responding to biological attacks known as Biotox.[46] Like many urban transit systems, the Paris Metro has also launched an information and security awareness campaign to

educate transit riders about how to report suspicious packages and persons, and what to do in case of an emergency on the subway train.

London, England

Background

London's transit system has been a target for terrorists for over three decades, with the Irish Republican Army routinely attacking infrastructure as part of its campaign against the British government. On July 7, 2005, London became the target of a different kind of terrorism. Islamic extremists attacked three London Underground locations and one bus, killing 37 people and injuring 700 others.[47]

Overlapping Jurisdictions

The British Transport Police have responsibility for all subway stations and rail lines both above ground and below ground in the greater London area. The Metropolitan Police are responsible for all law enforcement in the greater London area. The jurisdiction of the City of London Police encompassed the actual city of London, an area of approximately one square mile located in the center of the greater London metropolitan area. The London Underground, also known as Transport for London, maintains a security office as well.

Security Systems

The London Underground utilizes two separate sets of CCTV cameras, one to assist with rail operations and one for security. There are over 6,000 CCTV cameras and plans to emplace an additional 6,000 within the next 4 years. The feed from all cameras is transmitted to a central location controlled by the BTP. Over 600 officers of the BTP patrol the subway system, and the staff of the LU also routinely patrol their assigned stations and check station entrances.[48] All transit staff have received training on how to deal with unattended bags and how to recognize and react to chemical and biological agents. Using what is known as the HOT method, employees are trained to look for anything that's "Hidden, Obviously suspicious, or not Typical of the environment."[49]

The public education campaign in London has been very successful. The London Underground deals with 10,000 reports of unattended bags every month. Recognizing the interconnected nature of the public transportation systems in Europe, British officials place a great deal of emphasis on pan-European cooperation and information sharing. Geoff Dunmore, the Operational Security Manager of the London Underground, also serves as Chairman of the International Association of Public Transport's Commission on Security.

The London Underground is currently undergoing a large-scale renovation, and CPTED is being incorporated into the design of new stations and the renovation of existing stations. The LU has removed trash cans from subway stations or replaced them with see-through plastic trash bins. The LU utilizes redundant control rooms so that terrorists cannot shut down the entire transit system by targeting one location. In April 2005, London held a command and control simulation exercise involving all affected agencies, which contributed to their success in responding to the bombings on July 7, 2005.

Madrid, Spain[50]

Background

The Madrid transit system has been a target for domestic terrorism for the last three decades in much the same way as London. Basque separatists known as the ETA have targeted infrastructure and public officials in Madrid, and the ETA was initially blamed for an attack on March 11, 2004 on the national rail system. Spanish officials later determined that Islamic terrorists inspired by Al Qaeda were responsible for the attack that killed 191 people and wounded more than 1700 others.

Overlapping Jurisdictions

Spain has a national rail line, a commuter rail line, and a subway system operating inside Madrid. The transportation agencies look to the national government to promulgate standards and regulations.

Security Systems

Madrid's Metro security systems place less emphasis on public education than London because they fear added emphasis will result in decreased ridership. Instead, the Madrid Metro relies on transit staff and contracted private security personnel to patrol and monitor stations. RENFE and the Madrid Metro each have two personnel on the International Association of Public Transport's Commission on Security.

The Madrid Metro places emphasis on CPTED for new stations, including many of the same design features as London and Paris. While it is impractical to screen all passengers in the same way that airports conduct security screening, passengers who are travelling on high-speed rail lines in Madrid are screened into a passenger-only holding area.

Tokyo, Japan[51]

Background

On March 20, 1995, members of the religious movement Aum Shinrikyo released sarin gas in the Tokyo subway system using five coordinated attacks at different points, killing twelve people and injuring dozens more.

Overlapping Jurisdictions

Unlike Paris and Madrid, the national government in Japan plays a much smaller role in transit security in Tokyo. This is due at least in part to the diversity of transportation providers in the city. There are at least eight separate train companies and two subway companies operating in and around Tokyo. The Tokyo Metro and Toei Subway operate the majority of the public transit stations within Tokyo itself. Transit operators develop and implement their own security protocols. When guidance does come from national government, the government often first asks the transit operators whether the guidance is realistic in terms of implementation. This creates a helpful dialogue and prevents the imposition of infeasible security measures.

Security Systems

Like Madrid, Tokyo Metro and Toei Subways both rely on private security guards to patrol subway stations. Municipal police also patrol the busier stations, and Ginza and Kasumigaseki Station both have metal detectors in use to deter terrorism and crime. Tokyo has an active public education campaign directed at transit riders and employs CCTV cameras. CPTED is a key feature in the design of new stations, and trash cans have been removed or replaced with transparent trash bins in all stations.

Common International Security Features

Despite cultural and regional differences, all of the international cities studied have common security features. These commonalities fall into four categories – crime prevention through environmental design, the use of technology to enhance security, coordination between law enforcement officials and transit staff, and training exercises and simulations.

All of the cities studied seek to incorporate CPTED into the design of new stations. When possible given the constraints of cost and location, they also seek to update existing infrastructure with CPTED. Examples of CPTED include the use of transparent materials in station design, good lighting and the elimination of dark zones, and limiting the number of entrance points. New stations are designed to have clearly visible open corridors, platforms, and

waiting areas, which can be observed by transit staff and avoid unnecessary use of underground passages, footbridges, and winding corridors when possible. Elevator designs are often panoramic to allow good views from the outside. Vending machines and benches are designed to eliminate horizontal space above or beneath them that would provide concealed areas for unauthorized packages or explosive devices.

Transit systems often cross-jurisdictional boundaries of law enforcement agencies. Potential problems arising from this conflict are often addressed by close coordination between law enforcement units, government transportation agencies, and the staff of the transit system. In the cities studied, all of these disparate groups work together to establish clear lines of command and communication before an incident occurs. This coordination is enhanced by compatible communications systems and reinforced during training exercises or simulations. We note that none of these cities are in federal systems comparable to the United States. Coordination is easier for these cities for this reason. Cities, transit operators, and state and federal government agencies in the United States must work harder to achieve this coordination.

Screening Technologies

Overview

Millions of travelers utilize transportation networks with annual ridership figures in the billions. Mindful of this, it is imperative to provide the highest level of security with the least disruption to travel schedules. Unfortunately, considering the level of threat against the United States, we must continue to increase security efforts to protect our transportation infrastructure and citizens who rely upon it. With increasing costs and decreasing revenue, the United States must be careful to create a strong return on investment. As technology advances, transportation security is able to improve while limiting the affect on the ease of use of the system.

Although technology alone cannot provide a solution to the security needs of transportation systems, it is essential to maintain and upgrade our technological security measures. According to Kip Hawley, TSA Administrator, "there are three prongs to our approach to upgrade security: people, technology, and process."[52] While it is necessary to enhance all three prongs of security, technological advancements could have a significant ability to increase the effectiveness of screening passengers and employees of mass transit systems. Security can be greatly enhanced using a system-of-systems approach. As security enhancements are implemented, security personnel can be better trained and the process of screening can be refined.

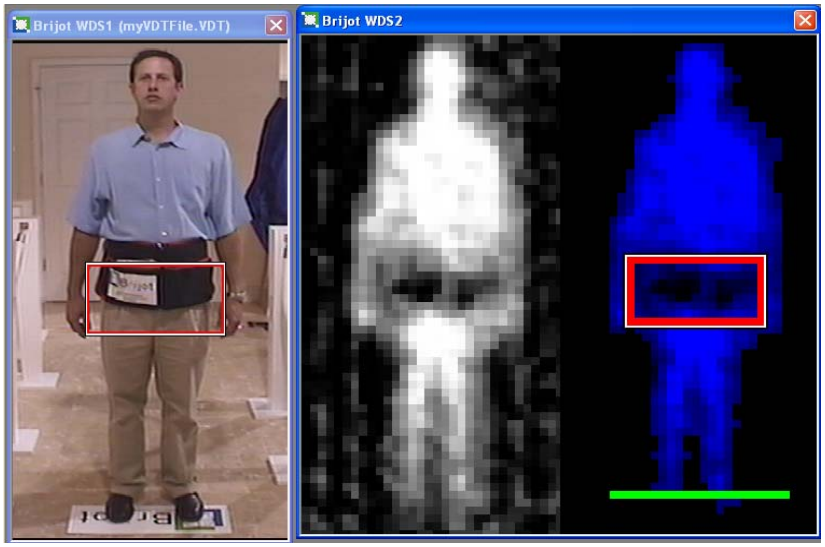
Passive Millimeter Wave Screening

An innovative and advanced form of security screening technology that is currently on the market, found predominantly in places such as international airports and federal courthouses, is Passive Millimeter Wave image screening. Millimeter waves are naturally occurring forms of electromagnetic wave energy, which, because of their relatively large wavelengths compared to the microstructure of most materials, tend to pass through such materials as clothing quite easily.[53]

Over a few seconds, this technology can detect weapons, explosives and other threat items concealed under layers of clothing, without physical contact from security personnel.[54] The system is design to detect for any anomalies against the human silhouette.[55] These anomalies are created by any suitable difference in millimeter wave emission, absorption or refraction between the subject and the object, such as thick packets of currency or paper. The three-dimensional image of the body, with facial features blurred for privacy, is displayed on a remote monitor for analysis. The system will not image a detailed form of the person.[56]

Each passenger will walk into the millimeter wave portal. Once inside, they will be asked to stand in two different positions and remain motionless for just a few moments while the technology creates a three-dimensional image of the passenger in real time. Once complete, the passenger will exit the opposite side of the millimeter wave portal. Images will be deleted immediately once viewed and will never be stored, transmitted or printed, since the passenger imaging units have zero storage capability.[57]

Figure 2. Passive Millimeter Wave Screening



(Brijot Imaging Systems)

Millimeter wave technology produces images, which are viewed by a Transportation Security Officer in a remote location. For comparison, the energy projected by the system is 10,000 times less than a cell phone transmission. Humans are exposed to millimeter wave energy on a daily basis and also generate it naturally. Hence, it is reasonable to infer that this technology will pose no safety concern to passengers.[58]

There are distinct advantages in the use Millimeter wave screening over a traditional metal detector. Walk-thru metal detectors only detect metallic threats, tell the operator minimal threat location information, possess a relatively high false alarm rate, and normally require hand-wand metal detector or pat-down for alarm resolution. There are also certain health concerns, in that there are posted warnings for pacemakers, and long-term medical concerns.[59]

An independent testing firm, Sypris Test & Management, conducted a benchmark performance measurement of the BIS-WDS GEN 2 automated detection engine that is currently being marketed by Brijot Imaging Systems, Inc. Its detection success rates were as follows: PVC Pipe Bombs (99.7%), Metal Pipe Bomb (99.8%), C4 Explosives (91.2%), Liquid Explosives (86.1%), and Combined Bombs (94.2%). In addition, it detected small knives at a

rate of (35.8%), small handguns (63.6%), large handguns (87.4%), and combined weapons (75.6%). The false alarm rate was roughly 5 percent.[60]

Figure 3. BIS-WDS Gen 2 by Brijot Imaging Systems, Inc.

(Brijot Imaging Systems)

There are certain areas where this technology struggles. For example, it is very sensitive to temperature, in that room temperatures should not exceed 80 degrees Fahrenheit (26 degree Celsius). There must be a contrast, or a difference in temperature, between the human and background in order for the screening to be successful.[61] In the event that the differential between the temperature of the object and the person is less than one degree Kelvin, the detection rate of the camera will be degraded. Millimeter wave screening cannot see through humans, so it is susceptible to a suspect hiding controlled substances in a body cavity.[62]

Our recommendation regarding Passive Millimeter Wave screening is one of hesitant optimism. As of today, it has not yet been integrated into any heavy rail systems domestically or abroad. We believe that down the road, it could be a formidable and reliable primary or supplemental resource for screening passengers in heavy rail systems throughout the United States. It passes the security, safety and privacy tests, but based on our observations, currently struggles in the area of cost-effectiveness and throughput efficiency. For example, the installation of one four-lane BIS-WDS GEN 2, which Brijot Imaging asserts can screen 2,880 passengers per hour, costs approximately $450,000 (before training and engineering costs, as well as the X-ray machine that screens passenger's bags).[63] To use the New York City subway as an example, it would cost approximately $210 million in installation costs (based on 468 stations) for each station in the five boroughs to be equipped with Millimeter Wave technology.

Because this technological market is still in a relative stage of infancy, the costs seem to be comparatively high. There are a number of companies, such as Brijot, Millivision, QinetiQ, Thruvision and Trex that are vigorously competing for the lion's market share of this technology. As the technology matures and competition becomes more dynamic, it is anticipated that prices will inevitably drop. In addition, there is ample doubt as to whether the infrastructure required for Millimeter Wave screening could be a feasible solution in tight, chaotic quarters of metropolitan subway stations found in New York City or D.C. It would require a fundamental shift in the daily routines of subway commuters, as they have grown strongly accustomed to freely moving in and out of stations without any delay. In conjunction with Brijot Imaging, the New York/New Jersey Port Authority has run a pilot program using passive millimeter wave technology. In short, we believe that this technology has significant potential, but would not offer our full endorsement until numerous matters are ironed out and fine-tuned.

Portable Explosive Detection Devices

In 2004, the Transit Cooperative Research Program, in conjunction with the Federal Transit Administration, conducted a thorough analysis of the applicability of Portable Explosive Detection Devices in mass transit environments. The report was directed toward a range of audiences within the transit community with a collective interest in transportation security.[64]

Regarding mobility, the study found the portable EDDs to be lightweight and very transportable. During this study they were carried in-between stations and set up, on average, eight times per day. There was no indication of operator fatigue in carrying the approximately 21 pounds of equipment, which included the detector, cord, battery, and wipes.[65]

The portable EDDs tested in this study proved reliable. They had no systematic failures and were able to operate well for extended periods of time. During this study, the devices were operated in the field for a total of 140 hours over a 17-day period. In 1,600 individual tests, conducted under an extensive range of environmental conditions, no systematic failures were noted. A concern with portable instrumentation operating in the field is battery lifetime and the need to carry spares.[66]

One aim of this study was to expose unfavorable conditions that could adversely affect the EDD's performance. These conditions might include operation where external fumes exist. The false positive alarm rate noted in this study was a relatively minor (1.7%) and is consistent with the false alarm rate seen at airports with trace detection equipment currently in use.[67]

Figure 4. Portable Explosive Detection Device

(National Instruments)

The cost and time commitment is minimal, and the training seminar provides the operator with a solid foundation for handling the equipment effectively. Currently, there are different training packages provided for the selected device. The cost can range from $1,500 to $2,800, depending on the type of training that is utilized.[68] The manufacturer had not established the need for an annual maintenance cycle. Consumables for the detection equipment tested include batteries, wipes, and filters. The cost of these for one week of heavy operations, as in this study, was estimated to be $90.[69]

In order to conduct a test, a swab is rubbed by hand over the article being tested. This requires the operator to have to handle the package extensively, but it does not require the operator to open the package. In cases where the transit official deems a package harmless and the operator is going to open it or dispose of the article, it is not necessary to take a swab sample.[70]

However, in the case of a suspicious abandoned package, the operator may make the decision not to handle the package for safety reasons. In this case, the trace detection equipment provides diminutive usefulness. The extensive handling necessary with use of detection equipment may be deemed unsafe, and the official has no alternative other than calling for Explosive Ordnance Disposal personnel to examine the object using dogs or X-ray equipment.

It is possible to use portable detection equipment to screen passengers, but there are severe limitations with this use. The first limitation is the throughput. The study concluded that while the average inspection time of 84 seconds is not significant for inspecting an abandoned

package, it is a considerable period of time for a commuter who needs to board a train, not to mention the amount of time spent waiting in line to be inspected.[71]

We conclude that portable Explosive Detection Devices could in fact have a niche within rail and subway systems, albeit a limited one. As of 2008, it has been utilized in both Washington, DC and Boston. EDDs are relatively inexpensive, mobile, and convenient security tools that are quite reliable. Unfortunately, they have two glaring weaknesses that prevent their widespread implementation throughout American heavy rail systems. First, as just mentioned, it is completely unrealistic to expect these devices to screen every single passenger. To spend 84 seconds on each of these individuals would create disastrous delays and inefficiencies. Therefore, while EDDs could not function as the primary screening technology in urban mass transit systems, they could be a valuable tool for security personnel in applying discretionary searches of suspicious luggage/passengers.

Second, EDDs are ineffective in examining bags without first applying a swab over the article. The Transit Cooperative Research Program suggested that a vapor-based system, which would sample the air surrounding the package without touching it, would be superior.[72] The problem is that modern explosives are not very volatile, and the existing equipment does not have the sensitivity to detect the explosive vapor directly. It seems highly counterintuitive that a device used to detect explosives would be virtually obsolete if a security officer believed that a suspected piece of luggage could potentially explode.

Biometrics

The study of biometrics can date back into the early 20th Century, and as it continues to advance, its uses have expanded. "Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic: a measurable biological anatomical, physiological, and behavioral characteristic that can be used for automated recognition. As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."[73] Biometrics can use many different measurements of the human body including, but not limited to, fingerprint analysis, facial recognition, iris scanning and hand geometry. The technology is also capable of indentifying individuals of interest and confirming the identities of transit staff in order to control access to critical areas.

Biometrics is currently employed within the Transportation Worker Identification Credential (TWIC) program. Biometric information is required to obtain the necessary credentials to gain access to secure areas. With the use of these credentials, individuals are able to gain unescorted access to secure areas of ports. Following the full implementation of TWIC

in port areas, DHS plans to assess the viability for other transportation networks.[74] The extension of this program could provide vital security to mass transit systems.

Biometrics technology can aid security efforts in transit systems by comparing individuals who enter the system against known terrorist lists. The major disadvantage to this system is that in order to be effective, security agencies must have biometric information, such as photographs or fingerprints, of known terrorists. Not all terrorists are known, and there may be missing information, which could lead to a false sense of security. The implementation of biometric technology will not produce increased security against unknown individuals.

The most effective use of biometric technology is related to employee security. In an effort to increase employee screening, biometrics can be used to verify the identity of employees who wish to gain access to secured areas. This would reduce the potential risks of lost or stolen identification cards and add an extra layer of defense to sensitive areas.

In addition to implementing biometric technology to increase employee security, mass transit systems may be able to create a program similar to the Registered Traveler program, which is in a pilot phase in the aviation transportation industry. A similar registered commuter program could add biometric sensors to the ticket turnstiles in the rail stations, which could allow security screeners to focus on travelers who do not regularly travel on rail systems. The program implemented by Electronic Data Systems, Corp. (EDS) for TSA at select airports allows for streamlined security screening for registered travelers who travel at least once per week.[75] A similar program for rail security could be more restrictive to commuters who use the mass transit multiple times each week. Such a program may not be feasible, it is recommended to monitor the current aviation program and make future assessments. Although the use of biometric technology is limited, it can still be an effective tool to increase the security of mass transit systems. Further, the implementation of biometric security may also provide political obstacles as some individuals are concerned about the storage of such information. As biometric information is gathered the storage and removal of such information could generate controversy.

FAST (Future Attribute Screening Technology)

"While it is necessary, it is no longer sufficient to focus on finding weapons and common explosives; we must enhance our ability to recognize suspicious behavioral patterns and demeanors to identify people who may have devised a new means to attack our transportation systems or passengers."[76]

The Science and Technology Directorate of the Department of Homeland Security (DHS) has undertaken a significant investment into technology that can provide additional security to the

Figure 5. Biometrics Overview[77]

transportation industry, while decreasing the inconvenience to passengers. With the creation of the Future Attribute Screening Technology Mobile Module (FAST M^2), DHS has developed a "means for research, development and integration of new behavior/physiological based screening methods for field use in multiple low and high traffic venues."[78] The FAST M^2 system combines multiple technologies to provide the capacity to screen both known and unknown threats to security. Included are, "Current/Future Observation Techniques, Hostile Intent Detection Technology, Physiological Sensors and, Interviewing/Questioning Techniques."[79] DHS has multiple goals associated with the development and testing of FAST M^2:

- Improve user experience and throughput
- Automate behavior based screening techniques
- Validate technical requirements analysis
- Establish performance metrics for screening systems[80]

The implementation of the FAST M^2 technology can provide significant resources to ease the concerns of the transportation industry. With future development of this technology, transportation systems will not need to rely on terrorist watch lists and other previously known information. Relying on this information provides a significant gap in security that could allow undetected access to carry out attacks. This technology can close the gap that still exists with the use of biometrics technology on its own. Since this technology is still in development and information is limited, it is difficult to assess potential costs, specifically the delays in transit created by increased screening. Theoretically, the concept behind FAST M^2 technology appears to provide significant security measures that are currently lacking. DHS should continue to invest in this vital technology that could potentially have a huge impact on future security screening capabilities.

Intelligent Video

Video surveillance is not a new technology that is going to provide preventative security measures to transportation systems, but with the way in which video surveillance has begun to revolutionize, there is the potential for increased security without hindering the use of mass transit systems by the public. Traditionally, video surveillance has been used as a deterrent to crime as well as a tool to determine the source of criminal activity. Since, video provides "real-time" data; there is room for this technology to improve the capabilities of law enforcement agencies and their ability to detect potential incidents. Recently, video surveillance has been used in "real-time."

Current video surveillance techniques typically entail one or more individuals monitoring up to hundreds of video feeds into a central location. "No matter how highly trained or how dedicated a human observer, it is impossible to provide full attention to more than one or two things at a time; and even then, only for a few minutes at a time."[81]

Software advancements have produced automated video surveillance, which allows the computer software to assist in monitoring the hundreds or even thousands of cameras that exist in mass transit systems. The computer software is capable of monitoring video streams and detecting "activities, events or behaviors that might be considered suspicious and provide an appropriate response when such actions occur."[82] Intelligent video not only monitors the video stream, it is capable of filtering out irrelevant information, which allows viewers to concentrate on more important events.[83]

Intelligent video surveillance is capable of being tailored to existing closed circuit television systems (CCTV) and does not require the acquisition of new cameras. Furthermore, each system can be customized to detect different threats, including left-behind baggage and human actions, which are out of the ordinary. In addition to enhancing surveillance capabilities, intelligent video surveillance can also aid in maintaining secure and sensitive areas that are critical to the operations of mass transit systems.

The Massachusetts Institute of Technology, in conjunction with Newton Labs, created the Tailgating Detection, Alarm and Recording system (T-DAR). The system was developed to "detect and track the movement of people passing through secure doors and passageways."[84] This system will detect individuals who do not have authorized access, it will then begin recording and sound an alarm for further attention from security personnel. "By itself, T-DAR is primarily a detection system, but when combined with a 'mantrap' device, a double-door entry corridor where the first door must be secured before the employee can pass through the second door, it can also be used to trap an unauthorized entrant."[85] This system can aid in protecting critical control stations from unauthorized entrance and potential disruptions of service to the millions of individuals who rely on mass transportation.

Use of this technology is gradually becoming more common, and it will continue to develop in the near future. It has been suggested that the capabilities and applications of intelligent video surveillance will double every 18 months. Despite the infancy of this technology, it has been deployed in multiple settings. Specifically, ObjectVideo, Inc. systems have been used by the National High-Speed Railway in Spain. There the technology was used to help better protect some of Spain's busiest high-speed rail lines against terrorist attack, theft, vandalism and provide employee safety. Intelligent video surveillance was used to monitor perimeters, loitering and objects left on tracks. This screening technique is employed as one of many layers of security, to mass transit systems as well as inter-city transportation and freight rail.[86] Similar technology has also been used domestically by the New Jersey Transit Authority. Applying this technology to mass transit, will increase the effectiveness of CCTV, and potentially allow security personnel to prevent events from happening, rather than using this technology as a resource. Since most of the infrastructure required for this technology is currently in place, investments to increase the use of CCTV systems would be minimal. With

the minimal investment and interruption to service, each mass transit system should be actively engaged in enhancing their CCTV capabilities.

Screening Technology Observations

Although the desired end-state of achieving 100 percent security in a mass transit environment is nearly impossible, advanced screening technologies can be integrated into current systems to enhance security. Biometrics (DHS/TSA TWIC Program) and intelligent video (New Jersey Transit, Spain) presently offer an additional capability to strengthen current rail security systems. As cutting-edge technology advances and decreases in cost over the coming years, Future Attribute Screening Technology, Portable Explosive Detection Devices (Boston, Washington, D.C.) and Passive Millimeter Wave (NY/NJ Port Authority Pilot Program) will likely serve to augment as additional layers of security. The federal government should aggressively collaborate with private sector companies in an effort to bring these technologies to rail systems in an expedited and cost-effective manner.

Figure 6. Screening Technology Advantages, Disadvantages, & Recommendations

Passenger Rail Security: Cost versus Benefit

This section discusses why a straightforward comparison of benefits minus costs among security options is not feasible and why the risk-based approach is more effective.[87] Costs of a security improvement can be measured relatively easily and many estimates of these costs are readily available. Benefits are much more difficult to measure, but come in essentially three forms: decreased probability of an attack (prevention), decreased consequences of an attack (mitigation) and decreases in general crime.

Generally, analysts should weigh the costs of purchasing and maintaining the improvement within the context of the fiscal climate and the level of risk associated with a particular agency against the decreased probability and consequences of an attack. Most improvements do not simultaneously address prevention and mitigation, so security improvements should be considered as part of a systems-based approach. Choices are not usually about one technology versus another, but how choosing two or three as a package will benefit the agency.

It is important to note that agencies' choices about particular technologies will always be made within the context of their existing security, which varies from one to another. For example, new chemical detectors may be more effective in a city with a sophisticated system of smart cameras than in a city with simple CCTV cameras.

Analyzing the costs and benefits of security options is important in the context of a world burdened by limitations. No security strategy can protect against all attacks, particularly in an inherently open and dynamic system like urban mass transit. Transit agencies, then, must make choices about which technology or technique to use. Furthermore, federal policymakers are limited in their ability to fund these improvements as mentioned in the previous section. Their choice centers on where to send the money and which improvements receive funding. This section attempts to provide insight on how to make these choices.

Monetary costs are relatively easy to measure. One can simply estimate the initial investment cost of a particular security improvement and then estimate the annual maintenance costs. Indeed, there is unclassified research available that examines these figures.[88] However, opportunity costs and other second-order effects of improvements on the transit system overall are not as clear. One problem is that increased security often results in decreased operational efficiency. Moreover, those mass transit systems that require the most security have the most to lose from decreased efficiency. For example, New York City could not function at its current scale without a fully functional subway system. This very fact is what contributes to New York City being such a high-risk target.

Estimating the benefits of a security improvement is even more difficult. Agencies do not always know when an attack has been averted. Even when a specific plot has been foiled, it is unlikely that one particular aspect of a complex security system was wholly responsible. For example, was an attack foiled by the additional 100 officers hired last year or the training they received?

Benefits are also difficult to measure because terrorist attacks are exceedingly rare. As of this writing, no American subway system has been attacked. Thus, a successful security improvement will not yield a measurable result at the margin since the best possible result (zero attacks) has been achieved in every American city in every year. This also poses significant methodological problems for analysts because most probability models are based on the past frequency of an event. Analyzing the probability of an event that has not previously occurred requires advanced methods that are more difficult to interpret.

The benefit of a particular security choice is also linked to the cost of a terrorist attack. This is difficult to measure. Costs can be measured through a multitude of variables including human death tolls, dollars of physical property damage, and economic loss, among others. These are effectively the *consequences* of an attack and go to the crux of DHS's risk-based funding methodology. Imperfections notwithstanding, risk-based decision-making is necessary to ensure a uniform, minimal level of risk throughout the United States.

U.S. Rail Security Funding: Transit Security Grant Program

Background

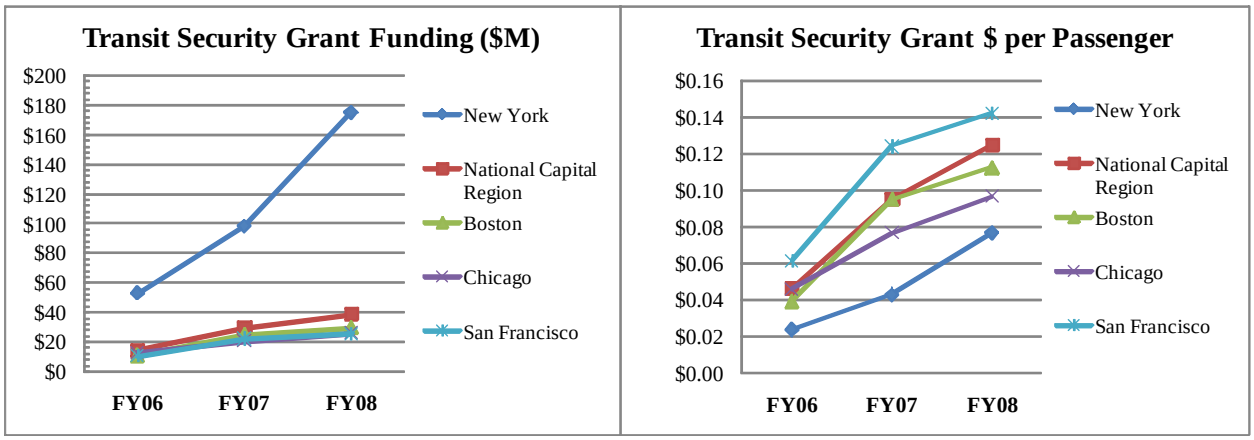
Although rail security is a shared responsibility between the federal, state and local governments, rail transit authorities rely heavily upon federal funding for both security-related operations and capital investments. Specifically, the Department of Homeland Security's infrastructure protection activities include five grant programs aimed at strengthening critical infrastructure nationwide.[89] Among these, the Transit Security Grant Program (TSGP) "provides funds to owners and operators of transit systems (which include intracity bus, rail, and ferry systems) to protect critical surface transportation infrastructure and the traveling public from acts of terrorism, major disasters, and other emergencies."[90] It funds projects aimed at hardening infrastructure from explosive attacks, preparedness efforts, planning activities, training, exercises, equipment, security management, and administration costs.[91] The TSGP also includes two sub-component grant programs: the Freight Rail Security Grant Program and the Intercity Passenger Rail Program, which provides funding to Amtrak for security-related projects.[92]

Recent Trends

DHS funding for securing transit infrastructure has increased and evolved in priority. In FY 2008, the TSGP will provide over $375 million to the owners and operators of transit systems and the National Passenger Rail Corporation (Amtrak) – more than double the funding of $143 million provided in 2006 (Figure 7).[93] With DHS having spent more than $3 billion on infrastructure protection since 2002, DHS Secretary Chertoff claimed a shifting investment focus from response and recovery capabilities to a "focus…in the direction of prevention and preparedness, and in particular, planning, exercising and training, which are the key to success in the area of prevention and preparedness" in his announcement of the FY 2008 awards.[94]

New York will receive the greatest increase and largest total sum of funding compared to its peer metropolitan regions. Its $173.38 million award for FY 2008 will be used for hardening and securing the region's suspension bridges, training and exercises, CCTV systems, bomb detection technology, and an increase in the number of K-9 dog teams.[95] However, the spending per passenger for New York ($0.07) lags well behind its peers and the national average of $0.09 (Figures 7 & 8). Both the massive funding increase and lagging $0.07 per passenger figure is attributed to the enormous volume of passengers the New York system services compared to all others nationwide. Given the nature of threats, vulnerabilities, and consequences of an attack in New York, this disproportionate funding is both appropriate and consistent with DHS's risk-based funding priorities.

Figure 7. Transit Security Grant Program Funding Trends (Top Five Urban Areas) [96,97]



Funding Priorities

The TSGP funds its awardees "based upon ongoing intelligence analysis, extensive security reviews, consultations with the transit industry and Congressional direction."[98] This risk-based approach results in a large portion of the federal funding directed toward the highest-risk transit systems in large metropolitan regions of the country. New York City, Washington D.C., Boston, San Francisco, and Chicago are the top five grant awardees as shown in Figures 7 and 8.

A new funding eligibility requirement for mass transit and passenger rail agencies was statutorily mandated by Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007." To receive security grant awards, applicants must have a current security plan that has been updated within the last three years and validated by its primary security provider or police force.[99] Those agencies meeting this requirement then undergo a 45-day application process through their State Administrative Agency (SAA), and the TSGP administrative officials to gain approval and disbursement of funding for their proposed security projects. Applying agencies must develop an Investment Justification and budget that reveal how each proposed initiative confronts current capability gaps identified in the security plan.[100] TSA grant officials then score each project based on three criteria: the agency's risk, the project's effectiveness, and quality of the project.[101]

Regional coordination is an important factor in funding approval as well. "DHS places a very high priority on ensuring that all TSGP applications reflect robust regional coordination and can show an investment strategy that institutionalizes regional security strategy integration."[102] Because major Tier I regions such as New York and the National Capital Region have multiple operating transit agencies, regional consultation is critical to achieving this integration and is evident through the cooperative agreements established throughout these higher-risk, regional

transit systems.[103] A recent development in coordination was the formation of Tier I Regional Transit Security Working Groups (RTSWGs) that develop and prioritize transit security investments that mitigate risk within their respective urban regions.[104]

Figure 8. Transit Security Grant Program (Top Five Urban Areas & Amtrak) [105,106,107,108]

Department of Homeland Security (TSA) Transit Security Funding (Top Urban Areas & Amtrak)

	FY2006	FY2007 (Base & Supp.)	FY2008
New York City Regional Area			
TSGP Funding	$52,500,000	$98,200,000	$175,380,995
Rail Ridership (Annual)	2,184,968,000	2,285,361,400	2,390,367,606*
$ per Passenger (Annual)	$0.02	$0.04	$0.07
National Capital Region			
TSGP Funding	$14,300,000	$29,355,505	$38,371,355
Rail Ridership (Annual)	307,726,500	307,935,200	308,144,041*
$ per Passenger (Annual)	$0.05	$0.10	$0.12
Boston Area			
TSGP Funding	$10,600,000	$24,724,394	$29,259,896
Rail Ridership (Annual)	270,535,000	260,192,200	250,244,815*
$ per Passenger (Annual)	$0.04	$0.10	$0.12
Chicago Area			
TSGP Funding	$12,500,000	$20,637,834	$25,997,331
Rail Ridership (Annual)	271,444,400	269,618,400	267,804,683*
$ per Passenger (Annual)	$0.05	$0.08	$0.10
San Francisco Bay Area			
TSGP Funding	$10,500,000	$22,220,695	$25,433,749
Rail Ridership (Annual)	170,953,400	179,124,700	187,686,575*
$ per Passenger (Annual)	$0.06	$0.12	$0.14
Amtrak (Intercity Passenger Rail)			
TSA - Intercity Rail Grant Funding	$7,242,855	$13,409,537	$25,000,000
Rail Ridership (Annual)	24,300,000	25,800,000	27,392,593*
$ per Passenger (Annual)	$0.30	$0.52	$0.91
Nationwide (TSGP & Intercity Pass. Rail)	$143,240,948	$257,770,670	$375,108,571
National Rail Ridership (Annual)	3,752,708,000	3,892,605,000	4,037,717,213*
National Avg $ per Rail Passenger (Annual)	$0.04	$0.07	$0.09

***FY08 ridership estimates based upon the assumption of an identical percentage increase/decrease from FY06 to FY07.**

Notes:

(a) TSA grant funding data from DHS publication "Overview: FY 2008 Infrastructure Protection Activities," May 16, 2008.

(b) Rail ridership data provided by American Public Transporation Association at www.apta.com.

(c) Amtrak ridership figures provided by the Amtrak Annual Reports for 2006 and 2007.

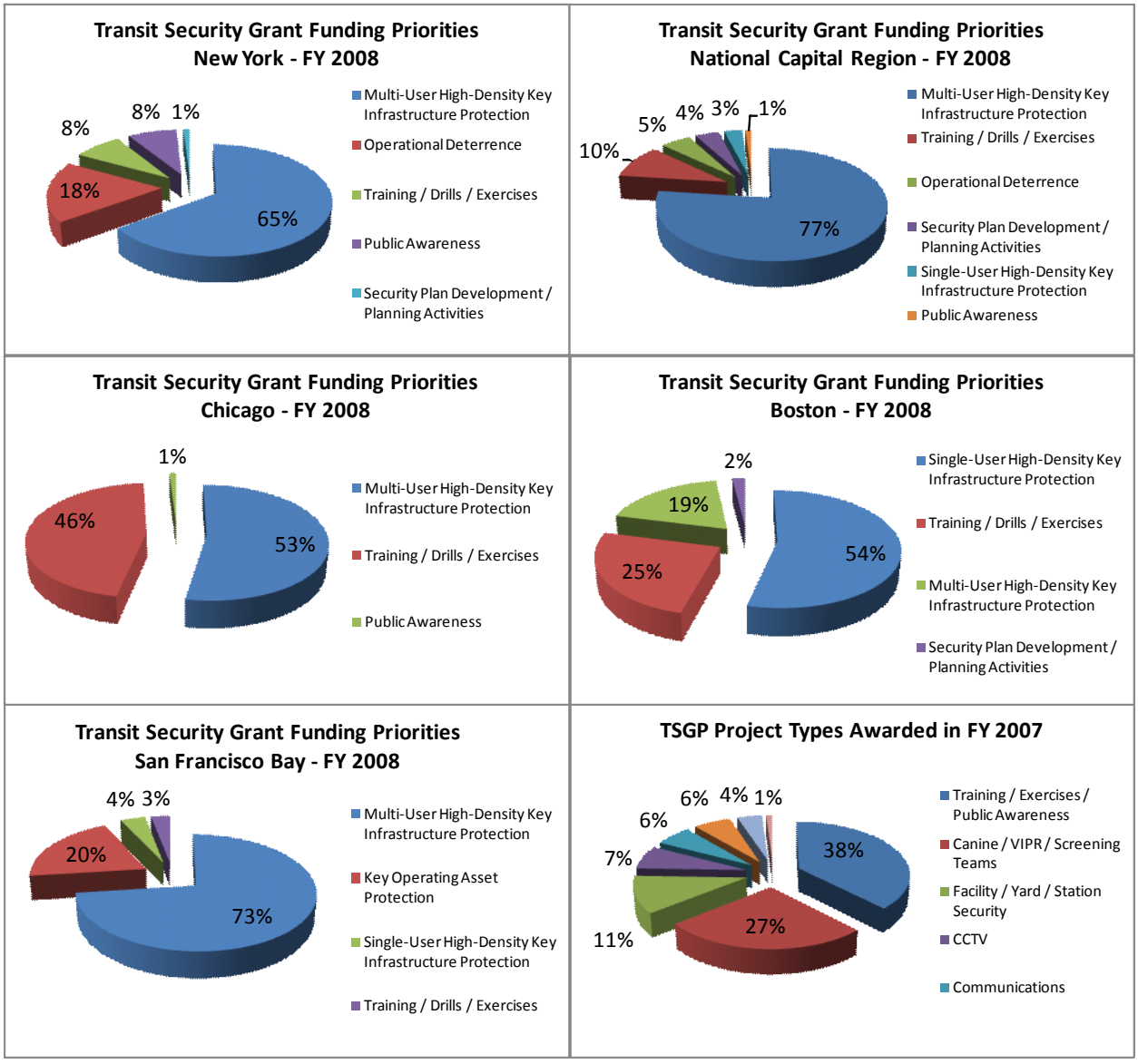
(d) Rail ridership figures include Heavy, Light, and Commuter Rail modes of transit.

(e) FY 2007 funding includes both the base and supplemental appropriations.

The pie charts in Figure 9 depict the spending priorities of the top five Tier I regions for FY 2008 in comparison to the project types awarded in FY 2007. Four of the five regions will be spending the majority of their FY08 funding on Multi-User High-Density Key Infrastructure Protection, including high-ticket projects such as intrusion detection, surveillance systems and tunnel hardening. Despite Secretary Chertoff's claim that the focus for grant funds is shifting

toward planning and exercises, it is apparent that, at least for the major Tier I regions, there remains a clear need for sustained investment in capital infrastructure protection projects.

Figure 9. Transit Security Grant Program Funding Priorities [109,110]



Funding Methodology

DHS scores and approves projects submitted for funding using a threat-based index score calculated by the following equation: **Project Score = Risk x Effectiveness + Quality + Regional Collaboration (if appropriate).**[111] Project risk is defined on a scale of 1 to 6 considering both the *threat*, determined by intelligence community assessments, passenger populations and economic impact, and the *vulnerability* or consequence of an attack governed by

ridership, underground track miles, and underwater tunnels.[112] Project effectiveness is rated between 1 and 4 based on a categorization of project types into four priority groups. For example, training security employees is considered highly effective at reducing risk and is included in the top priority group, while security enhancements at a rail yard are relatively less effective and are categorized in the lowest of the four groups. "These groups have been prioritized based upon Departmental priorities and their ability to elevate security on a system-wide level, to elevate security to critical infrastructure assets, and to reduce the risk of catastrophic events and consequences."[113] Figure 10 below provides examples of effectiveness ratings for a range of project types. Projects such as hardening of low-density stations, redundant control centers/mobile command centers, back-up generators/power supplies, and chemical/biological detection systems are not considered for funding under the current TSGP.[114] Subject matter experts estimate project quality by evaluating the project's cost effectiveness, feasibility, timeliness, and sustainability.[115]

Figure 10. Transit Security Grant Program Project Effectiveness Groups [116]

DHS Transit Security Grant Program
Project Effectiveness Groups Listed in Priority Order*

Priority Group #	Project Effectiveness Group Score	Description	Project Types
1	4	Training, Operational Deterrence, Drills, Public Awareness Activities	• Developing Security Plans • Training (basic before follow-on): Security Awareness, DHS-Approved Behavior Recognition Detection Courses, Counter-Surveillance, Immediate Actions for Security Threats/Incidents • Employee Security Threat Assessments (e.g. background checks) • Operational Deterrence: Canine Teams, Mobile Explosives Screening Teams, VIPR Teams • Crowd Assessment • Public Awareness
2	3	Multi-User High-Density Key Infrastructure Protection	Anti-terrorism security enhancement measures, such as intrusion detection, visual surveillance with live monitoring, alarms tied to visual surveillance system, recognition software, tunnel ventilation and drainage system protection, flood gates and plugs, portal lighting, and similar hardening actions for: • Tunnel Hardening • High-Density Elevated Operations • Multi-User High-Density Stations
3	2	Single-User High-Density Key Infrastructure Protection	Hardening of SCADA systems • Anti-terrorism security enhancement measures for High-Density Stations and Bridges
4	1	Key Operating Asset Protection	Physical Hardening of Control Centers: Bollards, Stand off, Access Control • Secure Parked trains, engines, and buses (Bus/Rail Yards) • Maintenance Facilities

* Table taken from U.S. Department of Homeland Security. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit." February 2008. pg. 7. Accessed at http://www.tsa.gov/join/grants/index.shtm.

Although the equation cited above is inherently risk-based, the final project score should also be a function of its ability to close target capability gaps. According to DHS, this scoring methodology and effectiveness grouping of project types places a premium on prevention and protection activities including deterrence, high-impact projects where risk is great such as tunnel hardening, and cost-effective projects such as training, exercises, and public awareness

campaigns.[117] While DHS's rubric is not without merit in its intent to ensure TSGP funds are spent wisely on projects that will reduce overall risk from a terrorist attack, it does not clearly integrate DHS's strategic goals and target capabilities identified in the National Infrastructure Protection Plan (NIPP) and Target Capabilities List (TCL). As mentioned above, the TSGP requires an Investment Justification explaining how each requested project would address a *local* gap in capability related to the local response plan. Any linkage to the national infrastructure protection goals or TCL is tenuous at best within the Investment Justification; moreover, this connection is absent within the project scoring function. As a result, this system of scoring and prioritizing projects for funding approval is problematic.

For example, under the current grant scoring process, an urban area is more likely to receive an award for an operational deterrence initiative such as employee training in its subways over investing in a high-tech screening technology, all else equal. While the training project may be marginally more risk and cost-effective according to DHS's standards, if the screening technology project specifically enhances a national Target Capability for that particular region but the training does not, the final project score is not an accurate reflection of national, strategic priority. In this case, a decision to fund the training project over the technology is of little *strategic* value in achieving a nationwide level of infrastructure protection and goes more toward subsidizing local operating costs for increasing security measures. While this trade-off scenario is unlikely to be true for all federally funded transit security projects, this example highlights the shortcomings of the current scoring method and one we recommend for reevaluation.

Funding Challenges

In the face of rising Congressional appropriations for TSGP funding, many transit-system operators maintain that the funding falls well short of their long-term needs "to complete their capital program[s] to maintain, modernize, and expand [their] security function."[118] The National Transit Systems Security Act of 2007 appropriated $2.6 billion for security-related capital projects and $840 million for related operating expenses over a four-year period; however, surveyed transit operators estimate a shortage of more than $6 billion in capital program shortages and $800 million in annual operating expenses.[119] Given the size of the current federal budget deficit and the forthcoming presidential election and new administration in 2009, the likelihood of future spending increases for rail security remain an unknown.

The political aspects of financing the TSGP can create difficulties in ensuring the right amount of money goes to the right state and local transit authorities. A 2007 RAND technical report on risk modeling and infrastructure protection found that considering fatalities alone, New York City accounts for 65 percent of the total national risk, followed by Chicago (12%) and all others negligible in comparison.[120] Likewise, 95 percent of the total national risk from terror attacks falls within the eight largest urban areas.[121] The fact that TSGP has allocated roughly 95

percent of the federal funding to the Tier I urban areas in FY07 and FY08 is a positive sign.[122] However, this does not imply that the allocations to the various cities within the Tier I and II groups are proportional to their relative national risk. New York City rightfully receives the majority of TSGP funding, but a comparison of New York's $175 million allocated for FY08 to the total national TSGP funding of $375 million results in a 46 percent allocation – well short of RAND's total national risk estimate of 65 percent (Figure 8).

Appropriating federal funds for transit security – like most grant programs – proves politically challenging without ensuring a relatively equitable distribution of grant funding across congressional districts, regardless of the level of risk.[123] In part, this helps to explain why the level of funding per passenger in San Francisco is nearly double that of a passenger in New York even while it only services less than one-tenth of New York's annual ridership (Figure 8). The obvious conclusion is that the nature of our political system limits any strict adherence to risk-based funding priorities. Social scientists applying game theory models to risk-based resource allocation and security have drawn helpful conclusions as well citing "that spending too much on defense of assets that are not highly valuable hurts the defender in two ways – not only by wasting resources on defense of assets that are unlikely to be attacked in any case, but also by increasing the likelihood of a more valuable asset being attacked."[124]

Intergovernmental Challenges in Securing Mass Transit [125]

Emergency Management and Federal Authority

The federal government has limited legal authority on the actual implementation of emergency response and preparation. The federal government has limited powers in regulating and mandating states to implement programs, capital projects, or other directives. The federal government can implement programs and directives itself, but it cannot commandeer state and local actors to act as agents of the federal government. The key is to create programs and policies that state and local actors will want to implement, attached with appropriate incentives in order to do so.

Results, not control, matter in the case of emergency management.[126] With the zero-tolerance for failure in protecting the infrastructure, resources, and people from terrorist attacks, the United States public expects more from their federal government, even when they are legally or resource restricted. Many problems arise when local government resources are overwhelmed, and the federal or state government is asked to intervene. State governments also become overwhelmed, as the frequency of declaring "state of emergency" has risen in the 1990s. Even in preparedness efforts, most local governments do not have the capacity to do extensive research and development of technology or best practices, and must rely on the private sector and the federal government to supplement this crucial area.

The federal government is also limited in its power to order state and local authorities to implement federal improvements in their rail and mass transit systems, but can provide incentives for compliance through grants and rewards. Other issues arise with the balance between state and federal power, and many governors are reluctant to allow federal intervention, even in disaster planning.[127] In addition, principal-agent problems can arise even when the federal government controls the resources; however, state and local governments have implementation discretion.[128] With these issues, it is vital for the federal government to acknowledge lack of coordination as the main problem in emergency management, and active coordination and solid planning foundations and support as the main solution.[129]

Relations with States: Home Rule and Dillon's Rule

Two different systems exist in the United States when it comes to state authorities over local municipalities. Although each state is unique in its relation to federal authorities, states follow either home rule, or Dillon's rule for delegation of powers to local municipalities. Dillon's rule limits local authority to powers the state explicitly delegates, whereas home rule allows local authority unless the state claims jurisdiction.[130] There are implications for both sets of power delegation: in Dillon's rule states, the federal government may have to deal with fewer stakeholders, and provide simpler incentives; in home rule states, the federal government may

have to deal with more levels of governments, and devise more comprehensive incentives and negotiations. However, many Dillon's rule states have delegated much of their authority down to local municipalities, and can be treated virtually as home rule states. Traditionally, the federal government has leverage only in directives that rely on heavy subsidies, such as highway infrastructure, or mass transit. This is crucial for mass transit, because the federal government has a responsibility to protect the homeland, but they have limited abilities to mandate or regulate how local governments implement security measures. Even with the strong economic incentive, many states or regions may not want to follow the regulations attached to federal grants. One example is that some municipalities are still not implementing the National Incident Management System (NIMS) and Incident Command System (ICS), even though they are tied to federal emergency preparedness grants.[131]

Relations with Local Authorities[132]

Emergency management begins at the local level. All homeland security events, whether they are terrorist-linked or natural disasters, begin as local events. There is no clear divide between natural and man-made disasters, and this distinction is difficult to make for first responders. For example, until the second plane hit the World Trade Center on September 11, 2001, first responders did not know it was a terrorist attack. Due to this difficulty, frontline first responders must be prepared to respond to all such events, as has been attempted through NIMS and all-hazards training such as CBRNE. The flexible Incident Command System (ICS) also helps with emergency response, because it keeps people accountable to and for others, and leaders are given responsibility without rigid bureaucracy or titles. It becomes essential for federal agencies to become coordinators and a network builder for best practices, as well as a research resource for local governments. There are fewer Tier 1 cities, and most of these cities have metropolitan authorities that regulate and manage mass transit. In this case, it can be anticipated that it will be easier for the federal government to work with those fewer authorities in securing mass transit.

Horizontal Coordination

The Department of Homeland Security is the spearhead organization for responding to attacks on American security against terrorist attacks. The mission of the organization includes protecting the homeland from terrorist attacks, responding to these attacks, and securing our borders.[133] However, the Department of Transportation, Department of Justice, and Department of Defense also have jurisdiction in rail and mass transit security, and need to coordinate efficiently in order to effectively protect our mass transit resources and infrastructure. The Department of Justice may need to be involved, especially with privacy and legal issues concerning security. In addition, when appropriate, the Department of Defense may need to be involved. Ultimately, the Transportation Security Administration has been given the task to coordinate the several federal agencies, as well as work with state and local governments under the Transit, Commuter and Long-Distance Rail Government Coordinating Council (TCLDR-

GCC). [134] This council meets to set priorities and positions before jointly working with the Mass Transit Sector Coordinating Council (SCC).[135] Other stakeholders in the transit community meet under the Mass Transit Sector Coordinating Council (SCC). Participating entities include the American Public Transportation Association, the Community Transportation Association of America, Amtrak, the Amalgamated Transit Union, and individual transit agencies representative of community in system size and geographic spread, as well as representatives of business organizations providing support services to the public transportation industry. The two councils meet independently in order to set their priorities and positions, and meet jointly to develop and implement security strategies and programs.[136] The TSA also engages in cooperation internationally through the International Working Group on Land Transport Security, focusing on passenger rail and mass transit security. Members include the Group of Eight (G8), the European Union, the Asia Pacific Economic Cooperation, and the Mexican and Canadian governments. TSA also participates in an international Rail and Urban Transport Working Group in support of technology testing and evaluation information sharing. [137]

Vertical Coordination

The federal government organizations have to work with state and metropolitan area authorities, local and regional police, fire, and other first responders, as well as with planning authorities for prevention and capital projects. With the shift in public expectations of security, especially since the establishment of the Department of Homeland Security, much of the accountability and responsibility has been placed on the federal government. However, absolute security is nearly impossible at that level, and federal authorities have to coordinate and work with local stakeholders to implement security changes and assess security needs. For example, the TSA has also joined the Greater New York/New Jersey/Connecticut Regional Transit Working Group to streamline the process of applying for federal funds to assist in securing the region's transit systems.[138]

TSA also hosts a twice-yearly Transit Security Roundtable with the Federal Transit Administration (FTA) in order to bring together security chiefs and directors of the top fifty transit agencies in order to tackle specific security challenges, as well as to foster networking and information sharing amongst the mass transit community.[139] The TSA has also established the Transit Policing and Security Peer Advisory Group as a consultative forum of transit agency security professionals to harness the application of resources and the development of programs to maximize the impact in enhancing security.[140]

Following the federalization of aviation security, the TSA will have an easier task in federalizing rail systems such as Amtrak for security purposes, than they will imposing security systems on intrastate mass transit. Therefore, it is critical for TSA to cooperate with these authorities, only some of which are multi-state. TSA's role can be to help regional authorities

with best practices, research, and other federal resources, while still allowing customization and discretion for different regions.

A Case in Response: The Pentagon and Arlington County on September 11, 2001[141]

When American Airlines flight 77 crashed through three levels of the Pentagon on September 11th, 2001, the damage and loss of life was mitigated by high levels of coordination of local, county, and federal government, as well as first responders and the health community. Both FBI field commanders and Arlington fire department commanders rapidly established their headquarters within minutes. Fire and rescue units from within the county and from nearby Ronald Reagan Washington National Airport came to aid. Neighboring Alexandria provided mutual aid to Arlington, sending a fire battalion chief and promise of any aid necessary. The area's hospitals were ready to receive the injured rapidly, and anticipated a shortage of specific supplies (skin grafts for burn victims) and created plans to relay them from Texas on ground, since all air transit was grounded at that time.

In the follow-up report, Arlington County was praised as "a model that every metropolitan area should emulate" for emergency management. The credit is given to the integrated command structure of their emergency response, mutual aid agreements with surrounding communities, a strong emergency team, an assistance program to support employees amid the stress of their work, and constant drilling over several years.[142]

A Case in Prevention: New York Metro Security Authorities

Jurisdiction issues alone can be overwhelming for emergency management. The New York City Metro system is an example of multiple agencies working in the same jurisdiction, performing overlapping and separate functions. Agencies at the city, regional, and state level all participate, with some input from federal authorities such as TSA. With over 3 million riders per day, and a daunting 24-hour nonstop schedule, New York City Metro is the most trafficked transit system in our nation. As the busiest mass transit system in our country, New York Metro has many law enforcement and security agencies working on preventing and responding to any potential mass transit attacks. The New York Police Department is a first responder agency and it performs random bag screenings at stations. In larger stations such as Pennsylvania Station and Rockefeller Center, NYPD heavily patrols with bomb sniffing dogs and automatic rifles under Operation Torch.[143] Metro Transit Authority police perform most of this function for the checkpoints commuter lines into and out of the city. Most of these agencies help sponsor or support the 1-888-NYC-SAFE program, which educates and encourages riders to report suspicious activity. The TSA and New York Department of Transportation work on security for other forms of transportation in the area.

Public Expectations

There is zero-tolerance for failure in the realm of homeland security. The public expectation of government is to protect them in public space through preventing and deterring domestic terrorism and responding effectively if an attack occurs. Unlike air travel, the public currently expects few, if any, delays in their mass transit and rail travel. They expect unobtrusive protection, not screening, but this expectation will need to shift in the near future with advancing technology and higher threat targets. With more media coverage and scrutiny, every failure in every region of the country potentially becomes the government's responsibility.[144] With the potential to move towards more invasive screening operations, and like every new implemented security measure in aviation, the public's expectation of mass transit must be taken into account and handled accordingly.

Target Hardening

From crime policy, target hardening is the concept of making a target too difficult to penetrate or attack in order to deter attacks, and making those preparations very visible and clear. Part of target hardening is opportunity reduction and closing capability gaps, but much of it is deterrence. Deterrence is part of prevention and preparedness, and must be accompanied by swift, certain, and severe response for whomever tries to pass the system.[145]

One issue with target hardening, however, is the unbalanced implementation of technology and operations across multiple targets. For example, if all resources are invested in protecting the New York City Metro system, but none in San Francisco's Bay Area Rapid Transit system, then San Francisco becomes a relatively more vulnerable target as New York becomes more secure. At the regional level, if the larger stations in New York's system are heavily protected against potential attacks, it would be relatively easy for a potential terrorist to enter on smaller, less dense stations and still carry out devastating attacks.

Another issue with target hardening is the tradeoff between deterrence and discovering potential terrorists. Although low-level homemade bombs may be detected by a system, more sophisticated operations and materials may appear to pass current technology. In addition, if potential terrorists never attempt to attack a system, they may seek to attack other venues, without being detected in the first system.

Barriers to Future Public Transit

Due to the rising cost of oil, continuing population growth, as well as a general environmental trend, mass transit is becoming more relevant and necessary, especially in large and mid-sized cities. Public transit already has traditional barriers, such as a heavy reliance on federal funding, jurisdictional consensus, and political hurdles that can span decades. Also, sufficient population densities are required to justify mass transit, but mass transit locations are linked to increased densities. For example, Los Angeles, with a population of 3.9 million and

some of the worst congestion in the country,[146] has little in the way of passenger rail systems for commuting and traveling within the city. Much of the rail system in Southern California is used to transfer cargo for the Ports of LA/Long Beach, and the city faces political problems approving mass transit. To help offset the cost expanding the system, the Metro authority of Los Angeles is proposing a half-cent sale tax increase,[147] yet is meeting with mixed reviews from its population.

However, security, and its associated costs, create another barrier for implementation of mass transit, and can hinder new growth in this sector. Security concerns create additional expectations from the public, and challenges in implementing mass transit in sufficiently dense areas. The public has higher expectations for security from a system built in 2010 than they do of one built in the 1900s. The cost of this level of public expectation can make secure mass transit even more prohibitive in cost.

Tradeoffs: Learning from Prior Events v. Anticipating New Challenges[148]

Much of the knowledge and best practices in emergency management come from learning from prior events. However, since attacks are relatively rare, at least in their final execution, that this makes it difficult to have multilayered, flexible systems that can adjust to different situations. This has led to playing catch up to innovative attacks and reactive systems, instead of proactive systems. Much of what needs to be done is the implement multilayered systems that help prepare for multiple situations. One large problem of the reactive nature of learning from prior events is the lack of anticipation for new, innovative attacks. It is not possible to reduce the threat risk to zero. However, multilayered systems can serve the dual purpose of creating flexibility in a system to adapt to new challenges and protect from known threats. For example, monitoring and reducing crime in subway stations can help monitor and reduce opportunities for suspicious persons in subway stations. In Boston, BFD practiced emergency management for the Red Sox World Series to help prepare them for crowd control, but this could also help in major evacuation and public disorder situations. Also, the region's fire and police departments developed redundant emergency communication systems, in case one of their headquarters goes offline due to a natural disaster, but it would also help in a terrorist attack on the city center.[149]

Creating a reliable learning system helps identify weaknesses in current procedures, as well as establish professional networks. Many of the problems that came out post-September 11th were related to lack of information sharing amongst agencies. While TSA's responsibility is not to centralize intelligence information, they do need to offer expertise, research, best practices, capacity building and funding to regional and local authorities.

Preparedness and response need to be linked together, and put into practice on a frequent basis. One practice that has been helpful has been training through sending units to emergencies outside of their jurisdiction, as well as establishing best practices and information sharing amongst the mass transit community. Another practice that has been helpful has been the

creation of mutual aid agreements between municipalities, such as in the case of Arlington and Alexandria after the attack on the Pentagon.

Tradeoffs: Limitations on Freedom v. Protection from Risks[150]

The public's expectations for security allow no tolerance for failure from their government. As evidenced by the heavy criticism after September 11, 2001, and Hurricane Katrina, the federal government is particularly prone to criticism for lack of preparation or inadequate response for any disaster. Considering problems with varying levels of preparedness in different systems, it is important to assess and ensure that prevention and security is linked with high-risk targets. One also has to be cognizant of problems with target hardening, concentrating too much on too few targets, and deterring attacks on some systems, but leaving others vulnerable. There needs to be assessments of risk, and an allocation of resources in proportion to those risks.

Aviation security exemplifies the tradeoff of privacy for security. However, what makes aviation different from mass transit is the central checkpoint for security, the amount of real estate available for security screening processes, and the public tolerance of delays due to security. Mass transit has a virtually open system, a much higher concentration of people, more costly infrastructure, and more accessibility.

Mass transit and rail have the additional need for rapid security and screening processes. With the increased pressure for mass transit due in part to oil price increases and environmental concerns, mass transit needs to stay a viable form of transportation, for our economy and people to function.[151] Ridership in most urban heavy rail systems increased from 2006 to 2007, with the exception of Boston and Chicago.[152] Mass transit in particular is heavily subsidized by government, but still relies on passenger fees to help with costs of the system. Transit needs to be safe and timely for people to use it, and more people need to use transit in order to fund it. In addition, transit infrastructure is vulnerable to disruption or damage, and needs to be protected but still be accessible to the public.

Endnotes

[1] American Public Transportation Association (APTA). "Public Transportation Ridership Statistics." http://www.apta.com/research/stats/ridership (accessed on May 23, 2008).
[2] International Association of Public Transport. http://www.uitp.org (accessed on May 28, 2008).
[3] Jenkins, Brian. "Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview." San Jose, CA: Mineta Transportation Institute. October, 2001, 1.
[4] Kelly, Ray, New York City Police Commissioner. *Remarks at Respect for Law Alliance Awards Banquet*. May 27, 2008.
[5] Wilson, Jeremy M., Jackson, Brian A., Eisman, Mel., Steinberg, Paul., Riley, K. Jack. *Securing America's Passenger-Rail Systems.* Santa Monica, CA: The RAND Corporation, 2007: 1.
[6] Fernandez, Bob. "Dow Falls 140 Points to End Its Worst Week Since WWII." *The Philadelphia Inquirer*, September 22, 2001.
[7] Fink, Camille N.Y., Taylor, Brian D., and Anastasia Loukaitou-Sideris. "From Policy and Response to System Design and Operations: Inter-Governmental Transit Security Planning in the U.S." *Journal of Public Transport* (2005): 2.
[8] Jenkins, 1.
[9] New York City has 468 subway stations according to the Metropolitan Transportation Authority website (http://www.mta.info/nyct/facts/ffsubway.htm). There are approximately 475 commercial airports in the United States according to the list compiled at http://en.wikipedia.org/wiki/Wikipedia:Airline_destination_lists:_North_America#United_States_of_America.
[10] Miller, Virginia and Mantill Williams. "Americans Take More than 10 Billion Trips on Public Transportation." American Public Transportation Association. http://www.apta.com/media/releases/070312_ten_billion.cfm (accessed on May 23, 2008).
[11] Jenkins, 2.
[12] The list of strategies in this section is not exhaustive. For example, many agencies also conduct passenger awareness campaigns, but the cost and effectiveness of these campaigns is relatively low.
[13] Wilson, et. al., 2007.
[14] Office of the President of the United States. "Fact Sheet: National Strategy for Homeland Security." http://www.whitehouse.gov/infocus/homeland/index.html (accessed May 22, 2008).
[15] Federal Transit Administration (FTA). "Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies." April 2007: 9.
[16] Hawley, Kip. "Oral Testimony of Kip Hawley, TSA Administrator Before The United States House of Representatives, Subcommittee on Transportation Security and Infrastructure Protection." February 6, 2007.
[17] Hawley, 2007.
[18] U.S. General Accountability Office. *Passenger Rail Security: Evaluating Foreign Practices and Risk Can Help Guide Security Efforts.* Report No. GAO-06-557T. Washington D.C., March 29, 2006.
[19] U.S. Transportation Security Administration. "Train Police Officers to Spot Terrorist Related Activity." Press Release. April 6, 2006.
[20] Lavoie, Denise. "Specialist on Profiling Says He Was a Victim." *Boston Globe*. December 4, 2007.
[21] FTA, 2007.
[22] Ibid.
[23] Massachusetts Bay Transit Authority. "Capital Investment Program FY2008-FY2012.", 117. http://mbta.com/about_the_mbta/financials/?id=1052 (accessed May 23, 2008).
[24] GAO, 2006.
[25] FTA, 2007 and GAO, 2006.
[26] FTA, 2007.
[27] GAO, 2006.
[28] Salzman, Avi. "Seeking a Safe Journey as Anxiety Rides the Rails." *New York Times*. July 24, 2005.
[29] Wilson, et. al., 2007.
[30] Kernodle, Katrina. "Synopsis: Chemical and Biological Agent Protection Systems." Frances Kernodle Associates. http://www.fkassociates.com/Chemical%20and%20Biological.html (accessed May 27, 2008).
[31] Haupt, et. al., 2004.

[32] Staes, Lisa, Reep, Amber, Chaudhary, Rajesh, Tucci, James, Sapper, Deborah, Borum, Randy and Arthur J. Kelly, III. "Identification of Cost-effective Methods to Improve Security at Transit Operating/Maintenance Facilities and Passenger Stations." Center for Urban Transportation Research, University of South Florida. July, 2006: 44.
[33] Washington Metropolitan Area Transportation Authority. "9/11 Has Changed All of Us." http://www.wmata.com/about/MET_NEWS/pressroom/media_advisory08262002.cfm (accessed May 29, 2008)
[34] GAO (2006), 12.
[35] Examples include the Homeland Security Institute, the Learned Lessons Information Sharing web site (LLIS.gov), and the Homeland Security Digital Library.
[36] New technologies will be covered in a later section of this report.
[37] Lewis, Raphael. "T to Check Packages, Bags at Random." *Boston Globe*. June 8, 2004.
[38] Preston, Julia. "Police Searches of Bags in Subways Are Ruled Constitutional." *New York Times.* December 2, 2005.
[39] Powell, Michael and Michelle Garcia. "New York's Subway Riders Face Bag Checks with Somber Tolerance." *The Washington Post*. July 23, 2005.
[40] Ibid.
[41] FTA (2007), 10-11.
[42] Loukaitou-Sideris, Anastasia, Taylor, Brian D. and Camille N. Y. Fink. "Rail Transit Security in an International Context: Lessons from Four Cities." *Urban Affairs Review*, 41 (2006): 732.
[43] Humi, Peter. "Bomb Explodes on Paris Subway." October 17, 1995. http://www.cnn.com/WORLD/9510/paris_bomb/10-17/index.html (accessed on May 23, 2008). See also "French Officials Say Bomb Caused Deadly Train Blast," December 3, 1996. http://www.cnn.com/WORLD/9612/03/subway.explosion/index.html (accessed on May 23, 2008).
[44] Loukaitou-Sideris, Taylor and Fink.
[45] Chrissement, Dominique. "The Growth of VIGIPIRATE in Ile-de-France." *Doctrine* (March 2005): 60-62.
[46] Carli, Pierre, Telion, Caroline, and David Baker. "Terrorism in France." *Prehospital and Disaster Medicine* (April-June 2003): 92-99.
[47] BBC. "London Bombing Toll Rises to 37." July 7, 2005. http://news.bbc.co.uk/2/hi/uk_news/4661059.stm (accessed on May 23, 2008).
[48] Dunmore, Geoff. "Protecting Passenger Transport Systems From the Threat of Terrorism," Public Transport International (2006): 8-11. Accessed at http://www.uitp-pti.com/img/cover1_2006/10-13-EN.pdf.
[49] U.S. Government Accountability Office (GAO). *Passenger Rail Security*. Report No. GAO-07-225T. Washington D.C., January 2007: 19.
[50] Loukaitou-Sideris, Taylor and Fink.
[51] Ibid.
[52] Hawley, Kip, "Oral Testimony of Kip Hawley, TSA Administrator Before The United States House of Representatives, Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection," April 15, 2008. http://www.tsa.gov/press/speeches/041508_hawley_house.shtm (accessed May 20, 2008).
[53] Transportation Security Administration (TSA). http://www.tsa.gov/approach/tech/mwave.shtm (accessed on May 23, 2008).
[54] Millivision Inc. *Concealed Threat /Object Detection Systems*. http://www.millivision.com/products.html (accessed on May 23, 2008).
[55] Transportation Research Board of the National Academies. "Appendix A: PSI Technologies." In *Appendixes to Transit Cooperative Research Program (TCRP) Report 86: Volume 13*. 2007: 3.
[56] TSA.
[57] TSA.
[58] Brijot Imaging Systems, Inc. *Object Detection and People Screening Technology: Competitor Analysis.* http://www.brijot.com/index.php (accessed June 1, 2008).
[59] Ibid.
[60] Ibid.
[61] QinetiQ, http://www.qinetiq.com/home/products.html (accessed on May 23, 2008).
[62] TSA.
[63] Brijot.

[64] Haupt, Steven G., Rowshan, Shahed, and William C. Sauntry. "Applicability of Portable Explosive Detection Devices in Transit Environments." Transit Cooperative Research Program Report 86: Volume 6. Transportation Research Board. 2004: 4.
[65] Ibid., 24.
[66] Ibid.
[67] Ibid, 25.
[68] Ibid., 24.
[69] Ibid.
[70] Ibid.
[71] Ibid., 25.
[72] TCRP Report 86, Vol. 6, 26.
[73] National Science and Technology Council. "Biometrics Overview." August 7, 2006, 1. http://biometrics.gov/Documents/BioOverview.pdf (accessed May 28, 2008).
[74] Transportation Security Administration. "Transportation Worker Identification Credential," http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed May 28, 2008).
[75] Electronic Data Systems Corporation. "Registered Traveler Pilot Program Creates Fast Lane for Airport Security: U.S. Transportation Administration." http://www.eds.com/insights/casestudies/tsa.aspx (accessed May 23, 2008).
[76] Hawley, Kip. "Statement of Kip Hawley, Assistant Secretary, Before the Committee on Commerce, Science and Transportation United States Senate." October 20, 2005. http://www.tsa.gov/assets/pdf/testimony_hawley_freight_oct_20_2006.pdf. (accessed May 20, 2008).
[77] National Science and Technology Council, 1.
[78] Burns, Bob. "S&T Stakeholders Conference: Future Attribute Screening Technology." http://www.homelandsecurity.org/StakeholdersMay07/Br40_Burns.pdf (accessed May 23, 2008).
[79] Ibid.
[80] Ibid.
[81] Lipton, Dr. Alan J., Heartwell, Craig H., Haering, Dr. Niels, and Donald Madden. "Critical Asset Protection, Perimeter Monitoring, and Threat Detection Using Automated Video Surveillance.", 2. http://www.objectvideo.com/objects/pdf/products/vew/OV_WP_IVS.pdf (accessed on May 26, 2008).
[82] Ibid.
[83] Mate Intelligent Video. "Intelligence at the Edge." Homeland Security Europe. http://www.mate.co.il/UserFiles/File/HSE%20online%20editorial.pdf (accessed May 30, 2008).
[84] Croft, John. "Intelligent Video System Nabs Illegal Entrants." *Aviation Week & Space Technology*, Vol. 156 Issue 22, June 3, 2002: 55.
[85] Ibid.
[86] Lipton, et. al.
[87] Researchers have attempted to apply advanced techniques to measure costs and benefits. See "The Economic Impacts of Terrorist Attacks" Edited by Harry W. Richardson, Peter Gordon, and James E. Moore II. Cheltenham, UK, and Northampton, MA: Edward Elgar, 2005. Also see research available at Center for Risk and Economic Analysis of Terrorist Events (CREATE) online at http://www.usc.edu/dept/create/
[88] For a comprehensive cost-effectiveness analysis, see RAND study by Wilson, et. al., 2007.
[89] U.S. Department of Homeland Security (DHS). "Overview: FY 2008 Infrastructure Protection Activities." May 16, 2008: 1. http://www.dhs.gov/xlibrary/assets/fy2008_infrastructure_protection_activities.pdf (accessed May 23, 2008).
[90] U.S. Department of Homeland Security. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit." February 2008: 4. http://www.tsa.gov/join/grants/index.shtm (accessed May 23, 2008).
[91] DHS. "Overview: FY 2008 Infrastructure Protection Activities.", 1.
[92] Ibid.
[93] U.S. Department of Homeland Security. "FY 2008 Fact Sheet Series: TSGP Overview." 2008:1. http://www.tsa.gov/assets/pdf/fy_2008_tsgp_fs.pdf (accessed May 23, 2008).
[94] Chertoff, Michael, U.S. Secretary of Homeland Security. Remarks by Secretary Chertoff on Release of FY 2008 Infrastructure Protection Awards. Union Station, Washington D.C., May 16, 2008. http://www.dhs.gov/xnews/speeches/sp_1211204489108.shtm (accessed May 23, 2008).
[95] Daily Record Staff. "N.Y. State Government Briefs: May 20, 200[8]. – Homeland Security Grant Funding Given to State." Daily Record, Rochester NY. Dolan Media Newswires, May 20, 2008. http://www.dolanmedia.com/view.cfm?recID=377401 (accessed May 23, 2008).

[96] DHS. "Overview: FY 2008 Infrastructure Protection Activities.", 9.
[97] APTA.
[98] DHS. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit.", 6.
[99] DHS. "FY 2008 Fact Sheet Series: TSGP Overview.", 1.
[100] Ibid.
[101] Ibid.
[102] DHS. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit.", 6.
[103] Ibid.
[104] U.S. Department of Homeland Security. "FY 2008 Transit Security Grant Program Workshop." February 2008. http://www.tsa.gov/assets/ppt/tsgp_workshop_presentation.ppt (accessed May 23, 2008).
[105] DHS. "Overview: FY 2008 Infrastructure Protection Activities.", 9.
[106]APTA.
[107] National Railroad Passenger Corporation (Amtrak). "2006 Annual Report." http://www.amtrak.com/servlet/ContentServer?pagename=Amtrak/am2Copy/Title_Image_Copy_Page&c=am2Copy&cid=1081794202462&ssid=161 (accessed May 23, 2008)..
[108] National Railroad Passenger Corporation (Amtrak). "2007 Annual Report." http://www.amtrak.com/servlet/ContentServer?pagename=Amtrak/am2Copy/Title_Image_Copy_Page&c=am2Copy&cid=1081794202462&ssid=161 (accessed May 23, 2008)..
[109] Transportation Security Agency (TSA). "Transportation Security Grant Programs." http://www.tsa.gov/join/grants/fy08_tsgp.shtm (accessed May 23, 2008)..
[110] DHS. "FY 2008 Transit Security Grant Program Workshop."
[111] Ibid.
[112] DHS. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit.", 7.
[113] Ibid., 6.
[114] DHS. "FY 2008 Fact Sheet Series: TSGP Overview.", 1.
[115] DHS. "FY 2008 Transit Security Grant Program Workshop."
[116] DHS. "Fiscal Year 2008 Transit Security Grant Program – Program Guidance and Application Kit.", 7.
[117] Ibid.
[118] Peterman, David Randall. "Passenger Rail Security: Issues and Legislation in the 110th Congress." CRS Report for Congress, RL32625. January 31, 2008: 9.
[119] Ibid., 8-9.
[120] Willis, Henry H., LaTourrette, Tom, Kelly, Terrence K., Hickey, Scot, and Samuel Neill. "Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection." Santa Monica, CA : RAND Technical Report, 2007: xiv.
[121] Ibid.
[122] TSA.
[123] Taylor, Brian D. "Terrorism and Transit Security: 12 Recommendations for Progress." Washington D.C.: Center for American Progress: 4.
[124] Bier, V.M., "Choosing What to Protect." Los Angeles, CA: CREATE Homeland Security Center, University of Southern California, 2005: 8.
[125] Kettl, Donald. "Contingent Coordination: Practical and Theoretical Puzzles for Homeland Security," *American Review of Public Administration* 33, no. 3 (2003): 253-77.
[126] Kettl, Donald. *System Under Stress: Homeland Security and American Politics*, 2nd ed. (Washington DC: CQ Press, 2007), 61-81.
[127] National Governors Association. "NGA Statement on Federalizing Emergencies," October 13, 2005.
[128] Kettl (2003), 262.
[129] Ibid.
[130] Koenig, Heidi and Amy Kise. "Law and the City Manager: Beginning to Understand the Sources of Influence on the Management of Local Government." *Journal of Public Administration Research and Theory* 6, no. 3 (1996): 443-59.
[131] Federal Emergency Management Agency (FEMA). "NIMS Frequently Asked Questions." http://www.fema.gov/emergency/nims/faq/compliance.shtm (accessed May 29, 2008).
[132] Kettl (2007), 78.
[133] U.S. Department of Homeland Security. "Strategic Plan – Securing Our Homeland." http://www.dhs.gov/xabout/strategicplan/index.shtm (accessed May 22, 2008).

[134] Transportation Security Administration. “Expanding Partnerships for Security Enhancement.” http://www.tsa.gov/what_we_do/tsnm/mass_transit/partnerships.shtm (accessed May 20, 2008).
[135] Ibid.
[136] Ibid.
[137] Ibid.
[138]Transportation Security Administration. “TSA Works with New York Transit Agencies To Increase Security.” http://www.tsa.gov/press/happenings/tsa_ny_transit_agencies.shtm (accessed May 20, 2008).
[139] Transportation Security Administration. “Expanding Partnerships for Security Enhancement.” http://www.tsa.gov/what_we_do/tsnm/mass_transit/partnerships.shtm (accessed May 20, 2008).
[140] Ibid.
[141] Titan Systems Corporation. *Arlington County After-action report on the response to the September 11 terrorist attack on the Pentagon*. 2002. http://www.arlingtonva.us/Departments/Fire/edu/about/docs/after_report.pdf (accessed May 28, 2008).
[142] Ibid.
[143] Baker, Al. “New Operation to Put Heavily Armed Officers in Subways.” *New York Times*, February 2, 2008. http://www.nytimes.com/2008/02/02/nyregion/02machinegun.html?emc=eta1 (accessed May 21, 2008).
[144] Blair, Tony. "The Changing Relationship between Politics and the Media in the 21st Century." London: Prime Minister's Office, 2007.
[145] Beccaria, Cesare. *Beccaria: 'On Crimes and Punishments' and Other Writings*, ed. Richard Bellamy, trans. Richard Davies (Cambridge, England: Cambridge University Press, 1995), 1-229.
[146] Malone, Robert. “Worst Cities For Traffic.” *Forbes*, February 7, 2006. http://www.forbes.com/2006/02/06/worst-traffic-nightmares-cx_rm_0207traffic.html (accessed May 29, 2008).
[147] Metro Media Relations. “Metro Board Takes Step Toward Putting New Transportation Sales Tax on November Ballot.” Metro Los Angeles, http://www.metro.net/news_info/press/Metro_066.htm (accessed May 26, 2008).
[148] Kettl (2003), 274.
[149] Interview with Boston Fire Department Lieutenant, November 1, 2007.
[150] Kettl (2003), 269.
[151] Krauss, Clifford. “Gas Prices Send Surge of Riders to Mass Transit.” *New York Times*. May 10, 2008. http://www.nytimes.com/2008/05/10/business/10transit.html?emc=eta1 (accessed May 30, 2008).
[152] American Public Transportation Association. “Heavy Rail Public Transportation Ridership Report.” http://www.apta.com/research/stats/ridership/riderep/documents/07q4hr.pdf (accessed May 28, 2008).