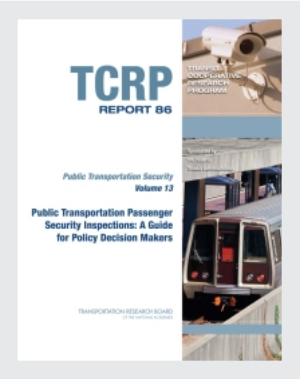

Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers

DETAILS

67 pages | | PAPERBACK
ISBN 978-0-309-42153-9 | DOI 10.17226/23150

AUTHORS

TRANSIT COOPERATIVE RESEARCH PROGRAM

TCRP REPORT 86

Public Transportation Security

Volume 13
Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers

Countermeasures Assessment and Security Experts, LLC
Camden, NJ

Waite & Associates
Reno, NV

Nakanishi Research and Consulting, LLC
New York, NY

Subject Areas
Planning and Administration • Public Transit • Transportation Law • Security

Research sponsored by the Federal Transit Administration in cooperation with the Transit Development Corporation

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2007
www.TRB.org

TRANSIT COOPERATIVE RESEARCH PROGRAM

The nation's growth and the need to meet mobility, environmental, and energy objectives place demands on public transit systems. Current systems, some of which are old and in need of upgrading, must expand service area, increase service frequency, and improve efficiency to serve these demands. Research is necessary to solve operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the transit industry. The Transit Cooperative Research Program (TCRP) serves as one of the principal means by which the transit industry can develop innovative near-term solutions to meet demands placed on it.

The need for TCRP was originally identified in *TRB Special Report 213—Research for Public Transit: New Directions,* published in 1987 and based on a study sponsored by the Urban Mass Transportation Administration—now the Federal Transit Administration (FTA). A report by the American Public Transportation Association (APTA), Transportation 2000, also recognized the need for local, problem-solving research. TCRP, modeled after the longstanding and successful National Cooperative Highway Research Program, undertakes research and other technical activities in response to the needs of transit service providers. The scope of TCRP includes a variety of transit research fields including planning, service configuration, equipment, facilities, operations, human resources, maintenance, policy, and administrative practices.

TCRP was established under FTA sponsorship in July 1992. Proposed by the U.S. Department of Transportation, TCRP was authorized as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). On May 13, 1992, a memorandum agreement outlining TCRP operating procedures was executed by the three cooperating organizations: FTA, the National Academies, acting through the Transportation Research Board (TRB); and the Transit Development Corporation, Inc. (TDC), a nonprofit educational and research organization established by APTA. TDC is responsible for forming the independent governing board, designated as the TCRP Oversight and Project Selection (TOPS) Committee.

Research problem statements for TCRP are solicited periodically but may be submitted to TRB by anyone at any time. It is the responsibility of the TOPS Committee to formulate the research program by identifying the highest priority projects. As part of the evaluation, the TOPS Committee defines funding levels and expected products.

Once selected, each project is assigned to an expert panel, appointed by the Transportation Research Board. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, TCRP project panels serve voluntarily without compensation.

Because research cannot have the desired impact if products fail to reach the intended audience, special emphasis is placed on disseminating TCRP results to the intended end users of the research: transit agencies, service providers, and suppliers. TRB provides a series of research reports, syntheses of transit practice, and other supporting material developed by TCRP research. APTA will arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by urban and rural transit industry practitioners.

The TCRP provides a forum where transit agencies can cooperatively address common operational problems. The TCRP results support and complement other ongoing transit research and training programs.

TCRP REPORT 86: VOLUME 13

Project J-10J
ISSN 1073-4872
ISBN: 978-0-309-09899-1
Library of Congress Control Number 2007906106

COPYRIGHT PERMISSION

NOTICE

The project that is the subject of this report was a part of the Transit Cooperative Research Program conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council. Such approval reflects the Governing Board's judgment that the project concerned is appropriate with respect to both the purposes and resources of the National Research Council.

The members of the technical advisory panel selected to monitor this project and to review this report were chosen for recognized scholarly competence and with due consideration for the balance of disciplines appropriate to the project. The opinions and conclusions expressed or implied are those of the research agency that performed the research, and while they have been accepted as appropriate by the technical panel, they are not necessarily those of the Transportation Research Board, the National Research Council, the Transit Development Corporation, or the Federal Transit Administration of the U.S. Department of Transportation.

Each report is reviewed and accepted for publication by the technical panel according to procedures established and monitored by the Transportation Research Board Executive Committee and the Governing Board of the National Research Council.

The Transportation Research Board of the National Academies, the National Research Council, the Transit Development Corporation, and the Federal Transit Administration (sponsor of the Transit Cooperative Research Program) do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the clarity and completeness of the project reporting.

Published reports of the

TRANSIT COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is one of six major divisions of the National Research Council, which serves as an independent adviser to the federal government and others on scientific and technical questions of national importance. The National Research Council is jointly administered by the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The mission of the Transportation Research Board is to provide leadership in transportation innovation and progress through research and information exchange, conducted within a setting that is objective, interdisciplinary, and multimodal. The Board's varied activities annually engage about 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

CRP STAFF FOR TCRP REPORT 86, VOLUME 13

Christopher W. Jenks, *Director, Cooperative Research Programs*
Crawford F. Jencks, *Deputy Director, Cooperative Research Programs*
S. A. Parker, *Senior Program Officer*
Eileen P. Delaney, *Director of Publications*
Ellen M. Chafee, *Assistant Editor*

TCRP PROJECT J-10J PANEL
Field of Special Projects

William J. Fleming, *Massachusetts Bay Transportation Authority Police,* (Chair)
Leonard E. Diamond, *Somerville, NJ*
Dorothy W. Dugger, *San Francisco Bay Area Rapid Transit District*
Ben Gomez, *Dallas Area Rapid Transit*
Michael E. Libonati, *Temple University, Philadelphia, PA*
Eugene Morabito, *Honeywell Technical Solutions, Inc.*
Erhart M. Olson, *Washington Metropolitan Area Transportation Authority*
Robin M. Reitzes, *San Francisco City Attorney's Office*
Richard Winston, *Chicago Transit Authority*
Anthony B. Tisdale, *FTA Liaison Representative*
Greg Hull, *APTA Liaison Representative*
Chas King, *Department of Homeland Security Liaison Representative*
Vincent P. Pearce, *U.S. Department of Transportation Liaison Representative*
Robert D. Phillips, *Transportation Security Administration Liaison Representative*

AUTHOR ACKNOWLEDGMENTS

The research reported herein was performed under TCRP Project J-10J by Countermeasures Assessment and Security Experts (CASE™), LLC, Camden, New Jersey. CASE™ was the contractor for this study, with Waite & Associates and Nakanishi Research and Consulting, LLC, serving as subcontractors.

Ernest "Ron" Frazier, Sr., Attorney, President of CASE™, was the Principal Investigator. Jocelyn K. Waite, Attorney, Principal of Waite & Associates, Reno, Nevada, was the Associate Investigator. Yuko J. Nakanishi, Ph.D, President of Nakanishi Research and Consulting, LLC, New York, New York, was the Assistant Investigator.

FOREWORD

By S. A. Parker
Staff Officer
Transportation Research Board

This thirteenth volume of *TCRP Report 86: Public Transportation Security* will assist public transportation agency senior staff, policy board staff, law enforcement, and security service providers in assessing the advantages and disadvantages of establishing a passenger security inspection program. The objective of *Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers* is to provide guidance that a public transportation agency may use when considering whether, where, when, and how to introduce a passenger security inspection program into its operations. The report is a useful ready reference guide that identifies (1) the most promising types of screening technologies and methods currently in use or being tested, (2) the operational considerations for the deployment of these technologies in land-based systems, (3) the legal precedent that either applies or that should be contemplated in connection with passenger screening activities, and (4) a passenger security inspection policy decision-making model. Detailed appendixes to this report are published as *TCRP Web-Only Document 38* and may be found on the TRB website at http://www.TRB.org/SecurityPubs.

Countermeasures Assessment and Security Experts, LLC, prepared this volume of *TCRP Report 86* under TCRP Project J-10J.

Emergencies arising from terrorist threats highlight the need for transportation managers to minimize the vulnerability of travelers, employees, and physical assets through incident prevention, preparedness, mitigation, response, and recovery. Managers seek to reduce the chances that transportation vehicles and facilities will be targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. By being prepared to respond to terrorism, each transportation agency is simultaneously prepared to respond to natural disasters such as hurricanes, floods, and wildfires, as well as human-caused events such as hazardous materials spills and other incidents.

This is the thirteenth volume of *TCRP Report 86: Public Transportation Security*, a series in which relevant information is assembled into single, concise volumes—each pertaining to a specific security problem and closely related issues. These volumes focus on the concerns that transportation agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the reports will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including a number of state departments of transportation. A topic panel of experts in the subject area was established to guide the researchers in organizing and evaluating the collected data and to review the final document.

This volume was prepared to meet an urgent need for information in this area. It records practices that were acceptable within the limitations of the knowledge available at the time of its preparation. Work in this area is proceeding swiftly, and readers are encouraged to be on the lookout for the most up-to-date information.

Volumes issued under *TCRP Report 86: Public Transportation Security* may be found on the TRB website at http://www.TRB.org/SecurityPubs.

CONTENTS

SUMMARY

Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers

Introduction

Securing transit, passenger rail, and other surface transportation systems in the United States is an issue of major importance for government and transportation agencies. The attacks against the transit and commuter systems of Madrid, Moscow, Mumbai, and London underscore the vulnerability of public transportation and the necessity of providing security for the people who depend on it daily. Public transportation facilities and systems present potential terrorists with highly visible symbolic targets, which, when attacked, yield maximum effect and devastation. Transit is essential to the economy of a metropolitan region, transporting workers to their place of employment and residents to shopping areas, essential services, and leisure activities. Also, the very essence of public transportation—providing open, accessible mobility to large numbers of persons—makes it extremely vulnerable to terrorism. Passengers congregate in transit vehicles, on platforms, and in waiting areas within terminals, making them ideal targets. Accessing the system anonymously is easy, and leaving the system is just as easy.

To protect their passengers, employees, and assets, U.S. transportation agencies have been conducting risk assessments, training employees and customers, and investing in a variety of security improvements. One of the security measures agencies have considered implementing is passenger security inspections (PSIs). PSIs are inspections conducted without warrants or individualized suspicion. Generally, such inspections are legally permissible only if they can be justified under exceptions to the warrant and individualized suspicion requirements of the Fourth Amendment to the U.S. Constitution. When individualized suspicion exists, inspections are subject to normal policing procedures.

PSIs include manual, visual, and technology-based inspections; canine inspections; and behavioral assessments. These four types of PSI are described below.

- PSIs using **manual inspection** methods usually involve the random selection of transit passengers and inspection of the contents of their bags or other objects in their possession. The officer may move the contents to reveal hidden items and open/unzip pouches within the article.
- PSIs using **visual inspection** methods also involve the random selection of transit passengers and inspection of the contents of their bags or other objects in their possession. However, in a visual inspection, the passenger or officer opens the bag, and the officer visually inspects the contents.
- PSIs using **technologies** can help transit police and transit personnel in the identification of explosives, metal, and other threat materials. Bulk detection technologies typically work by imaging the actual explosives, whereas trace detection technologies identify trace particles or

vapor residues from explosives. Some of these trace detection technologies and some metal detectors are available in mobile, portable, and handheld formats.
- PSIs can use properly trained **canines** that are able to perform inspections for explosives and are able to identify the source of the explosives. A key disadvantage is the canine's short effective work period (usually 30 to 45 minutes) and the canine's inability to inform its handler when it is "off-duty."
- PSIs using **behavioral assessment** involve the observation of passengers for suspicious behavior and can be performed by either transit police or transit personnel. If specific behaviors are observed, the passenger may be questioned, and an identification check may occur to further evaluate the passenger's behavior.

Purpose of the Research

The purpose of this research has been to develop guidance that a transit agency may use when considering whether to institute PSIs. The decision can involve a complex set of economic, political, operational, and legal elements. A transit agency must consider whether to implement passenger screening at all, and, if so, how it should be conducted. Should screening be suspicionless or based on behavioral profiling? Should screening be conducted daily or on the basis of threat levels? What method should be used for conducting the screening? Further complicating the decision of whether and how to implement passenger screening is the fact that these final two questions are related: screening methods that might be inappropriate for daily use may be appropriate under more specific circumstances. Each of the decisions concerning how to implement passenger screening has legal as well as operational implications.

For those agencies that make the decision to implement PSIs, the PSI method must be rationalized and justified. Agencies that decide not to implement PSIs should still develop contingency plans for changes in the threat environment.

The research team addressed these key questions about PSIs:

- When should PSIs be implemented?
- What PSI methods exist and which ones are appropriate under which conditions?
- What are the advantages and disadvantages of various PSI methods?
- What operational factors need to be considered?

PSI methods vary not only in effectiveness, intrusiveness, cost, and efficiency, but also in their legal ramifications, in terms of both constitutional and tort law. In fact, some methods that are less vulnerable to attack on constitutional grounds may be more vulnerable to tort actions. However, developing a constitutional passenger security screening program that is based on basic principles of sound planning should also result in a program that is reasonably defensible against tort actions. Therefore, the legal implications are important in that they affect both the development and implementation of the inspection policy, including the need for training to help minimize liability exposure.

The legal issues examined in this research were the following:

- Constitutional limitations on conducting PSIs (relevant case law includes cases related to fixed checkpoints, behavioral assessment, consent, profiling, drug-seeking or explosives detection dogs, luggage searches, administrative searches, special needs, airport security searches, and transit searches);
- Tort liability (in general, for constitutional violations, invasion of privacy, failure to exercise sufficient care, and dog exposure);
- Screening technology issues (federal standards, tort liability for invasion of privacy, tort liability for true innocuous/false positives, state health restrictions on certain screening technologies); and
- The legal implications of providing accommodations to people with disabilities.

Generally, random passenger inspections can be legally justified under an exception to the constitutional requirements for warrants or reasonable suspicion, provided that the inspections are properly configured, that is, designed to meet a substantial government need, no more intrusive than required, subject to neutral criteria, reasonably effective, and aimed at an objective other than general law enforcement. The legal cases to date suggest that a random inspection protocol (as opposed to one that requires inspecting all passengers) may pass constitutional muster if it creates sufficient uncertainty for would-be terrorists. Behavioral assessments may raise issues of racial/ethnic profiling and in some states may be subject to greater regulation under state law than under federal law.

One benefit of PSIs, in addition to detecting or deterring terrorist attacks, may include a perception of increased security on the part of customers; this, in turn, has potential secondary benefits of maintaining or increasing ridership. PSIs may also make the general public perceive their community to be more secure. However, none of these additional benefits can, on their own, provide a legal rationale for conducting PSIs.

The overarching rationale for determining when to deploy PSI countermeasures should be based on an assessment of the risk of terrorist attack of the specific transportation agency.

Findings

The following summarizes findings based on transit agency interviews and the literature review performed for this research.

Risk Assessment

Disparities were noted between large and small agencies in their perceptions of the risk of terrorist attack. There were also significant differences among agencies located in different geographic regions. Not surprisingly, the perception of risk has influenced whether and how PSIs have been implemented. The greatest disparity was observed between East Coast transit agencies and transit agencies in the rest of the United States. More specifically, transit customers in metropolitan regions affected by the terrorist attacks of September 11, 2001, were much more aware of their transit system's vulnerability and perceived risk levels to be higher than transit customers did in other regions. Transit customers in metropolitan regions were also more tolerant of security measures, including those that would cause delay and inconvenience.

With the exception of ferry operators, PSI implementation and method were heavily influenced by transit agency perceptions of how their customers perceived the risk of terrorist attack. The exception is caused by the existence of maritime security regulations that set the requirements for implementation of specific PSI procedures to which ferry operators must adhere.

Vulnerability

Different modes of transportation were perceived as having different levels of vulnerability. Rail was believed by transit agencies to be more vulnerable than buses, and ferries carrying vehicles were considered more vulnerable than ferries carrying passengers only. At all agencies interviewed by the research team, transit labor organizations have been requesting increased security and related training for their members.

Threats

The primary focus of PSI programs has been explosives because explosives have been the weapon of choice in many prior transit attacks. Significant amounts of explosives placed in key locations have the ability to cause severe damage to people and property and inflict significant financial loss. Agencies, however, are cognizant of other threats, such as chemical, biological,

radiological, and nuclear threats (CBRN) and have implemented or are considering the deployment of CBRN countermeasures.

Current PSI Deployment

Visual/Manual PSIs

In July 2004, during the Democratic National Convention (DNC), Boston became the first city in the United States to conduct random visual/manual baggage inspections. These PSIs, conducted by the Massachusetts Bay Transit Authority (MBTA) Police, were implemented in response to heightened concerns related to the DNC as a high-profile political event. The concern stemmed from the timing of the Madrid train bombings, which occurred just prior to Spain's elections.

In July 2005, in response to the London Underground bombings, the transit agencies in the New York/New Jersey metropolitan area also began random inspections of bags and other articles using manual/visual inspections.[1]

Technology-Based PSIs

PSI technologies have a long history of use in the U.S. aviation industry for passenger and baggage screening. Although aviation-style technologies have been tested on U.S. public transportation systems, they have not been deployed due to a number of issues.[2] While some of these issues, such as privacy, appear to overlap with issues that arise for passenger screening in aviation, public transit is markedly different from aviation or any other industry in several aspects. Public transit is designed to be easily accessible and reliable, it often has tight headways, and older systems have significant space constraints.

Transportation Security Administration (TSA) testing in 2006 of screening conducted on rail systems revealed significant problems with false alarm rates and the time it took to conduct secondary screenings. While the pilot testing conducted at a Port Authority Trans-Hudson Corporation (PATH) station in New Jersey demonstrated the operational feasibility of inspecting all passengers at a selected station using explosives detection equipment, it also revealed high operational costs and the relatively high space needs for the system. Furthermore, all interviewees except one ferry operator stated that it would be infeasible for them to implement an airport-style screening system because of operational and financial constraints.

Detection equipment that does not affect operations, cause customer delays, and require a large number of personnel is highly desirable. For instance, portable detection equipment is used by some agencies to screen suspicious or abandoned articles. Also, sensors that are embedded into ticketing machines or fare collection devices are being explored by the Department of Homeland Security (DHS). These types of technologies, as well as environmental monitoring technologies, are particularly appealing for use in transit environments with high ridership.

PSIs Using Canines

For a number of years canine teams have been used by airports and some transit agencies to detect explosives and drugs. Since the attacks of September 11, 2001, use of canines for explosives

---

[1]Public advocacy, civil liberties, and other organizations in both New York City and Boston have protested these PSIs and brought legal action against the agencies. However, the courts have upheld the agencies' right to conduct them. MacWade v. Kelly, Docket No. 05-6765-cv (2d Cir. August 11, 2006); MacWade v. Kelly, (slip op.) 2005 WL 3338573 (S.D.N.Y.); American-Arab Anti-discrimination Committee et al. v. Massachusetts Bay Transportation Authority, 2004 WL 1682859 (D. Mass. 2004).

[2]There has been limited use of portable trace detection technology as a countermeasure enhancement during the conduct of visual/manual inspections.

detection has been expanding. In 2004, TSA introduced its National Explosive Detection Canine Team program to encourage the use of canine teams for explosives detection on transit systems. Canine teams are able to detect explosives and clear suspicious packages and are viewed as being less intrusive to passengers than other PSI methods.

Behavioral Assessment as a PSI

Since September 11, 2001, state troopers at Boston's Logan Airport trained in the Behavior Assessment Screening System (BASS) have observed passengers for suspicious behavior and questioned passengers whose behavior triggers the system. Some transit agencies have begun to provide BASS training to their employees. For instance, the Washington Metropolitan Area Transit Authority (WMATA) has provided an 8-hour BASS training course to transit police. The course teaches officers to "assign a number value to certain behaviors and the total number determines the type of response required."[3] The TSA has also implemented a behavioral assessment program, Screening of Passengers by Observation Techniques (SPOT), which is being introduced at U.S. airports. In an attempt to reach beyond air security, the TSA formed Visible Intermodal Protection and Response (VIPR) teams to patrol mass transit systems. While there were initial start-up problems, the program was deployed in September 2006 at MBTA stations in Boston.

Legal Issues

Most interviewed agencies had considered the full range of constitutional and tort issues involved in implementing a PSI program, including invasion of privacy, injury/health effects, canine searches, and failure to exercise the required level of care before formulating PSI program policy objectives and methodology and implementing the program.

From a liability standpoint, agencies performing bag inspections preferred to inspect either all passengers entering a particular station or perform random inspections on the basis of a random number criterion in order to avoid allegations of racial profiling. There were no cases of a non-ferry transit system in which a PSI that involved inspection of all passengers had been implemented, except on a trial basis.

In terms of lawsuits, only two agencies that had implemented bag inspections had experienced lawsuits from civil rights/advocacy groups, and these lawsuits have been dismissed. No lawsuits have been brought against the other interviewed transit agencies conducting PSI programs.

Impact of PSI Programs on Agency Image and Customer Satisfaction

In general, interviewed agencies indicated that their customers were pleased to see increased presence of transit security personnel and increased security measures, including the PSI programs. The PSI bag inspection and canine inspection programs in major metropolitan areas have been receiving positive feedback from customers across the board and have improved agency image, customer perception of security, and customer satisfaction.

Collaboration with Local Law Enforcement, Emergency Responders, and the Community

Close collaboration with local law enforcement is important, especially for agencies with systems covering a large service area. In major incidents, having supplemental resources at hand will

[3]WMATA, "Metro Transit Police to Take Course to Identify Terrorists" (WMATA press release, March 9, 2006). www.wmata.com/about/met_news/PressReleaseDetail.cfm?ReleaseID=1140.

increase the response capability of the agency. One of the large multimodal transit agencies, which serves a large geographic area, has been training officers in local law enforcement agencies in emergency response procedures to augment transit agency forces in major emergencies, including terrorist attacks. The other large multimodal agencies also have a strong level of collaboration with local responders and their communities.

Conclusions

The insights gained from this project are summarized below.

Risk Assessment. PSI countermeasures should be appropriate for defending against the most likely potential threat in terms of both the would-be perpetrator and the threat material, (e.g. explosives). Agencies should be cognizant of sources, such as federal government intelligence agencies, through which threats against them may be identified, and the potential need to rapidly deploy PSIs in response to these identified threats. The potential for the government to establish security requirements for transit systems that include implementation of PSIs, as has been done in the maritime industry for ferry systems, should also be recognized.

Visual/Manual Inspections. From the perspective of the U.S. Constitution, suspicionless inspections should either apply to all passengers or be done on a (objectively) random basis. For most transit systems, it is not operationally feasible to inspect all passengers, so random inspections are the most likely choice for suspicionless inspections. As random inspections are random both in terms of *who* will be inspected and *where* the inspections will take place, they provide a strong deterrent to attackers, who seek to reduce the risk of detection through avoiding uncertainty. Involving counterterrorism experts in the development of the random protocol should increase the chance that the plan will be held to be reasonably effective.

Technology. Airport-style screening requires a large number of intensively trained personnel and was ruled out by all of the interviewed agencies, even those that had tested it. However, portable and handheld technologies were seen as being more amenable to transit for the following reasons:

- Handheld electronic explosives detection equipment assists transit officers in conducting PSIs;
- Portable trace detectors can quickly scan abandoned and suspicious packages for explosives, eliminating the possibility of having to shut down a system for hours; and
- Radiation pagers can continuously monitor for radiological threats and are mobile, so officers can patrol an entire system on foot.

Canines. Canine teams with explosives detection capability were seen as the best PSI option by many of the agencies. Canines' unobtrusiveness and their adaptability to the transit environment make them a viable countermeasure for broad-based implementation.

Behavioral Assessment. This method, which has been successfully used in Israeli airports, is starting to take hold with transit systems. With the right training (which may need to be extensive), personnel can be taught to look for suspicious behavior. Behavioral assessment programs do not require significant expenditures because existing staff can be trained in how to effectively use the PSI method.

Legal Issues. In addition to ensuring that inspections are random, key factors in developing a constitutional, suspicionless, inspection protocol include the following:

- Articulating the risk, which will support the existence of a substantial government interest;
- Ensuring that the privacy intrusion is reasonably effective, yet no greater than what is required to further the government interest;

- Ensuring that the inspection protocol does not further general law enforcement purposes;
- Basing inspection selections on neutral criteria; and
- Affording reasonable notice and opportunity to avoid the inspection.

Behavioral assessments may give rise to claims of racial profiling, and protocols for deploying this type of PSI should be carefully evaluated under state law. Properly conducted canine inspections are generally considered less intrusive than visual, manual, or technology-based inspections—under some circumstances they are not even considered searches for Fourth Amendment purposes. State law may prohibit the deployment of certain technologies or require licensing of inspection personnel and inspection of equipment at specified intervals.

Recommendations

On the basis of the research conducted for this study, the following recommendations are made:

1. **Conduct a Risk Assessment.** In order to determine the types and levels of countermeasures, including PSIs, required to provide adequate security for a transit system, the agency must conduct a risk assessment to understand the nature of current and future threats and vulnerabilities.
2. **Establish a Security Plan.** Having a system security plan that eliminates, reduces, or mitigates risk is essential for transit agencies. Even if an agency does not perceive an existing threat or vulnerability, a contingency plan for unexpected changes in the threat environment should be maintained. Establishing a security plan that includes contingencies for the implementation of a PSI program or provides a rationale for why such a program would not be implemented is advised.
3. **Understand Legal and Liability Issues.** State laws concerning searches, racial profiling, and the use of radiating technology on or near people may vary, as will standards for imposing civil liability for unauthorized searches (based on constitutional violations or invasions of privacy), racial profiling, and injuries to health caused by inspection technology. Each transit agency should conduct research on the laws of its own jurisdiction before adopting any PSI method and developing an implementation protocol. Protocols should minimize any invasion of privacy entailed in the inspection process. Appropriate training is critical to avoiding constitutional, privacy, or false imprisonment claims. Inspecting officers should be trained on when to call for or conduct secondary inspections and should be educated concerning the possibility of positive readings on detection equipment due to innocuous, nonthreatening circumstances. Such training of officers should help to avoid constitutional, privacy, or false imprisonment claims and minimize liability should claims arise. To fulfill requirements of the U.S. Constitution, suspicionless inspections should be kept separate from normal law enforcement activities.
4. **Understand Customer Perceptions.** In many cases, agency perceptions of risk differ from customer perceptions of risk. When this is the case, more customer education may be needed. Transit agencies may need to educate customers about specific risks and threats facing the system and what the agency needs to do to enhance security. However, such customer education should not involve releasing any information which would jeopardize security.
5. **Conduct Customer and Community Outreach.** Providing information about why the program is being implemented and what to expect, including possible delays, will help customers anticipate changes in their daily routine. Outreach is critical not just for good customer relations; it can also, in many instances, ensure the constitutionality of the program. In addition, outreach can be used to develop additional passive surveillance by encouraging the local community to alert law enforcement to suspicious activity or suspicious persons trying to gain access to the system.

6. **Collaborate with Local Law Enforcement and First Responders.** Close collaboration with local law enforcement on potential responses to terrorist incidents is important, especially for agencies with systems covering a large service area. In major incidents, having supplemental resources at hand will increase the response capability of the agency.

The PSI Decision-Making Model

Based on the research for this project, a decision-making model has been developed. The PSI decision-making model is designed to assist agencies in sorting through the complexities of this decision while maintaining the correct focus on risk reduction, elimination, or mitigation. The PSI decision-making model can also assist decision makers in determining the most appropriate PSI countermeasures for reducing the risk of would-be terrorists mingling with regular passengers as a means of attacking a transit system. When used as a part of an overall systems security approach, PSIs can help provide a more secure operating environment, even in the open access framework that typifies transit systems. The decision-making model is summarized below.

Risk Assessment

The first decision that must be made by a transit agency is whether there are any circumstances under which PSIs should be used as a countermeasure to protect critical assets. If the agency determines that there may be circumstances under which PSIs may be appropriate, an evaluation of PSI methods would then be made. The level or intensity of inspections should coincide with the level of risk of attack. A low risk of attack would signal the use of passive measures, with a contingency plan for heightened alert or specific intelligence scenarios. A medium risk would suggest the use of passive measures and low-level inspections, along with a contingency plan. A high risk would indicate the use of passive measures, visual/manual inspections, technology-based inspections, and plans for intensified screening.

Evaluation of PSI Methods

If the transit agency determines that there are circumstances under which PSIs may be appropriate, the transit agency must examine whether there are specific PSI countermeasures that should be deployed and the operating conditions associated with their use. The first step is to conduct an initial operational evaluation, determining the agency's operational parameters (such as available locations for deploying inspections, available operating environments, available personnel for conducting inspections, maximum time to inspect that can be tolerated, and budget for training and equipment acquisition) and comparing the operational features of various PSIs to the agency's operational parameters to determine whether there are PSI methods that the transit agency will not use regardless of legal analysis. For example, the agency may determine that its system configuration precludes deploying any PSI method that requires significant space for conducting inspections.

Following the initial operational evaluation, the transit agency must analyze the legal implications of any PSI methods still under consideration. The decision-making model contains information regarding the legal assessment of constitutional, tort, and Americans with Disability Act (ADA) ramifications, major risks, and mitigation of major risks for each PSI countermeasure. For example, for each method, training on necessary protocols is likely to mitigate liability.

For each suspicionless method, Fourth Amendment liability is likely to be mitigated by tying the inspections to clearly articulated threats, providing adequate notice of inspections, affording the opportunity to avoid the inspections, and limiting the scope of inspections to the threat.

Although the notice aspect would be nonapplicable, using these same mitigation methods to limit liability would apply to suspicion-based inspections as well.

Policy/Protocol Development

Once the transit agency has determined that there is sufficient justification to deploy PSIs as a countermeasure to terrorism, the next step is to establish written policy to govern inspections that specifies the purpose and scope of the inspections. Deterrence of terrorist attack is an acceptable purpose for an appropriately designed inspection policy. The agency should also develop protocols and procedures for personnel to follow in implementing the policy. In addition to articulating the purpose of the inspections, the protocol should calibrate the inspection to discover the identified threat, have credible support for the program design, be deployable as set forth in the policy, contain procedural safeguards, limit the discretion of the inspecting officer, provide adequate notice of the inspections and opportunity to avoid them by not entering the system, specify when secondary inspections are necessary, and minimize invasion of privacy. Other issues to cover include dealing with passengers who decline screening and attempt re-entry, explaining when the inspection crosses the threshold from administrative inspection to suspicion-based search (still allowed), providing direction as to how to handle the discovery of contraband, and announcing threats to the public. In the event the agency decides not to immediately implement inspections, the agency should identify particular threat levels or other indicators that will control when inspections will take place. As a part of this contingency planning, those countermeasures that can be deployed rapidly in response to changing conditions should be prioritized. Indicators will also be relevant for intensifying existing inspection methods. The transit agency should also consider measures that will mitigate any potential legal liability. Mitigation issues to consider include the intrusiveness of the inspections (constitutional implications and privacy concerns), possible claims for unreasonable detention, and the health risks of various technologies.

Assessment of PSI Methods

Once the transit agency identifies PSI countermeasures deemed appropriate, it must consider whether there are further options for deployment. For example, if the agency selects canine inspections, it will have to determine what opportunities exist for receiving assistance and support from DHS and/or TSA or whether to acquire the canines through other means. If the canines are to be acquired through other means, the agency will have to decide between in-house and contracted provision of services, requiring evaluation of training methods and procurement sources. Should the agency select a technology-based method, such as trace detection, it will have to evaluate different models of the equipment. In the case of officer inspections, there may be options in terms of whether to contract with outside security firms to perform the inspections. To assist agencies in the decision-making process, the following parameters, in the form of checklists, are provided in the decision-making model: equipment parameters, personnel parameters, passenger service impact parameters, cost parameters, and operational parameters.

CHAPTER 1

Introduction

The inherent characteristics of public transportation systems make them vulnerable and attractive in terms of terrorist attacks. The U.S. Department of Transportation's Office of Intelligence and Security estimated that in the 1990s transit was the target of 20 to 35% of terrorist attacks worldwide.[1] Transit is a transportation mode that is vast, open, and widely available to the general public. Commuters in crowded urban areas use it on a daily basis. Transit vehicles "containerize" and enclose transit riders in a limited space. Platforms and waiting areas at passenger terminals are usually enclosed areas where large numbers of passengers congregate. Getting access to the transit system anonymously is easy, and leaving the system is just as easy.

The objective of this project was to develop guidance for public transportation agencies considering the introduction of a passenger security inspection (PSI) program into their operations. The project's aim was to provide guidance on evaluating whether or not a PSI program should be established, as well as on where, when, and how such a program, if established, should be implemented. The research team examined the existing and emerging security inspection methods and technologies and interviewed agencies to determine their perspectives on PSIs and on the techniques and use of screening technologies.[2] The interviews conducted for this research revealed that transit agencies in the New York/New Jersey metropolitan area have been conducting PSIs, in the form of bag inspections, since July 2005, as a result of the bombings of transit in Madrid (2004) and London (2005). Boston conducted PSIs in conjunction with the 2004 Democratic National Convention and has recently initiated bag inspections as well. State troopers at Boston's Logan Airport began implementing behavioral assessments after the attacks of September 11, 2001. Several other transit agencies are also conducting, or have begun training in, behavioral assessments. The use of canine teams as a PSI method is more prevalent. Even before September 11, 2001, some agencies had been using canine teams to detect narcotics and illegal weapons. A Government Accounting Office (GAO) study revealed that 21 passenger rail operators were using canine teams, primarily for explosives detection purposes.[3]

It is important to understand the characteristics of public transportation that distinguish it from other forms of transportation, including aviation, and that need to be considered in the selection and implementation of PSI methods and technology. Public transit is a mode that has been designed to be open and available to the general public, more so than any other mode. Commuters in crowded urban areas use public transit on a daily basis. For many, especially those riders without automobiles and low-income riders, public transit is the only available mode of transportation; without it, they would find it very difficult to conduct the activities essential to daily living. Therefore, public transit is viewed by many people as a necessity and also as a right. Another characteristic of public transportation systems is their significant space constraints. The subway systems in urban areas were built decades ago, some of them near the turn of the twentieth century. These systems are especially difficult to modify. A third characteristic of public transportation is frequent service, especially during peak hours and in urban areas. In the airline industry, flights to a particular destination may depart every 2 or 3 hours, and passengers are required to arrive at the airport at least 90 minutes prior to their departure time. In the transit industry, train and bus headways are often 5 minutes or less, and passengers arrive randomly when service is frequent. Slight delays could

[1] FTA, http://transit-safety.volpe.dot.gov/Security/Default.asp.

[2] In this report, the terms "inspection" and "screening" are used interchangeably.

[3] U.S. General Accounting Office (GAO), *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts* (Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives—Statement of Cathleen A. Berrick, Director, Homeland Security and Justice Issues), GAO-07-459T (Washington, DC: GAO, February 2000).

cause major disruptions of the regularity of transit service by overcrowding ticketing areas or platforms. Delays that cause a passenger to miss a train or bus would be a problem even during periods of time when there is infrequent service. Finally, it is important to note that public transportation systems are the most vulnerable mode of transportation in terms of terrorist attacks. According to a 2002 GAO report, about one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked.[4]

Modal Perspective

According to the Bureau of Transportation Statistics, 9.6 billion unlinked passenger trips using public transportation were made in 2004 and approximately 33 million transit trips are taken each weekday. The number of trips has grown by more than 23% since 1995.[5] Public transportation can be categorized into specific modes, and each has attributes that influence the system's vulnerability to attack. The primary modes are subway, bus, light rail, commuter rail, motorcoach, and ferry. The characteristics of each mode are summarized below.

Subway

In 2004, 9.4 million subway trips were taken daily, and many agencies consider subway the most vulnerable mode.[6] Large numbers of people are able to access trains anonymously, especially during peak hours. Older systems have many hiding places for terrorists and criminals. Also, packages and bags abandoned on platforms are difficult to identify and assess.

Bus

Sixty percent of all daily transit trips (19.6 million in 2004) are taken by bus.[7] While buses have been attacked in Israel and other countries, bus transit receives less attention than subway in the United States and is perceived to be less vulnerable. However, local buses are also vulnerable to being commandeered by terrorists, and bus passengers are vulnerable to being taken hostage. The buses themselves have the potential to be used as weapons. Bus transit security measures typically include video monitoring, canine inspections, bus operator awareness/observation, and pre-trip inspections. While it would be infeasible for agencies to install detection portals at all bus stops, even within a small system, and difficult to conduct random PSIs, multimodal passenger terminals are feasible locations for PSIs and installation of detection equipment. Note that testing of a baggage screening system has taken place in an intercity bus terminal setting.

A 2002 International Transit Studies research effort sponsored by the TCRP assessed safety and security at bus systems in small- to medium-sized cities in Western Europe.[8] This assessment noted than European transit agencies agreed that although the potential existed for random acts of terror, system security interests were best served by addressing day-to-day "acts of lawlessness," which have a direct and immediate effect on personnel and services. The agencies reported that they have lived with random acts of terror for decades and have adapted themselves to the condition.

Light Rail

In 2004, 1.2 million light rail trips were taken daily.[9] Because light rail systems often operate as open systems, without defined access points or turnstiles, the systems are vulnerable to attack; at the same time, certain PSIs are difficult to implement. However, PSIs using canines are being implemented. In addition, fare inspections provide deterrence against attacks because of the presence of transit officers.

Commuter Rail

In 2004, 1.4 million commuter rail trips were taken daily.[10] Commuter rail was the target of a massive terrorist attack in Madrid in 2004; therefore, attacks are of concern to rail system operators in the United States. Metro-North Railroad, a large commuter railroad system in the New York City metropolitan area, has been conducting PSIs since the London transit bombings in 2005 and has been implementing other security measures since the attacks of September 11, 2001. The National Railroad Passenger Corporation (AMTRAK) requires passengers to present a valid form of photo identification while on the system. All persons 18 years or older must have identification to purchase a ticket from a station agent or to check baggage. At boarding gates or on board trains, passengers are subject to random checks to ensure that they possess a form of identification that matches their issued ticket.

---

[4] GAO, *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges* (Report to Congressional Requesters), GAO-03-263 (Washington, DC: GAO, December 2002).

[5] Bureau of Transportation Statistics, http://www.bts.gov/publications/national_transportation_statistics/2006/html/table_transit_profile.html.

[6] Ibid.

[7] Ibid.

[8] K. Harrington-Hughes, *TCRP Research Results Digest 58: Safety and Security Issues at All-Bus Systems in Small- to Medium-Sized Cities in Western Europe* (Washington, DC: Transportation Research Board of the National Academies, 2003).

[9] Bureau of Transportation Statistics, http://www.bts.gov/publications/national_transportation_statistics/2006/html/table_transit_profile.html.

[10] Ibid.

Motorcoach

The motorcoach industry operates intercity buses and chartered tour buses. As of 1999, the industry consisted of 4,000 private motorcoach companies operating in the United States and Canada who carried a total of about 860 million passengers.[11] The need for PSIs is underscored by the fact that intercity bus drivers and passengers have often been the targets of assaults. Buses are also vulnerable to being commandeered by terrorists, and their passengers are vulnerable to being taken hostage. The buses themselves are potential weapons. To enhance the security of their bus operations, intercity bus operators have been steadily increasing the number of security guards and video cameras at terminals and have instituted more thorough pre- and post-trip inspection procedures.[12]

The Transportation Security Administration (TSA), Greyhound Lines, Inc., and Peter Pan Bus Lines have tested a baggage screening program in Washington, D.C. The program, which took place in September 2006, screened luggage for explosives or bomb-making products. Greyhound was already randomly checking some passengers and carry-on luggage with a metal-detection wand on certain buses at certain terminals.[13] Motorcoach bus passengers generally arrive earlier at bus terminals than bus transit passengers because motorcoach bus service is less frequent than bus transit service; therefore, there is more time to screen motorcoach bus passengers than there is to screen bus transit passengers. Also, the larger bus terminals available to motorcoach operators facilitate passenger screening operations.

Ferry Operations

Many of the 487 ferry routes in the United States operate along the Eastern and Western seaboards in 26,000 miles of navigable channels.[14] Ferries typically carry many passengers and vehicles in an enclosed space. Vehicles are able to transport large amounts of explosives and have many areas where items can be concealed. These facts make ferries vulnerable to terrorist attacks. All vehicles on ferries are subject to screening requirements set by the Maritime Transportation Security Act of 2002 (MTSA). Regulations based on the MTSA became effective on July 1, 2004. As mandated, all passenger vessels regulated under 46 CFR subchapters H and K need to comply with 33 CFR Part 104, Vessel Security. Small passenger vessels regulated under 46 CFR subchapter T on domestic voyages need only comply with the new rules for general security and port security found in 33 CFR Parts 101 and 103. In addition to screening requirements, there are added and new regulations for training and drills for vessels and terminals, approved security plans, onsite assessments by the Coast Guard, designated company and vessel security officers, Declarations of Security between terminals and vessels, and Automatic Identification Systems (AIS).[15] Immediately after the London bombings in July 2005, the national security threat level was increased to Orange, indicating a high risk of terrorist attacks for mass transit. The Coast Guard directed an increase in security measures to Maritime Security Level 2 for the 300 or so ferries that had the capacity to carry 150 passengers or more. These 300 ferries transport more than 135 million persons annually.[16]

Federal and State Mandates and Initiatives

Currently, with the exception of ferry operations, there are no federal mandates for transit agencies to perform PSIs. However, federal agencies have been providing both money and resources to assist agencies in security training and implementation of security measures. The Department of Homeland Security's (DHS's) Office of Grants and Training has given over $320 million in grants to rail transit agencies through the Urban Area Security Initiative (UASI) and the Transit Security Grant Programs. As a condition for receiving these grants, an agency must complete a risk assessment that allows an agency to allocate resources to the highest priority security needs. The FTA has sponsored the creation of security awareness courses and other basic security courses for transit agencies. The FTA also requires that 1% of its funds be spent on security improvements. Additionally, federal agencies have been promoting the development of explosives and other threat detection equipment, and TSA has been partnering with transit agencies across the United States to test existing and emerging security technologies. The Transportation Security Act of 2001 mandated the screening of all checked baggage at airports. This has fueled the increase in the development, production, and procurement of both bulk detection and trace detection equipment.

Security Practices

For U.S. transit systems, the traditional and most common method of PSI has been the deployment of police or

[11] Bureau of Transportation Statistics, http://www.bts.gov/publications/transportation_statistics_annual_report/2001/html/chapter_03_table_01_036. html.
[12] U.S. House of Representatives Committee on Transportation and Infrastructure Subcommittee on Highways, Transit and Pipelines, *Transit and Over-the-Road Bus Security,* Prepared Statement Submitted by Peter J. Pantuso, 109th Cong., 2nd sess., March 29, 2006, 127–139.
[13] Keith Gates of TSA, conversation with author at Critical Transportation Infrastructure Protection Committee Meeting at TRB Annual Meeting, January 24, 2006.
[14] Bureau of Transportation Statistics, http://www.bts.gov/publications/pocket_guide_to_transportation/2006/html/table_01.html.
[15] 33 C.F.R. Part 104—Maritime Security: Vessels (2007). http://www.mxak.org/regulations/homeland/33cfr104.htm.
[16] S. Sapp, "Coast Guard Increases Security Following London Bombings" (U.S. Coast Guard Press Release, July 12, 2005).

security forces. Trained security personnel who are skilled in observation and surveillance are deployed at transportation facilities to detect suspicious activities and prevent security incidents. However, in July 2004, in conjunction with security concerns at the Democratic National Convention, the Massachusetts Bay Transportation Authority (MBTA) police used administrative search criteria to conduct warrantless searches of passenger luggage and belongings. Since that time, police in the New York and New Jersey area and in other cities have initiated similar programs. Transit agencies have also sought out technology that can improve security. Police and security forces are increasingly being augmented by technologies designed to improve detection capabilities.

Like foreign agencies, most U.S. transit agencies have increased transit officer presence and the number of roving patrols and have established customer awareness programs that inform transit passengers of the importance of being aware of—and alerting staff or security personnel to—suspicious packages, persons, and behavior. Domestic agencies have been providing all operational personnel and most other employees with basic security awareness training. Counterterrorism training and other specialized training are not generally provided by agencies, particularly not on a widespread basis. Also, while some agencies do engage in agencywide or multiagency drills and exercises, frontline operators are often excluded. Financial constraints have been cited as a reason. The need for additional training and security resources has been recognized by labor organizations, which have been requesting increased security measures, including more security training for their members. U.S. and foreign transit agencies are also starting to incorporate security considerations into the design of transit systems and facilities.

A recent GAO study on passenger rail security reports that foreign transit systems use three security practices not used in the United States.[17] They are random screening, covert testing, and a national clearinghouse on technologies and best practices. The study also notes that four European nations—England, France, Belgium, and Spain—each have one nationalized rail system with the national police force patrolling it. Some of the transit agencies interviewed for this project indicated that they engage in random inspections and covert testing; most of these transit agencies established these security practices in the period following September 11, 2001. Results of TCRP studies (such as this project) that describe best practices and technologies are disseminated or are readily available to all U.S. transit agencies.

Security Inspection Technologies

Security inspection technologies to address public transportation system security vulnerabilities are rapidly changing. Some technologies have been in existence and in use in aviation settings for decades. Examples include X-ray scanning technology, explosives detection canines, radiation pagers, and metal detectors. Newer products and technologies have been undergoing intensive development since September 11, 2001. Some of these technologies are being introduced at airports and are being tested for the transit environment. These technologies include puffer portals and document scanners that use trace detection technologies such as ion mobility spectrometry (IMS). More advanced security solutions, such as automated environmental sensors and nanotechnologies, are being researched. These technologies are expected to deliver quantum improvements in functionality.

Older generations of security technologies are being utilized in innovative ways. For instance, closed-circuit televisions (CCTVs) have been the most common form of security technology that has been implemented by U.S. transit agencies. Advanced use of this technology includes smart video surveillance that alerts personnel to suspicious activities and abandoned packages. Smart video technology has been implemented by major European transit authorities; however, it has been implemented by only a few U.S. systems. The combination of this technology with radiological and other threat sensors allowing the visual tracking of the sources of radiological threats is under development.

Electronic access control has also been widely implemented in the United States to prevent unauthorized personnel from entering railyards, bus depots, command centers, or other potentially sensitive transit facilities. Biometric technologies integrated into electronic access control mechanisms are being introduced to provide another significant layer of security. Transportation industry identity authentication systems are usually characterized by three factors: (1) something that you know, such as a password; (2) something that you have, such as an ID badge; and/or (3) something that you are, such as your fingerprints or your face. Agencies are starting to implement the third factor, biometric applications, in their authentication processes; expanded use of biometrics is expected once the Transportation Worker Identification Credential (TWIC) program is fully under way.[18]

Radiological detection equipment is in use by some of the larger U.S. agencies, and chemical detection equipment is being used or tested as well. Biological detection equipment is under development. Explosives detection equipment,

[17] GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (Report to Congressional Requesters), GAO-05-851 (Washington, DC: GAO, September 2005).

[18] Y. J. Nakanishi and J. L. Western, "Advancing the State of the Art in Identification and Verification: Biometric and Multibiometric Systems" (paper presented at 86th Annual Meeting of the Transportation Research Board, Washington, DC, January 2007).

primarily portable trace detectors, has been procured and is in use in some of the transit systems. In transit systems, trace detectors are used to screen suspicious or abandoned packages or objects for explosives, minimizing or alleviating the need to shut down the system for an extended period of time.

Additional coverage of security technologies for PSIs is provided in subsequent sections of this report. Airport-style screening equipment, including magnetometers and baggage conveyors, has been tested in evaluation programs led and sponsored by TSA. Currently, one agency, a ferry operator, is using airport-style inspection methodology. In general, however, transit agencies that conduct (or are planning to conduct) PSIs prefer methods such as canine inspections, desktop or portable trace detectors, and manual and visual/behavioral inspections.

CHAPTER 2

Passenger Security Inspection (PSI) Methods

Cities and transit systems outside the United States have had considerably more experience than U.S. cities and transit systems with terrorism and have already implemented many security measures, including CCTVs and smart cameras. PSIs and other security measures—such as video surveillance of public locations—are more acceptable to the populations and customers of systems outside the United States than they are to populations and customers of systems in the United States. In Israel, PSIs using behavioral assessments and technologies, such as handheld metal detectors and explosives detection portals, occur on a daily basis. PSIs occur not only at Israeli airports but also at transit terminals and bus and train stations. In fact, these security inspections have been integrated into daily life; they occur at shopping malls, supermarkets, office buildings, and other public places. This integration of PSIs into daily life in Israel has made implementation of PSIs in its transit systems easier and more amenable to the public. In Europe, Eurostart—a high-speed train connecting London to Paris, Brussels, and other cities through the channel tunnel—has implemented an airport-style screening system. Passengers are required to arrive about 45 minutes ahead of their scheduled departures and must go through a security checkpoint that uses magnetometer walk-through portals.

In the United States, Boston was the first city to conduct PSIs. In July 2004, during the Democratic National Convention, MBTA transit police conducted random baggage and identification checks at major rail stations in response to increased security concerns following the Madrid commuter rail attacks earlier that year. Behavior pattern recognition training was provided to the MBTA transit police by state police officers stationed at Logan airport so that suspicious behavior could be identified.[19] In July 2005, in response to the London transit bombings, the transit agencies in the New York/New Jersey metropolitan area began random inspections of bags and other objects, primarily at major transit hubs. Initially, these inspections were limited to manual and visual checks; however, in 2006, the inspections were expanded to include the use of electronic trace detection equipment.[20] Canine inspection is also used at one agency for both primary and secondary inspections at random checkpoints.

Public advocacy groups, civil liberties groups, and other organizations in both New York and Boston have protested the PSIs adopted in response to transit bombings overseas and have brought legal action against the agencies. However, the courts have upheld the right of the agencies in conducting them.[21] As evidenced by the transit agency interview results, agencies in other metropolitan areas conduct PSIs using canines because canine inspection is viewed as less intrusive than manual, visual, and electronic inspection methods.

Boston has also been using behavioral assessment to conduct PSIs within its transit system and at its airports. Because behavioral assessment has been highly successful in airline passenger screening in Israel, it has been gaining interest in the United States and is being introduced into transit systems in other cities.

PSI methods can be used for primary and/or secondary screening. Certain methods, such as explosives detection portals, would be more likely to be used for primary inspections than for secondary inspections. Other methods, such as canine inspections, can be used for either.

The randomness of PSI location is important because inspection of 100% of passengers is not feasible for most transit systems. Randomness provides legal, operational, and security

[19] M. Daniel, "MBTA set to begin passenger ID stops," Boston.com, May 22, 2004. http://www.boston.com/news/local/articles/2004/05/22/mbta_set_to_begin_passenger_id_stops/.

[20] A summary of the New York and New Jersey programs can be found in B. M. Jenkins and B. R. Butterworth, *Selective Screening of Rail Passengers,* MTI Report 06-07 (San Jose, CA: Mineta Transportation Institute, February 2007), 36–37.

[21] J. Preston, "Police Searches in the Subways Are Upheld," *New York Times,* December 3, 2005.

benefits. Legal benefits include a diminished probability of allegations of racial/ethnic profiling, operational benefits include a decreased probability of queues occurring, and security benefits include the deterrence effect of randomness.

PSIs Using Manual or Visual Inspection Methods

PSIs using manual or visual inspection methods involve the random selection of transit passengers and inspection of the contents of their bags or other objects in their possession. In a manual inspection, an officer opens a passenger's bag, inspects the contents, and may move the items within the bag to obtain a better view of the contents. In a visual inspection, the passenger opens his or her bag and the officer observes the contents but does not touch them. In order to minimize the invasion of passengers' privacy, officers may be trained to hide the contents of a bag from other passengers and not to read letters or other documents within the bag. Further details of these procedures are described in the summary of the transit agency interviews in Chapter 3.

PSI Technologies

PSI technologies have a long history of use in the U.S. aviation industry for passenger and baggage screening. Recently, use of PSI technologies has been initiated in port security to screen cargo. Although these technologies are being explored by, and some have been tested on, U.S. public transportation systems, they have not been deployed for 100% passenger inspections because of a number of issues. While some of these issues, such as privacy, appear to overlap with issues that arise in passenger screening for aviation, public transit is different in many aspects from aviation and other industries.

The two categories of explosives detection technologies are bulk detection and trace detection technologies. It should be noted that detection systems using these technologies still require human judgment and intervention to a greater or lesser extent. When the system issues an alarm, identification of the source of the alarm is needed. This is accomplished through secondary screening.

Bulk detection devices detect explosives by imaging the baggage contents and locating shapes of the explosive charge itself. Bulk detection devices can also identify any detonators, timers, or connecting wires. Bulk detection devices—specifically, certified Explosives Detection Systems (EDSs)—can also identify explosives in a direct manner by detecting the chemical or dielectric properties of the material. The key categories of bulk detection technologies are X-rays (including computer tomography for the current generation of EDSs), neutrons, electromagnetic imaging, and gamma rays.

Trace detection focuses on vapors or particles given off by explosives. These vapors or particles may be found on the surface of items that have come in contact with explosives or that have been in close proximity to explosives. These items include luggage, backpacks, documents such as tickets and boarding passes, and skin. Trace detection can be electronic/chemical or optical, or it can use biosensors.

The large investment in airport security and the attention given to the screeners and screening process suggest that a great deal of time, effort, and resources would be needed for transit agencies to develop and implement a robust screening system, especially when the system requires human intervention. A GAO report on screener training and performance measurement concludes that despite screener training and the resources expended on the screening process, "overall, weaknesses and vulnerabilities continue to exist in the passenger and checked baggage screening systems at airports of all sizes, at airports with federal screeners, and at airports with private-sector screeners."[22] This finding, combined with the perspective of many transit agencies that airport equipment would be operationally and financially infeasible for them, makes it unlikely that transit agencies, especially non-ferry agencies, will implement airport-style 100% passenger inspection systems. A description of the TSA airport screening methodology and training program is provided in Appendix C of this report.[23]

Detection equipment that does not affect operations and cause customer delays is highly desirable. For instance, sensors that are embedded in ticketing machines or fare collection devices are being reviewed by DHS, and plans are being made for testing them. These types of technologies, as well as environmental monitoring technologies, are particularly appealing for use at high ridership transit environments such as major transit hubs.

PSI technologies range from large scanners to portable and handheld devices. In terms of public perception and privacy for passenger screening, devices such as walk-through portals are generally considered less intrusive than handheld wands or manual searches because physical contact between the detector and the passenger does not occur. Standoff technologies are typically even less intrusive. Standoff detection is defined by the Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques of the National Research Council as follows:

---

[22] GAO, *Aviation Security Screener Training and Performance Measurement Strengthened, but More Work Remains* (Report to the Chairman, Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives), GAO-05-457 (Washington, DC: GAO, May 2005).

[23] For further reading on robust screening, see B. M. Jenkins and B. R. Butterworth, *Selective Screening of Rail Passengers*, MTI Report 06-07 (San Jose, CA: Mineta Transportation Institute, February 2007).

> Standoff explosive detection involves passive and active methods for sensing the presence of explosive devices when vital assets and those individuals monitoring, operating, and responding to the means of detection are physically separated from the explosive device. The physical separation should put the individuals and vital assets outside the zone of severe damage from a potential detonation of the device.[24]

However, one standoff technology, the X-ray backscatter technology, "sees" through clothing and has caused related privacy concerns.

The different PSI technologies have been categorized as people screening, baggage screening, and vehicle screening and are summarized below.

People Screening Technology

Portable Devices. Portable devices tend to be the size of a large suitcase, and some are heavy enough to require a hand/luggage cart to move. However, this type of device is still feasible to maneuver within various areas of a transit system, including on platforms and within trains and buses. The advantage of these mobile detectors is that they allow a variety of screening locations. Randomly altering screening locations may act as a high deterrent to terrorists.

Handheld Wands. Handheld wands are metal detectors used to detect weapons and contraband or trace detectors used to detect traces of explosives. Wands that are able to detect both metallic and nonmetallic objects concealed under clothing are under development.[25]

Walk-Through Portals. Walk-through portals can house traditional X-ray detectors, X-ray backscatter technology, or trace detection technologies. For trace detection technologies, the puffer method is used to direct streams of air that will dislodge explosive traces on clothing (if there are any) so that the detector will be able to identify them.[26, 27]

Fingertip Scan. The scan is small enough to be integrated into transit ticketing machines and could reduce potential delays that may be caused by other detection methods. Also, a detection device integrated into turnstiles is being tested by TSA.

Facial Recognition. Facial recognition technology has been used for surveillance and identification of suspected terrorists or criminals. Facial recognition is also in use by some states for identification purposes in the issuance of driver's licenses and identification cards. The advantage of this technology is that images can be acquired using standard camera or video equipment and can be compared against static photos without user cooperation. The use of this technology in transit terminals could assist officers in identifying terrorists and criminals. The disadvantages of this technology include a need for secondary screening (because the technology currently has a high false rejection rate) and privacy concerns.

Baggage Screening Technology

EDS Scanner. EDS is a system certified by TSA to find the "types, amounts, and configurations" of explosives than can bring down an airliner. Currently, EDS scanners all use CAT scanning technology, but not all EDS scanners will use CAT scanning in the future. A 1999 report points out that in this screening device a CAT scan uses medical technology housed in an EDS scanner to identify explosives and contraband. The equipment has the following key disadvantages: it is large (possibly too large for many locations within a transit system), extremely heavy, and expensive ($1 million or more per unit).[28]

Document Scan. A document scanner is a tabletop machine that evaluates tickets and other documents for traces of explosives.

Portable Devices. Handheld detectors may also be used to screen baggage.

Handheld Wands. Handheld detectors may also be used to screen baggage.

Vehicle Screening Technology

Car-Bomb Screener. One type of detection equipment that may be used to screen for vehicle-borne bombs is a mobile van or truck that houses explosives detection technology and sampling equipment. The van moves alongside a target vehicle and alerts the screener if a bomb is detected. This method is suitable for ferry terminals, which offer sufficient space for this type of screening technology.

---

[24] Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, *Existing and Potential Standoff Explosives Detection Techniques* (Washington, DC: National Research Council, 2004).

[25] S. G. Haupt, S. Rowshan, and W. C. Sauntry, *TCRP Report 86: Public Transportation Security—Volume 6: Applicability of Portable Explosive Detection Devices in Transit Environments* (Washington, DC: Transportation Research Board of the National Academies, 2004).

[26] Panel on Assessment of Technologies Deployed to Improve Aviation Security, Commission on Engineering and Technical Systems, *Assessment of Technologies Deployed to Improve Aviation Security: First Report* (Washington, DC: National Research Council, 1999).

[27] GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains* (Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives—Statement of Cathleen A. Berrick, Director, Homeland Security and Justice Issues), GAO-07-448T (Washington, DC: GAO, February 2007).

[28] Panel on Assessment of Technologies Deployed to Improve Aviation Security, Commission on Engineering and Technical Systems, *Assessment of Technologies Deployed to Improve Aviation Security: First Report* (Washington, DC: National Research Council, 1999).

Technology Assessment

In assessing PSI technologies, the first logical step would be to evaluate the operational feasibility of the technology types in a transit environment. The second step would be to compare technologies based on the following factors: accuracy, operational issues, legal issues, customer acceptance, health issues, and cost. If an objective evaluation is desired, the competing technologies would need to be implemented in the same location under the same conditions; otherwise, the test results may not be comparable. Once a technology has been selected, there are additional factors to consider in selecting a specific vendor and equipment model. These factors include the portability of the equipment, alarm capability, detection states, start-up time, resistance to interferants, power capabilities, battery needs, operational environment, and durability.[29] Finally, a pilot test is recommended to ensure that the selected model does indeed function as expected. Details about these assessment criteria are provided in Appendix B.

It should be noted that secondary inspections are always required to identify the source of an alarm, and the efficiency and effectiveness of secondary inspections should be considered by the agency in the selection of the PSI method for secondary inspections as well.

PSI Using Canines

Canine teams are viewed by many transit systems as a cost-effective way to enhance security. This PSI method, which has been used by airports and some transit agencies for a number of years in narcotics detection, is also perceived as minimizing constitutional and liability issues. In late 2005, TSA introduced a National Explosive Detection Canine Team to encourage the use of canine teams for explosives detection on transit systems. Ten transit agencies are a part of the National Explosive Detection Canine Team established by the TSA. The agencies selected for the program are the following: the MBTA, the San Francisco Bay Area Rapid Transit District (BART), the Southeastern Pennsylvania Transportation Authority (SEPTA), the Washington Metropolitan Area Transit Authority (WMATA), the Port Authority Trans-Hudson Corporation (PATH), the Chicago Transit Authority (CTA), the Los Angeles County Metropolitan Transportation Authority (Metro), the Maryland Transit Administration (MTA), the San Francisco Municipal Railway (Muni), and the San Diego Trolley, Inc. (SDTI). Other agencies using canine teams include New York City Transit (NYCT), New Jersey Transit (NJ TRANSIT), Dallas Area Rapid Transit (DART), MTA Metro-North Railroad (Metro-North), and Tri-County Metropolitan Transportation (TriMet).[30]

An important advantage of the canine teams of the National Explosive Detection Canine Team program is that they are not only able to detect explosives and clear suspicious packages but they can also follow trace residues to their source. Other canine teams that are already in use at the agencies that are part of the National Explosive Detection Canine Team program have been trained to perform one or more of these security- and safety related duties: act as deterrent patrols in stations, on platforms, in vehicles, in transfer centers, and in parking facilities; support special events management or crowd control; track persons, including lost or missing children; perform safety checks of transit facilities; locate victims during emergencies; support narcotics searches and forfeiture programs; pursue or search for persons who threaten the canine handler or other persons; and defend and/or protect public safety officers or other persons. Disadvantages of canines include their short effective work period and the inability of the canine to inform the handler when they have become ineffective. The latter is significant because the handler may believe that the canine is continuing to perform inspections when it is not.

Although its publication predated TSA's National Explosive Detection Canine Team program, the research reported in the second volume of *TCRP Report 86: Public Transportation Security* (titled *Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers*) indicated some advantages and disadvantages of using canine teams.

The advantages of using canine teams were the following:

- Use of canines is good for public relations, supports outreach with community and media, and provides a strong symbol for public safety.
- Canines are an effective tool for deterrence and order maintenance, passengers generally like the canine unit, and criminals are often fearful of trained police dogs.
- Use of canines supports a higher level of officer safety, and criminal fear of dogs reduces resistance during apprehension.
- Canines provide an effective resource for facility searches. One canine team can perform the work of four patrol officers.
- Canines are the most effective resource available for nonrepetitive detection of narcotics and explosives; no technology or other resource is better.
- Grants are currently available for dual function patrol and drug detection dogs.

[29] A. Fatah, J. Barrett, R. Arcilesi, K. Ewing, C. Lattin, M. Helsinki, *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders,* NIJ Guide 100-00 (Washington DC: National Institute of Justice, June 2000).

[30] DHS, "TSA Expanding National Explosives Detection Canine Teams to Mass Transit and Commuter Rail Systems," DHS Press Release (Washington, DC: TSA, October 6, 2005).

The disadvantages of using canine teams were the following:

- Consequences of poor planning are exacerbated by the importance of initial decision making to program capabilities and performance. Bad decisions cannot easily be overcome.
- Reliance on outside technical support is often necessary to start a canine program, a major vulnerability for a system new to this function.
- High program start-up costs, not averaged evenly over time, place a large emphasis on cost savings during the phase of project when spending is most essential.
- The difficulty of finding good dogs. Patrolling the transportation environment places additional strains on canines; selection testing is critical, but it is also expensive and not ready made for public transportation.
- The difficulty of selecting the right handler. Public transportation systems with limited experience may value the wrong traits or fail to recognize potential shortcomings prior to a major investment.
- The legal and public relations consequences of bites. The public has zero tolerance for what may be perceived as inappropriate force exerted by police dogs.
- The high demands of canine administration on supervisors with other responsibilities. Scheduling challenges limit availability of canines for service.
- Success requires a long-term investment—several months to a year.
- Constant effort is required to ensure that law enforcement and operations personnel are using the resources of the canine unit.

The estimated initial cost for one canine team that includes one handler and one canine was $118,650. This includes the handler's salary of $60,000 and initial training expenses of $9,000.[31]

Canine teams may be the only short-term method of screening a large number of people arriving in a terminal for the presence of explosives, as TSA is demonstrating at the Metropolitan Atlanta Rapid Transit Authority (MARTA). The dogs, however, must be trained to focus on people rather than objects. Additional costs for canine teams are continuing quality control and testing and the cost of ensuring proper control of explosives or simulants used in testing and training, particularly to prevent cross contamination.

[31] J. Balog, P. Bromley, J. Strongin, A. Boyd, J. Canton, and D. Mitchell, *TCRP Report 86: Public Transportation Security—Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers* (Washington, DC: Transportation Research Board, National Research Council, 2002).

Behavioral Assessment

Two long-standing law enforcement techniques—drug courier profiling[32] and hijacker profiling[33]—both employ the concept of behavioral assessment to detect and deter crime. As of September 2005, according to the GAO, behavior assessment is being utilized by at least eight rail transit systems as a countermeasure to terrorism.[34]

As of November 2006, there are several programs under which transportation authorities conduct behavioral assessments to screen passengers. These programs include TSA's Screening of Passengers by Observation Techniques (SPOT) program, TSA's Visible Intermodal Prevention and Response (VIPR) teams, and other TSA programs, as well as the Behavior Assessment Screening System (BASS) and the Behavioral Pattern Recognition program.

SPOT

SPOT is based on a previous TSA program called the Passenger Assessment Screening System, which was itself based on BASS. As of July 2006, SPOT was in use in 12 international airports in the United States and in trial runs in several smaller airports.[35] The TSA program, SPOT, employs routine screeners who have received an extra 4 days of classroom training in observation and questioning techniques and 3 days of field practice.[36] TSA describes the SPOT program as using "behavior observation and analysis techniques to identify potentially high-risk passengers" and further asserts that "individuals that exhibit suspicious behaviors, such as physical and physiological reactions, may be required to undergo additional screening."[37] TSA screeners have no law enforcement powers, so they cannot conduct interrogation themselves.[38] According to one source, screeners using SPOT

[32] *See, e.g.,* United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

[33] United States v. Bell, 464 F.2d 667 (2d Cir. 1972). When airplane hijacking became a major concern in the 1970s, detection relied heavily upon hijacker profiling and traditional policing. United States v. Moreno, 475 F.2d 44, 47 (5th Circ. 1973), *cert. denied,* 414 U.S. 840 (1973).

[34] GAO, *Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts* (Testimony Before the Committee on Transportation and Infrastructure, Subcommittee on Highways, Transit, and Pipelines, House of Representatives—Statement of JayEtta Z. Hecker, Director, Physical Infrastructure Issues), GAO-06-557T (Washington, DC: GAO, March 29, 2006), 10. www.gao.gov/new.items/d06557t.pdf.

[35] J. Martin, "Behavior Assessment: Targeting Suspects Scientifically," *GSN: Government Security News.* www.gsnmagazine.com/jul_06/behavior.html.

[36] E. Lipton, "Faces, Too, Are Searched at U.S. Airports," *New York Times,* August 17, 2006, Late Edition—Final, sec. A, p. 1, col. 3. www.nytimes.com/2006/08/17/washington/17screeners.html. (Article available for purchase at this URL.)

[37] TSA, "Where We Stand: TSA Trains Hard for New Threats." www.tsa.gov/press/where_we_stand/training.shtm.

[38] E. Lipton, "Faces, Too, Are Searched at U.S. Airports," *New York Times*, August 17, 2006, Late Edition—Final, sec. A, p. 1, col. 3. www.nytimes.com/2006 08/17/washington/17screeners.html. (Article available for purchase at this URL.)

look for "anxious, frightened, or deceptive behaviors." They then question passengers exhibiting such behaviors and score their answers against the SPOT index. The screeners then have four choices: they can (1) send the passenger through more intense checkpoints; (2) call local or airport police, who can conduct further questioning; (3) call in counterterrorism experts; or (4) take no further action.[39] The Israeli security official who helped train the officers for the BASS program has recommended that secondary questioning also be done by an officer with behavioral training.[40]

VIPR Teams

In an attempt to reach beyond air security, the TSA formed teams planned to patrol, among other things, mass transit systems in Atlanta, Philadelphia, Baltimore, and Washington, D.C., during December 2005. The teams included "two air marshals, one TSA bomb-sniffing canine team, one or two transportation security inspectors, one local law enforcement officer, and one other TSA employee."[41] However, it appeared that the program was not coordinated with local transit authorities, and it was significantly scaled back.[42] The program was deployed in September 2006 at MBTA stations that are significant links to Logan International Airport.[43]

Other TSA Programs

During the 2005 presidential inauguration, WMATA police were trained to observe passengers for suspicious behavior, including "avoid[ing] eye contact, loiter[ing], or appear[ing] to be looking around transit stations more than other passengers" and to question persons exhibiting such behavior about their activities and planned destinations. Security experts commenting on these procedures suggested that police should be able to articulate a reason for questioning a passenger.[44]

BASS

Since September 11, 2001, state troopers at Boston's Logan Airport trained in BASS have observed passengers for suspicious behavior and questioned passengers whose behavior triggers the system. Questioning may seem routine, such as asking the passenger's destination and requesting identification. The officers look for stress indicators in the passenger's response that suggest the person may be prepared to undertake a suicide mission.[45] BASS purports not to use "apparent race, ethnicity or religion as a basis of suspicion."[46] However, as discussed below, a lawsuit has been filed alleging that the program at Logan Airport employs illegal racial profiling. Dallas/Fort Worth International Airport has also deployed BASS-trained officers.[47]

Transit authorities have begun to employ BASS training. WMATA has provided an 8-hour BASS training course to transit police.[48] The course teaches officers to "assign a number value to certain behaviors and the total number determines the type of response required."[49] According to the Metro Transit police, posing operational questions to transit personnel, carrying maps or blueprints, or taking pictures of infrastructure would be deemed suspicious activities. The course also includes interview techniques, risk mitigation measures, and explanation of Fourth Amendment issues.[50] When the MBTA resumed random bag inspections in October 2006, it announced that it would also deploy tactically uniformed teams trained in antiterrorism and behavioral recognition techniques.[51]

---

[39] Associated Press, "MSP to Test Behavioral Screening System" (Minneapolis, MN: WCCO-TV, December 4, 2005). http://wcco.com/local/local_story_338134911.html.

[40] E. Lipton, "Faces, Too, Are Searched at U.S. Airports," *New York Times*, August 17, 2006, Late Edition—Final, sec. A, p. 1, col. 3. www.nytimes.com/2006/08/17/washington/17screeners.html. (Article available for purchase at this URL.)

[41] S. K. Goo, "Marshals to Patrol Land, Sea Transport: TSA Test Includes Surveillance Teams on Metro System," *Washington Post,* p. A1, December 14, 2005. www.washingtonpost.com/wp-dyn/content/article/2005/12/13/AR2005121301709.html.

[42] S. K. Goo, "New TSA Surveillance Tactic Curtailed Officials Confused over Test of Air Marshals at Transit Hubs: Metro Not in Program," *Washington Post,* p. A2, December 15, 2005. www.washingtonpost.com/wp-dyn/content/article/2005/12/14/AR2005121402366.html. CBS and Associated Press, "TSA Expands Marshal's Scope: Officers Descending on Transit Systems, Bus Stations, Ferries" (*CBS News* website, December 14, 2005). www.cbsnews.com/stories/2005/12/14/terror/main1124534.shtml.

[43] M. Daniel, "Heightened Security at Bus, Train Stops: Teams Assigned at Busiest Hubs to Logan Airport," *Boston Globe,* September 14, 2006. http://www.boston.com/news/local/articles/2006/09/14/heightened_security_at_bus_train_stops.

[44] S. K. Goo, "Metro Officers Keep a Keen Eye on Riders: New Behavioral Profiling Techniques, TSA Training Help Target Suspicious Subway Passengers," January 10, 2005, p. A6. www.washingtonpost.com/wp-dyn/articles/A61700-2005Jan9. html.

[45] A. Beshkin, "U.S. Airport Screeners Look for Behaviors" (NewsVOAcom [Voice of America website], October 2, 2006). www.voanews.com/english/archive/2006-10/2006-10-02-voa40.cfm.

[46] Institute of Police Technology and Management, "Terrorist Identification and Interdiction" (Brochure for 2-day course offered in June 2005). www.Iptm.Org/Flyers/027152.Pdf.

[47] M. Grabell, "Dallas/Forth Worth Airport Police Train to Detect Terrorists: Behavior Screening Helps Airport Officers See Suspicious Situations," *Dallas Morning News,* October 3, 2004. Article accessed and available at PoliceOne.com (title: "Texas Police Train to Detect Terrorists at Airport"). www.policeone.com/training/articles/92506/.

[48] WMATA, "Metro Security Enhanced Since the 2005 London Transit Bombings" (WMATA press release, July 6, 2006). http://www.wmata.com/about/met_news/PressReleaseDetail.cfm?ReleaseID=1296.

[49] WMATA, "Metro Transit Police to Take Course to Identify Terrorists" (WMATA press release, March 9, 2006). www.wmata.com/about/met_news/PressReleaseDetail.cfm?ReleaseID=1140.

[50] Ibid.

[51] M. Daniel, "MBTA Transit Police to Resume Random Bag Inspections" (MBTA Press Release, October 11, 2006). http://transitpolice.us/Press-News%20Releases%202006.htm.

Behavioral Pattern Recognition

Raffi Ron, an Israeli security expert, has trained personnel who work throughout airports, including parking lot attendants and flight attendants, in recognizing suspicious behavior. These personnel receive 4 hours of training about what behaviors to look for and where to report any suspicions. Law enforcement personnel receive 5 days of training that covers techniques for interviewing persons suspected of posing a terrorist threat, tactical response, and suspicious object handling. After the classroom instruction, the officers receive 4 hours of on-the-job training from experienced personnel.[52]

The National Transit Institute (NTI) has developed a Terrorist Activity Recognition and Reaction (TARR) course for transit employees who have direct contact with the public. According to the course description on the NTI website:

> The goals of the course are to provide participants with the knowledge and skills to:
>
> - Explain the importance of identifying and reporting pre-attack terrorist activity
> - Recognize the difference between normal, suspicious, and dangerous activity
> - Define their role in recognizing and reacting to suspicious activity
> - Describe their immediate actions when confronted with dangerous activity.

Tuition is waived for federal, state and local government employees who work in transportation or related areas. (See http://www.ntionline.com/CourseInfo.asp?CourseNumber=SA006a.)

Legal Implications of PSIs

The decision-making process concerning the implementation of passenger screening involves numerous considerations. A transit agency must consider whether to implement passenger screening at all, and if so, under what conditions. Should screening be suspicionless or based on behavioral profiling?[53] Should screening be conducted daily or based on threat levels? What method should be used for conducting the screening? These issues are interrelated, as screening methods that might be inappropriate for daily use may be appropriate under more specific circumstances.

Each of the decisions concerning passenger screening has legal as well as operational implications. The legal implications will inform both the development and implementation of the policy, including the need for training to help minimize liability. Passenger security screening can be accomplished using visual inspections (including behavioral assessments), physical inspections, explosives detection canines, X-ray equipment, and other explosives detection technology. These methods may vary not only in effectiveness, intrusiveness, cost, and efficiency, but also in their legal ramifications with regard to constitutional and tort law. In fact, some methods that are less vulnerable to attack on constitutional grounds may be more vulnerable to tort actions. However, the basic principles of sound planning needed to develop a constitutional passenger security screening program should also result in a program reasonably defensible against tort actions.

The legal issues examined in this research are the following:

- Constitutional limitations on conducting PSIs (fixed checkpoints, behavioral assessment, consent, profiling, drug-seeking or explosives detection dogs, luggage searches, administrative searches, specials needs, airport security searches, and transit searches).
- Tort liability (in general, for constitutional violations, for invasion of privacy, for failure to exercise sufficient care, and for exposure to canines).
- Screening technology issues (tort liability for invasion of privacy, tort liability for false/true innocuous positives, and state health restrictions on certain screening technologies).
- Legal implications of providing accommodations to people with disabilities.

These issues are discussed at length in the Appendix D of this report.

Conceptually, random transit security screening procedures can be shown to meet the constitutional requirements that they are (1) used in circumstances in which requiring reasonable suspicion or a warrant is impractical and (2) used to fulfill a substantial government need.[54] Procedures will be judged based on their intrusiveness (which will be balanced against the governmental need), will have to be subject to neutral criteria,[55] and must be reasonably effective. Notice of random inspections reduces the intrusiveness of the search. Prospective passengers should be afforded the opportunity to exit the system

---

[52] R. Elliott, "Assessing Threats from Passengers," *Security Management,* September 2006.

[53] MBTA has used a behavioral screening system to identify passengers exhibiting suspicious behavior. See GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (Report to Congressional Requesters), GAO-05-851 (Washington, DC: GAO, September 2005), 53. For discussion of the importance of training in recognizing terrorist behavior see "Statement by Raffi Ron to the Senate Committee on Homeland Security and Governmental Affairs, September 21, 2005." http://hsgac.senate.gov/_files/092105Ron.pdf.

[54] *See* United States v. Martinez-Fuerte, 428 U.S. 543 (1976). Inspections based on behavioral assessments will rely on reasonable suspicion rather than random selection.

[55] *See* Michigan Dept. of State Police v. Sitz, 496 U.S. 444 (1990).

without being subject to random inspection, and doing so should not, in and of itself, be considered suspicious behavior. The procedures will have to be clearly aimed at something (e.g., preventing explosives from entering the transit system) other than general law enforcement,[56] and should protect a need that cannot be protected by general policing. Not all security threats may be sufficient to establish a vital government interest as a matter of law. Deterrence may be judged a sufficient goal, and an inspection protocol that generates sufficient uncertainty for would-be terrorists may be judged reasonably effective under the legal balancing-of-interests test, even though many passengers are not searched. It should be noted that the inspection protocol should not vitiate the normal principles of reasonable suspicion, and training should cover differences between legitimate refusal to be inspected and behavior that can be reasonably considered suspicious.

Legal Implications of Behavioral Assessments

Introduction

The legal issues likely to be posed by conducting behavioral assessment to screen transit passengers include the reasonableness of any resulting searches and seizures[57] under both federal and state constitutions, and challenges to such searches and seizures as being race-based procedures in violation of the Fourteenth Amendment[58] and relevant state constitutions. In the heyday of airline hijacker profiling, some concern was expressed about pretexting, that is, using the hijacker profiles as an excuse to stop suspected drug offenders.[59] The use of behavioral assessment in the context of transit counterterrorism, let alone the law governing such use, is not yet sufficiently developed to determine whether pretexting will become an issue. Some states have rules concerning racial profiling that are stricter than the federal government's. Therefore, to the extent that racial/ethnic profiling is employed, caution is warranted because behavioral assessment is an area in which state and federal law may differ substantially.[60]

Recent Cases

There do not appear to be any recent decisions involving behavioral assessment in transportation, let alone in the transit context. The airport-related case of *Downing v. Massport* [61]—as of November 2006 still in pre-trial status—appears to be the only action challenging the constitutionality of a current behavioral assessment program. The following information about the case is provided for illustrative purposes only. There is no legal analysis inferred or implied.

Downing v. Massport involves a challenge to BASS implementation at Logan International Airport. The plaintiff alleges that he was unlawfully detained at the airport by state troopers and threatened with arrest unless he produced identification and his travel documents. The plaintiff's central argument is that state troopers took these actions despite the fact that there was no reasonable suspicion that he was engaged in wrongdoing.

The central allegations of *Downing v. Massport* are that the BASS training does the following:

- Directs or authorizes state police troopers to stop, question, and/or arrest certain individuals at Logan despite the absence of reasonable suspicion that the individuals were committing, had committed, or were about to commit any crime;
- Authorizes state police officers to deny access to Logan to any person who refuses to cooperate with police requests for identification or other information; and
- Effectively condones and encourages racial and ethnic profiling.[62]

The plaintiff is an African American and the national coordinator of the American Civil Liberties Union's (ACLU's) Campaign against Racial Profiling. The following summarizes the description given in the complaint of his encounter with state troopers at Logan:

---

[56] *See* City of Indianapolis v. Edmond, 531 U.S. 32 (2000). Plaintiffs in MacWade v. Kelly, 2005 WL 3338573 (S.D.N.Y.) argued unsuccessfully that a bag search policy on the New York City subway was ordinary law enforcement.

[57] For a more detailed discussion of search and seizure cases, see J. Waite, *TCRP Legal Research Digest 22: The Case for Searches on Public Transportation* (Washington, DC: Transportation Research Board of the National Academies, 2005).

[58] The Supreme Court, which has upheld some ethnic profiling, United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975); United States v. Martinez-Fuerte, 428 U.S. 543, 563 (1976), has held that it will decide challenges to searches motivated by race under the Fourteenth, rather than the Fourth, Amendment. Any such searches will be subject to strict scrutiny. Whren v. United States, 517 U.S. 806 (1996).

[59] Some judges expressed concern that airport searches based on hijacking profiles were turning up far more illegal drugs than the weapons that were ostensibly the targets of the searches. See United States v. Legato, 480 F.2d 408, 414 (5th Cir. 1973) (Goldberg, J., specially concurring), *cert. denied,* 414 U.S. 979 (1973); United States v. Cyzewski, 484 F.2d 509, 515-16 (5th Cir. 1973) (Thornberry, J., dissenting), *cert. denied*, 415 U.S. 902 (1974). However, one commentator has suggested that since air hijacking and drug courier profiling have come into use, the only objections have been in law review articles and dissenting opinions. J. L. Miller, *Search and Seizure of Air Passengers and Pilots: The Fourth Amendment Takes Flight,* 22 TRANSP. L.J. 199, 209–11 (1994).

[60] See "Profiling" in *TCRP Legal Research Digest 22,* pp. 18–20.

[61] King Downing, Plaintiff, v. Massachusetts Port Authority; the Massachusetts Department of State Police, State Police Trooper Thompson, State Police Sergeant Croxton, Thomas G. Robbins, and Peter J. Didomenica, Defendants. Complaint and Demand for Jury Trial, November 10, 2004. www.aclu.org/FilesPDFs/downing.pdf.

[62] Ibid., 4.

> After plaintiff, who was sporting a short beard and wearing casual clothing, deplaned at Logan, he made a phone call in a general access area of the airport. The plaintiff noticed that a state trooper was standing near him, apparently trying to overhear his conversation. The trooper demanded that plaintiff produce identification. The trooper refused to say why he wanted to see the identification, but told plaintiff that he would be removed from the airport if he refused to provide identification. Plaintiff then left the airport, but the trooper followed him outside and again demanded to see identification, responding to plaintiff's question whether he was under arrest, but refusing to state the grounds for the arrest. Before detaining plaintiff, the trooper did not ask any questions about plaintiff's travel that might have dispelled any suspicions he might have had about plaintiff's presence at Logan. The trooper radioed for assistance. A superior officer told plaintiff that he was being detained because the first trooper had concluded that he had acted suspiciously, but the superior officer could not, or would not, provide any description of the allegedly suspicious behavior or what had aroused the trooper's suspicion. Under threat of being handcuffed and taken to police lock-up, plaintiff produced his driver's license. After running the license through the police computer, the troopers insisted that plaintiff, under threat of being placed on Logan's trespass list, produce his airline ticket. After doing so plaintiff was released.[63]

Plaintiff has alleged that the BASS training employs a lesser standard than reasonable suspicion, uses race and ethnicity as a factor in determining whether a person is "suspicious," and uses a person's assertion of his constitutional rights as a basis for further detention or interrogation.[64] Plaintiff further alleged that his treatment violated Articles 1 and 14 of the Massachusetts Declaration of Rights, the Fourth and Fourteenth Amendments to the United States Constitution, and 42 U.S.C. § 1983. Although discretion is not addressed in the complaint, the ACLU has elsewhere asserted that BASS appears to leave the determination of what constitutes unusual or anxious behavior requiring action to the discretion of individual officers.[65]

Analysis of Legal Issues

Based on existing case law and as illustrated by the *Downing* complaint, the aspects of behavioral assessment that may raise constitutional issues include the following:

- Basis for reasonable suspicion
  - Use of subjective versus objective criteria
  - Amount of discretion exercised by officials conducting the assessments
  - Amount of training afforded the officials conducting the assessments
- Use of racial/ethnic criteria
- Consent
- Request for identification
- Questioning passengers about destination, travel plans, and related information.

Basis for Reasonable Suspicion.[66] The validity of hijacker profiles was generally recognized as a basis for reasonable suspicion without much analysis.[67] In one case, a defendant was searched for meeting a hijacker profile because he "paid cash for his tickets, did not furnish a phone number on his passenger information sheet, was Hispanic, was scheduled to board a flight within the range of Cuba, bought two one-way tickets, and declined to check any of the couple's five pieces of luggage."[68] Case review shows that the hijacker profile appears to have been generally used to move suspects to secondary screening and does not appear to have been enough in and of itself to have justified a search.[69] The officer's experience in using a profile appears to be a factor in upholding its legitimacy in developing a reasonable suspicion to search someone.[70] In addition to illustrating the importance of the officer's experience in developing reasonable suspicion, *United States v. Moreno* illustrated the types of factors that taken together can support reasonable suspicion. In this case, the Fifth Circuit found several facts that, taken together, constituted reasonable suspicion and justified investigating the defendant's behavior. These facts included the following: (1) the defendant appeared

[63] Ibid., 5–7.

[64] Ibid., 7.

[65] ACLU/ACLU Foundation of Massachusetts, *Racial Justice Report* (ACLU, June 2005), p. 3. www.aclu-mass.org/pdf/RacialJustice.pdf. "ACLU of Massachusetts Challenges Use of Behavioral Profiling at Logan Airport" (ACLU press release, November 10, 2004). www.aclu.org/safefree/general/18765prs20041110.html.

[66] The term "reasonable suspicion" came to prominence in Terry v. Ohio, 392 U.S. 1 (1968), in which the Supreme Court held that a police officer could stop and search a suspect for weapons to ensure the safety of the officer and nearby civilians, and that the basis need not rise to the level of probable cause, but could rest on "the specific reasonable inferences which [the officer] is entitled to draw from the facts in light of his experience." *Id.* at 27. The Supreme Court subsequently acknowledged that "[a]rticulating precisely what 'reasonable suspicion' and 'probable cause' mean is not possible. They are commonsense, nontechnical conceptions that deal with the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Ornelas v. United States, 517 U.S. 690 (1996) (Internal quotes and citations omitted). Nonetheless, the Court went on to explain that reasonable suspicion is "simply . . . a particularized and objective basis for suspecting the person stopped of criminal activity." (Internal quotes and citations omitted). *Id.* The Court then went on to state that "[t]he principal components of a determination of reasonable suspicion or probable cause will be the events which occurred leading up to the stop or search, and then the decision whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to reasonable suspicion or to probable cause." *Id.*

[67] *E.g.*, United States v. Skipwith, 482 F.2d 1272, 1274–75 (5th Cir. 1973). See also United States v. Lopez-Pages, 767 F.2d 776, 778 (11th Cir. 1985) (upholding Eastern Airlines' use of behavioral profile for searching passengers).

[68] United States v. Lopez-Pages, 767 F.2d 776, 778 (11th Cir. 1985).

[69] *E.g.*, United States v. Bell, 464 F.2d 667, 672 (2d Cir. 1972) (The fact that the passenger met FAA's profile of potential hijacker was found to be a legitimate factor in developing a reasonable suspicion that there was cause to stop and frisk passenger), *cert. denied*, 409 U.S. 991; United States v. Lopez, 328 F. Supp. 1077 (EDNY 1971) (upheld *Terry*-type frisk of individual at airport boarding gate on grounds of matching hijacker profile and activating magnetometer).

[70] See United States v. Moreno, 475 F.2d 44, 50 (5th Cir. 1973).

to be nervous, as observed by an experienced anti-piracy officer; (2) the defendant had flown into San Antonio, taken a taxi to a downtown bus station, and returned to the airport 2 hours later; (3) the defendant had changed waiting lines and then purchased a ticket from a different airline; and (4) the defendant had a prominent bulge in his overcoat. Upon investigation, the officer determined that the suspect lied to him about his whereabouts while visiting San Antonio, which further supported the finding of reasonable suspicion.[71]

In the context of drug-courier profiles, the Supreme Court has held that the fact that the articulated facts supporting an officer's reasonable suspicion are consistent with the description in a drug courier profile does not detract from their evidentiary value.[72] The Supreme Court has also upheld a detention based on the reasonable suspicion that the defendant met the profile of an alimentary canal balloon smuggler.[73]

In the context of illegal immigration, the Supreme Court has upheld racial profiling to help develop reasonable suspicion by United States Border Patrol agents making stops along the United States–Mexico border.[74] The fact that the agents were policing the border was integral to the Court's determination.[75] While Mexican ancestry was deemed a relevant factor in developing reasonable suspicion of illegal immigration, it was not deemed sufficient as the sole factor.[76] The officers' experience in enforcing immigration laws was arguably a factor in the Court's finding on this point.[77] The Court subsequently approved the use of ethnic classifications as one factor in deciding which cars to refer to a secondary fixed checkpoint, stating "even if it be assumed that such referrals are made largely on the basis of apparent Mexican ancestry, we perceive no constitutional violation."[78]

Use of Racial/Ethnic Criteria. The Supreme Court has held that it will decide challenges to searches motivated by race under the Fourteenth, rather than the Fourth Amendment. Any such searches will be subject to strict scrutiny.[79] Lower courts have come to different decisions depending on whether racial identity is the sole factor in developing reasonable suspicion or one of several factors.[80] In some states, any program that is challenged for employing racial profiling will also be subject to challenge as violating state law, as a number of states have either outlawed racial profiling by statute or have invalidated pretextual stops involving racial profiling.[81]

Consent.[82] One possible rationale for questioning and inspecting passengers is consent. The Supreme Court has held that the voluntariness of consent to search is a question of fact to be determined from "the totality of all the circumstances," and that knowledge of the right to refuse consent is merely one factor to consider.[83] Therefore, although the government does have the burden of establishing that consent to a search was voluntary, it need not, in order to meet that burden, establish that the person searched knew that he had the right to refuse the search.[84] In order to give valid consent, however, the situation must be such that a reasonable person would feel free to leave.[85] Some states have increased the burden of proof of establishing consent beyond that required by the Supreme Court. New Jersey, for example, has held that the subject of a search must know of the right to refuse in order for consent to be voluntary.[86]

Request for Identification. Police are free to ask any passenger for identification.[87] The critical issue is the point at which the passenger can no longer refuse to provide the identification. The Supreme Court has long held that a "stop and identify" statute is unconstitutional when the initial stop is not based on "specific, objective facts establishing reasonable suspicion to believe the suspect was involved in criminal activity."[88] In addition, "stop and identify" statutes that do not provide a clear standard for determining what a suspect must do to comply are unconstitutional.[89] The Court has held, however, that a statute requiring the subject of a valid *Terry* stop to provide his or her name is constitutional. Of potential significance in the context of requiring identification as part of behavioral assessment, the Court noted that the Nevada statute at issue in *Hiibel* "does not require a suspect to give the officer a driver's license or any other docu-

---

[71] United States v. Moreno, 475 F.2d 44 (5th Cir. 1973), *cert. denied*, 414 U.S. 840 (1973).

[72] United States v. Sokolow, 490 U.S. 1, 7 (1989). Justice Brennan, dissenting, argued that "[r]eflexive reliance on a profile of drug courier characteristics runs a far greater risk than does ordinary, case-by-case police work of subjecting innocent individuals to unwarranted police harassment and detention." *Id*. at 13.

[73] United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

[74] United States v. Brignoni-Ponce, 422 U.S. 873 (1975).

[75] S. M. Haines, "Comment: Rounding Up the Usual Suspects: The Rights of Arab Detainees in a Post-September 11 World," *Arkansas Law Review 57*, no. 146, (2004): 122.

[76] United States v. Brignoni-Ponce, 422 U.S. 873, 885–86 (1975).

[77] Haines, "Comment: Rounding Up the Usual Suspects," 123.

[78] United States v. Martinez-Fuerte, 428 U.S. 543, 563 (1976) (footnote omitted). Justice Brennan, dissenting, stated: "Today we are told that secondary referrals may be based on criteria that would not sustain a roving-patrol stop, and specifically that such referrals may be based largely on Mexican ancestry.... That law in this country should tolerate use of one's ancestry as probative of possible criminal conduct is repugnant under any circumstances." 428 U.S. 571, n.1.

[79] *Whren v. United States*, 517 U.S. 806 (1996).

[80] *Cf. United States v. Weaver*, 966 F.2d 391 (8th Cir. 1992) (officer had grounds for reasonable suspicion, only one of which was racial identity: no Fourth Amendment violation) and *Gonzalez-Rivera v. INS*, 22 F.3d 1441, 1448 (9th Cir. 1994) (racial identity was sole factor, unconstitutional).

[81] See Waite, *TCRP Legal Research Digest* 22, 18–20.

[82] For a more detailed discussion of consent cases, see Waite, *TCRP Legal Research Digest 22*, 16–18.

[83] Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973).

[84] 412 U.S. 248–49.

[85] Florida v. Royer, 460 U.S. 491, 502 (1983).

[86] State v. Johnson, 346 A.2d 66, 68 (N.J. 1975).

[87] *See* INS v. Delgado, 466 U.S. 210, 216 (1984).

[88] Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 124 S. Ct. 2451, 2457 (2004), citing Brown v. Texas, 443 U.S. 47, 52 (1979).

[89] Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 124 S. Ct. 2451, 2457 (2004), citing Kolender v. Lawson, 461 U.S. 352 (1983).

ment."[90] The Court noted that police discretion to arrest is limited in that in order to arrest the request for identification must be "reasonably related to the circumstances justifying the stop."[91] Individual state constitutions may place greater restrictions on the right of police to request identification than does the Fourth Amendment.

Questioning about Destination, Travel Plans, and Related Information. The Fourth Amendment is not relevant if an official merely approaches an individual on the street or in another public place and asks if he or she is willing to answer some questions.[92] When, however, there is some constraint on the individual's liberty, Fourth Amendment requirements come into play.[93] Thus, in order to detain a person to question him or her, or because he or she has refused to be questioned, the police should have a reasonable suspicion that the person is involved in criminal activity. A refusal to answer questions should not be the sole basis of reasonable suspicion. Individual state constitutions may place greater restrictions on the right of police to question passengers than does the Fourth Amendment.

In summary, factors that may enter into evaluating the reasonableness of the officer's suspicion include whether the criteria are subjective or objective, the amount of discretion exercised by the officers conducting the assessments, and the amount of training/experience of the officers conducting the assessments.

The specific issues posed by particular behavioral assessment programs will depend in part on aspects of the protocol such as the following:

- The **purpose** of the behavioral assessment (e.g., deterrence, detection, or back-up for other inspectors);
- Whether the behavioral assessment includes **objective indicators**, such as interest in operational details, or relies solely on **subjective indicators**, such as appearing nervous;
- The amount of **discretion** afforded the inspecting officer;
- Whether a person who declines to provide information will be detained, will be asked to leave the system, or will have no further **action taken**;
- Whether the protocol includes **questions designed to confirm or dispel suspicion** before further actions are taken;
- Whether the behavioral assessment will be used to move passengers who reach a certain threshold to **secondary screening**; and
- The **location** in the system where the behavioral assessment is conducted—on arriving passengers, departing passengers, or both.

The effect of each aspect of the protocol listed above on the risk that a court may find the protocol invalid is as follows:

- **Purpose.** The reasonableness of the protocol will be affected by the relation between the articulated purpose and elements of deployment such as location of assessments and treatment of questioned passengers. For example, if the purpose is deterrence, the existence, but not the operational details, of the program should be made public.
- **Indicators.** The more subjective the indicators, the more vulnerable the protocol is to challenges of unreasonable vagueness, abuse of discretion by the inspecting officer, and racial profiling. Having multiple indicators may mitigate legal risk. Use of racial/ethnic characteristics as an indicator may be illegal in some states. Even where racial/ethnic profiling is not per se illegal, using such characteristics as the sole indicator may increase the risk that a court will find the protocol unconstitutional.
- **Discretion.** Unlike random inspections, behavioral assessments require a modicum of discretion on the part of the inspecting officer. Nonetheless, the greater the inspecting officer's discretion, the more vulnerable the protocol is to challenges of unreasonable vagueness, abuse of discretion by the inspecting officer, and racial profiling. Adequate training is key to mitigating the risk of legal challenges based on exercise of discretion.
- **Action taken.** Actions taken based on behavioral assessment should have a reasonable relation to the purpose of the assessments. If, for example, the purpose is deterrence, following passengers out of the station may be inconsistent with that purpose.
- **Confirming/dispelling questions.** Requiring the officer to ask questions to confirm or dispel reasonable suspicion should lessen the risk that a court will find the protocol unconstitutional.
- **Secondary screening.** Employing secondary screening, particularly objectively based methods such a trace/bulk detection equipment, should lessen the risk of legal challenge.
- **Location.** The location of behavioral assessments in the transit system should be reasonably related to the purpose of conducting the assessments. The location of assessments may affect how courts view the reasonableness of the procedures in cases involving either arriving or departing passengers.

---

[90] Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 124 S. Ct. 2451, 2457 (2004).

[91] Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 124 S. Ct. 2451, 2459 (2004). Justices Breyer, Souter, and Ginsburg dissented, arguing that the police are free to question a *Terry* detainee to try to dispel suspicions, but that the detainee cannot be obliged to respond. *Id*. at 2465.

[92] Fla. v. Royer, 460 U.S. 491, 497 (1983). See also Fla. v. Bostick, 501 U.S. 429 (1991).

[93] United States v. Mendenhall, 446 U.S. 544, 554 (1980). Some courts have required that (1) there be a show of authority by police such that a reasonable person in the surrounding circumstances would not believe he was free to leave and (2) that the person yield or acquiesce to that show of authority. *E.g.* Cal. v. Hodari D., 499 U.S. 621, 624–29 (1991); United States v. Santamaria-Hernandez, 968 F.2d 980, 983 (9th Cir. 1992).

CHAPTER 3

Transit Agency Interviews

Transit agencies of various sizes have been implementing a range of security measures to protect their transit systems. All larger agencies and multimodal agencies interviewed for this research had some type of inspection program in place. There was only one smaller multimodal agency that did not have a PSI program. All interviewed ferry operators and agencies providing ferry service had implemented a PSI program according to mandated federal maritime security regulations. The most prevalent PSI method was the use of canines. With the inception of TSA's program to encourage canine use for PSIs, agencies have been acquiring canines capable of detecting explosives and providing TSA-sponsored training and other related training to relevant staff. Other PSI methods included manual and electronic searches, visual inspections, and behavioral assessments.

Currently, the primary focus of PSI programs in terms of threats has been explosives because explosives have been the weapon of choice in many transit attacks. Placed in significant amounts in contained locations where large numbers of passengers are present, explosives have the ability to cause severe damage to people and property as well as inflict economic loss. Agencies, however, are cognizant of other threats as well—such as chemical, biological, and nuclear threats—and have implemented or are planning to implement appropriate countermeasures.

Interviews with transit agencies showed that large agencies, small agencies, and agencies located in different geographic regions differ in their perceptions of terrorist risk and differ as well in whether and how they implemented PSIs. With the exception of ferry operators, PSI implementation and method were related to customer perception of terrorist risk. The reason for the exception is that ferry operators are governed by maritime security regulations and are expected to have implemented specific PSI procedures. In terms of vulnerability based on mode, rail modes were believed to be more vulnerable than bus modes, and ferries carrying vehicles were considered more vulnerable than ferries carrying passengers only.

While pilot testing at a PATH station in New Jersey demonstrated the operational feasibility of airport type detection equipment, it also revealed high operational costs, including the intensive personnel and training requirements of the system and the relatively high space needs for the system. During the PATH test, commuters heading to work in Manhattan were required to walk through metal detectors and feed their bags into X-ray machines. Furthermore, all interviewees except one ferry operator stated that it would be infeasible for them to implement an airport-style screening system because of operational feasibility concerns and financial constraints. Agencies that operated as open systems would be required to construct a barrier, which could be costly. The need for increased security personnel to operate the equipment and perform secondary screenings and the need for training were considered to be just as substantial as the unit acquisition and ongoing maintenance costs. Constitutional and liability issues and impact on the agency's image were other concerns cited by the agencies.

In terms of security measures other than PSIs, practically all agencies use roving patrols and security presence to enhance safety and security. Agencies have also been using canine units to detect nonexplosives such as weapons and narcotics. Systems operating on the honor system routinely conduct passenger fare inspections, which allow security personnel to observe passengers and make the presence of security personnel known. Many agencies have also implemented antiterrorism hotlines and performed significant customer education and outreach activities.

Security technologies to protect transit property and provide surveillance within transit vehicles have also been installed at many agencies. These security technologies include access control systems to control centers, railyards, bus depots, and other facilities, as well as video surveillance via CCTV. The largest agencies have been testing and installing chemical, biological, radiological, nuclear, and explosives (CBRNE) detection equipment and intelligent video systems. They also have specialized hazardous material (HazMat)

teams and special operations teams focusing on specific threats. Interoperable communications and hotlines from control centers to local emergency responders have also been deployed by some agencies.

Specific technologies for buses include CCTVs, two-way radios connecting bus operator to the control center, silent alarms, and automatic vehicle location (AVL) technology. Specific technologies for rail include call boxes along tracks; public address systems; intercoms on trains and platforms with which passengers can call station managers; intercoms on trains with which passengers can call rail operators; two-way radios connecting train operators to the control center; and automated, electronic, fire protection systems in stations and tunnels.

Perception of Terrorist Risk

There is a marked difference in perception of terrorist risk between East Coast transit agencies and transit agencies in the rest of the United States. More specifically, transit customers in metropolitan regions affected by the attacks of September 11, 2001, were much more aware of their transit system's vulnerability and perceived higher risk levels than transit customers did in other regions. Transit customers in metropolitan regions affected by the attacks of September 11, 2001, were also more tolerant of security measures, including those that cause delay and inconvenience.

At most smaller agencies, agency management perceived the system to be at higher risk of terrorist attack than their customers did. In fact, the only service areas in which customers were perceived by transit officials to be as concerned about terrorism as agency management were the metropolitan areas affected by the attacks of September 11, 2001.[94] Generally, customers in smaller service areas were not demanding security-related improvements to reduce the threat of terrorism and were more concerned with routine acts of crime and lawlessness. According to transit officials interviewed, these customers would not be tolerant of security-related delays or inconveniences to reduce the threat of terrorism. These results may be due to the fact that customers of small transit agencies are more likely to encounter (or to have already encountered) routine acts of crime and lawlessness than they are to encounter random acts of terrorism. One transit system respondent believed that if a terrorist strike were to occur on the system, this tolerance level would likely increase.

[94] Author interviews with MTA–NYCT personnel. (Michael Lombardi, Senior Vice President/Department of Subways; John Jimerson, Chief, Division of Security/Department of Subways; Joseph Nugent, Interagency Counterterrorism Liaison); MTA Metro-North interviewee (Sean McLaughlin, Assistant Deputy Chief). MTA–NYCT, Department of Subways, New York, NY, November 2005; Metropolitan Transportation Authority Police Department, New York, NY, November 2005.

The only service area where customers were perceived to be as concerned about terrorism as they were about crime was the New York City metropolitan area. This was due to several factors: the significant decrease in crime rates in the past decade; the significant increase in the threat of terrorism with the September 11, 2001, attack on the World Trade Center; and the war in Iraq.

The mentality of transit customers living on the East Coast appears to be different than the mentality of transit customers on the West Coast and in other parts of the nation, and it is most likely that this is the case because the tragic events of September 11, 2001, involved three East Coast cities—New York, Washington, D.C., and Boston.

Transit labor organizations for all agencies (large, mid-size, and small) have been requesting increased security and related training for their members. The financial and other constraints faced by transit agencies make it difficult for them to provide intensive training to all of their frontline workers. The training, even if it were provided on site by FTA-sponsored programs such as the National Transit Institute, would also need to follow the strict contract guidelines in place at many agencies. If workers are provided training in addition to their normal work hours, they would likely be eligible for, and would receive, overtime pay. If workers attend training courses during their normal work hours, substitute workers would be needed to continue transit operations. Smaller agencies may need to send their workers to offsite training and would incur the workers' travel expenses as well.

For larger systems, security sweeps and the visible presence of officers increase passenger perception of security and safety. Agencies serving large metropolitan areas receive few or no complaints about the presence of officers and use of canines. In fact, they often receive accolades from passengers.

Perception of Risk by Mode

Bus

The perception of transit personnel that buses are less vulnerable than other modes is likely due to the presence of a bus operator on every bus transit vehicle. Bus operators are seen to be an important first line of defense against terrorism. Most bus operators have access to silent alarms and radio communications with a central command center, providing ready access to law enforcement. Also, bus operators are trained to spot suspicious packages and devices inside and underneath the vehicle.

Subway and Commuter Rail

Subway and commuter rail systems are viewed as being more vulnerable to terrorism than buses because of the large numbers of passengers carried by the systems. There are more

locations in subway and commuter rail systems in which explosives or other threat items may be hidden. Also, in the absence of PSIs, passengers may board trains without being seen by transit staff or security personnel. Because of the higher vulnerability to attack of subway and commuter rail systems, PSI programs have primarily been focused on these modes. However, there is a key difference between commuter rail and the modes of subway and bus: if a passenger leaves an item behind in a subway or bus, other passengers usually alert the passenger. If several items are left behind by various passengers, passengers will most likely report the incident to transit personnel or police. On commuter rail, passengers typically place their belongings on a baggage rack near their seat. However, if they happen to walk toward the food car or exit the train, it is unlikely that rail passengers would notice.

Light Rail

Because many light rail systems are open systems with no fixed entry points, interviewed agencies tended to use canines if there was a PSI program in place. Bag inspections or PSI programs using airport equipment were seen by interviewed agencies to be operationally infeasible because of the open architecture of the systems. Also, according to transit officials interviewed, the perception of vulnerability was lower on light rail systems than on subway or commuter rail systems.

Ferry

Ferries carrying vehicles are viewed as more vulnerable to attack than passenger-only ferries. This is because vehicle-borne explosives could do more damage to a ferry than a suicide bomber. It is interesting to note that the maritime industry, including ferry operators, is governed by many more security and safety regulations than other surface modes. These regulations include PSI requirements which are directly linked to the maritime security (MARSEC) threat level determined by the U.S. Coast Guard.

Inspection Policy and Protocol

Most transit agencies that perform PSIs have formal, written inspection policy and protocols. Many of these documents, which may be embedded within Standard Operating Procedures (SOPs), are developed within, or in close coordination with, internal or external law enforcement agencies. These documents contain detailed information about the goals and objectives of the PSIs, primary and secondary inspection methodologies, determination of inspection locations, passenger selection criteria, and other sensitive information. They are therefore classified and cannot be released to the public.

Objectives

The primary stated objectives of PSIs are deterrence and detection, with the understanding that while 100% detection is never possible, a lower level of detection is possible, and well-functioning inspection programs provide a strong deterrent to terrorism. A secondary objective, or derived benefit, from PSI programs is enhancing customer perception of security on the system and improving the image of the agency. Interviewees that had implemented PSI programs stated that the random nature of their inspection programs contributes significantly to their success. At the same time, much of the inspection effort is concentrated in peak periods on weekdays—the systems' highest ridership periods—when the consequences of an attack in terms of damage to human life would be highest.

Precipitating Events

The precipitating events in the New York/New Jersey metropolitan area for the establishment of inspection programs were the bombings of the London Underground (2005) and the Madrid commuter rail attack (2004). The inspection programs were initiated by area agencies immediately after the second London bombing in July of 2005. The manual inspection program began at that time, and electronic equipment to assist in the PSI process was acquired and implemented in November 2005. The rapid implementation of the programs by the New York/New Jersey metropolitan area transit agencies was the result of the successful comprehensive interagency security planning that had been taking place since the attacks of September 11, 2001.

For Boston's MBTA, the precipitating event was the Democratic National Convention (DNC) in June 2004. Approximately 100,000 inspections were performed during the DNC; however, MBTA's PSI program was suspended until recently. In July 2004, a temporary restraining order was sought against the agency but not issued. There was a suit to enjoin the performance of baggage inspections during the DNC; however, the request for injunctive relief was narrowed to cover the implementation of the policy requiring 100% inspection of bags at selected stations pursuant to the federal designation of the DNC as a National Security Event.

It was announced on October 6, 2006, that the MBTA's PSI program would resume systemwide on subways, buses, boats, and commuter rails. The continuation of MBTA's PSI program was based on the attacks in New York and Washington, D.C., on September 11, 2001, and the more recent Madrid and London transit attacks. The threshold for conducting inspections and changes to the inspection method are based primarily on specific intelligence.

For the canine PSI programs, there was no clear precipitating event common to all agencies, although some indicated

that the Madrid and London incidents did factor into their decisions. Two of the four canine-only PSI programs were very new: one had just started in January 2006, and the other was in the process of implementation and would not begin until late 2007. The other two canine-only PSI programs were expansions of existing narcotics-detection canine units; explosives detection capability was added by these agencies in 2000 and 2002.

Items to Be Inspected

Although PSIs are termed "bag" inspections or searches, other objects of interest may also be inspected. For bag inspections using manual, trace detection, and canine methods, any backpack, briefcase, suitcase, shopping bag, handbag, fanny pack, or similar container reasonably capable of concealing a device or substance that could reasonably be used as a weapon to kill or injure victims may be inspected.

Prohibited Items

Typically, transit agencies will have in place a list of prohibited items. These lists are relatively similar and include the obvious—weapons and explosives. If other contraband is found during the PSI process, the passenger will be subject to further inspection and/or arrest.

Changes to inspection protocols and methods are generally determined at the command level, although some agencies provide more discretion to inspecting officers than others.

Agencies have expressed the intention to communicate their inspection policy to customers before the inception of the program, although many agencies did not have an established inspection notice or pre-implementation communications procedure. Once an inspection program begins, agencies communicate this to passengers by posting appropriate notices and making announcements. Some agencies have indicated the importance of keeping certain information regarding PSIs confidential, including specific schedules of inspection days, times, and locations.

For canine walk-through inspections, if the canine indicates the presence of an explosive, the officer can search the passenger and his or her baggage under exigent emergency circumstances. Note that canine units are virtually always segregated into explosives units and other units, including drug units. Dogs are rarely, if ever, cross-trained to detect both explosives and drugs because of the legal problems that can result. A drug canine "hit" serves solely as probable cause for further inspection.

In general, the agencies interviewed were planning to continue the inspections programs that were under way indefinitely. Some of the canine programs were expected to expand.

Procedure for Manual and Explosives Trace Detector Bag Inspections

PSIs are usually performed by agencies on all days during both peak and off-peak periods; however, PSIs are more focused and more personnel are provided on weekdays during peak periods when passenger volumes are the highest. To increase their deterrence effect, the PSIs occur at random locations at various times. Inspection intensity and methodology are directly linked to intelligence but not necessarily to publicized threat levels (unlike the case for ferry operators).

Passenger baggage inspections are performed by transit or police officers near turnstiles. At one agency, all choke points for a selected station have a checkpoint. Therefore, for that agency, stations with multiple entrances require multiple checkpoints. Transit or police officers are also able to perform primary inspections. Passengers are selected randomly (e.g., every eighth passenger carrying an item of interest) to avoid the appearance of racial profiling. The item to be inspected is determined by current intelligence. For example, at one point, strollers were thought to be used by attackers, so strollers were targeted for inspection. The inspections may be performed manually or electronically. While inspection protocol is nondiscretionary and changes to the protocol are usually determined at the command level, needed changes can be implemented almost instantaneously. For instance, at two of the agencies, the Chief of Police or another command supervisor has the discretion to modify inspection procedures on the basis of passenger flow. Modifications include setting up a separate "no baggage" security checkpoint for passengers who are not carrying baggage if passenger queues become too long.

At some agencies, if contraband is found during the inspection, the passenger will be arrested. Also, passengers who appear to enter the station inspection area but immediately exit the area on viewing the inspection checkpoint may be questioned and could be followed. At one agency, however, officers are advised that security inspections are limited and will not be used to gather evidence for criminal prosecutions or otherwise to enforce ordinary criminal laws.

One multimodal agency conducting PSIs considers any passenger in line to proceed through a checkpoint who reaches the selection point to have implied consent to an administrative security inspection. Further, passengers in line to proceed through a checkpoint who reach the selection point are considered to have no right to refuse inspection of any of their baggage in the event that they are randomly selected. According to this policy, unless and until a passenger in line to proceed through a checkpoint reaches the selection point, the passenger has the right to avoid having his or her baggage subjected to the PSI. Before reaching the

selection point, the passenger may elect to get out of line; importantly, a passenger's decision to exercise this right cannot be used as a legal basis for "reasonable suspicion" that the person may be carrying an item that could be used as a weapon on the mass transit system or is otherwise engaged in criminal activity.

Agencies conducting PSIs minimize the degree of privacy intrusion and avoid, to the greatest extent practicable, revealing the contents of baggage to other members of the public. For instance, officers are not permitted to read or scrutinize the contents of any documents, writing, or photographs.

For both manual and electronic inspections, one supervisor and a minimum of three officers are necessary at each checkpoint. One officer is the counter and is responsible for the passenger selection process. Another officer explains the inspection process to the selected passenger. The passenger is then asked to place his or her bag on the table and to step away from the bag (so that they cannot reach in and detonate an explosive). The third officer inspects the bag. While the officer inspects the bag, the passenger may not touch the bag. The remaining officers and, at some agencies, BASS-trained plainclothes officers, watch the inspection officers to ensure their safety. The supervisor is there to resolve concerns or any problems that might arise. To conduct secondary inspections at some of the agencies, a canine team may be present during the PSIs.

Electronic Equipment

Accuracy, costs, and specificity of the information provided to officers (e.g., substance detected) are the most important criteria in the equipment selection process, according to two of the agencies interviewed. The electronic trace detection units being used for the PSIs include portable trace detectors and a larger unit requiring power—a desktop trace detector. During the inception period of the electronic equipment, one of the interviewed agencies determined that the false positive rate was higher than desired, so the threshold was adjusted to alleviate the problem.

One of the agencies conducting PSIs has a target average inspection time of 30 seconds. Another agency reports that its typical inspection time averages 8 to15 seconds per passenger and that no passenger has missed a train because of the PSI. At another agency, the average time for manual baggage inspections is less than 1 minute, and the average time for electronic baggage inspections is less than 30 seconds. As stated earlier, these delays are generally accepted by passengers, and the increased security measures are welcomed by most transit customers.

In addition to their use during PSIs, the electronic detection units are used to screen unattended baggage and checked baggage at the Greyhound or Amtrak baggage storage areas at some locations. In addition, one agency issues portable units to certified canine teams. The canine team is used first; if the canine does not detect explosives, the inspections team may opt to use a portable trace detector as a means of double-checking the accuracy of the negative canine alert.

Use of Canine Units for PSIs

A multimodal agency conducting PSIs at station entrances has eight canine units with explosives detection capability. Each unit also has explosives trace detection equipment for supplemental screening. The explosives detection canine units have gone through intensive training, but have not gone through the TSA program. The canine units are used to provide primary or secondary detection during PSIs. They are also used to check unattended baggage or checked baggage in storage areas. Other agencies also use canines as a secondary inspection method.

Customer Notice of PSI Program

For the bag inspection PSI programs, notice to passengers is provided by signage at the inspection checkpoints. Prior to the inception of inspections in most PSI programs (including canine programs), a press release, news conference, and other communications have usually been provided to the public. However, agencies note the importance of keeping the exact locations and times of the inspections confidential.

PSI Measures of Effectiveness

The avoidance of terrorist incidents is the primary measure of program effectiveness, according to transit agency interviewees. Ideally, both deterrence and detection ought to be measured to evaluate the performance of PSI programs. However, although measuring the number of deterred attacks would be a good indicator of the deterrent level of a PSI method, this is impossible to do. Threat detection rates, on the other hand, can be determined via covert tests using simulants.

The number of ordinary contraband items seized as the result of inspections activity is not relevant for purposes of PSI program evaluation. Other measures (e.g., the number of passengers inspected) are also used to determine the effectiveness of specific checkpoint officers.

The number or percentage of inspections may be considered an output measure. Two agencies stated that they keep detailed PSI records (e.g., time, date, inspection intervals, type, number of inspections, characteristics of selected passengers such as ethnicity and age, and the number of refusals).

One agency is developing a security survey to capture customer perception of security and security-related activities. The agency believes that the results of such surveys can be used as measures of effectiveness.

Officers must be able to communicate effectively with passengers and be temperamentally suited for the program. Another agency emphasized the importance of having the right officers involved in the PSI program and related that sergeants in charge of each checkpoint are carefully selected. Officers must also successfully participate in pilot runs before they are deployed in the program. Also, one of the agencies provides translation services to officers conducting PSIs, when needed.

Legal Issues Related to PSIs

All agencies performing or planning to perform PSIs stated that they were not immune to liability under state or local laws, with the exception of one agency that maintains sovereign immunity against lawsuits although its police officers may be subject to individual suits.

Interviewed agencies had considered the full range of constitutional and tort issues, including invasion of privacy, injury/health effects, canine searches, and failure to exercise the required level of care in formulating PSI program policy objectives and methodology and in implementing the PSI program. A large commuter rail agency has indicated that their primary legal concern was constitutional, although tort issues were also considered. One of the larger multimodal agencies stated that their legal issues of concern were primarily constitutional, particularly Article 12 of their state constitution.

Only one agency, located in the western United States, indicated that they had not taken legal issues into account when establishing their canine PSI program (which currently consists of only one canine team). The main issues of concern for this agency were the cost and type of dogs selected for the program and the avoidance of racial profiling.

For reasons of liability and to avoid any allegations of racial profiling, agencies performing bag inspections generally prefer either to inspect all passengers entering a particular station or to perform inspections based on a random number criterion. There were no non-ferry transit systems in which PSIs for all passengers were implemented, except on a trial basis (TSA testing of detection equipment at PATH's Exchange Place station, TSA TRIP testing of detection equipment on a commuter rail car, and TSA testing of detection equipment at ferry terminals).

Only two agencies that had implemented bag inspections had experienced lawsuits from civil rights/advocacy groups, and these lawsuits have been dismissed. No lawsuits have been brought against the other interviewed transit agencies conducting PSI programs.

Impact of PSI Programs on Agency Image and Customer Satisfaction

In general, transit customers were pleased to see an increased presence of transit security personnel and increased security measures, including PSI programs. While the interviewees indicated that it is difficult to determine the impact the inspection programs have on ridership levels, the PSI bag inspection and canine inspection programs in major metropolitan areas had been receiving positive feedback from transit customers across the board. Improvements had been seen in customers' image of the agency, customer perception of security, and customer satisfaction. None of the interviewees indicated problems with customer anxiety regarding increased officer presence or presence of canine units.

Training

Basic Security Training

Agencies are striving to balance the need to provide adequate security training to frontline workers with agency resource constraints. Extensive training for employees under contract rules can be prohibitive in terms of cost, even if the training itself is freely available. Most transit employees attend basic security awareness training that is provided by, or that uses materials provided by, the National Transit Institute (NTI). Also, most agencies operating subway or rail systems have provided evacuation procedures training to their operational staff. Agencies are also providing training in the mandated National Incident Management System (NIMS) to give incident command and control information to employees. Larger agencies are also providing targeted training to specific workers needing specialized training. Targeted training includes antiterrorism training, strategies to respond to terrorist attacks, vendor training, and HazMat training.

The training that is provided by transit police and contractors to operational and support employees includes the following:

- Counterterrorism Training,
- Strategies to Respond to Terrorist Attacks,
- NIMS and Incident Command System (ICS) courses provided by the Federal Emergency Management Agency (FEMA),
- System Security Awareness, and
- Community Emergency Response Team Training.

Canine Training

Canine training is provided to canine handlers at transit agencies through a variety of sources. The sources of training include TSA, FAA, the transit agency itself, contractors, local airports, and local law enforcement. There was a general consensus among interviewed agencies that TSA training needs to be supplemented by training that familiarizes the canine with transit systems in general and the specific system

the canine will be operating in. Agencies are required to have some type of certification (e.g., TSA, United States Police Canine Association [USPCA], or FAA) to use canine teams.

Search and Seizure Training

Transit officers conducting PSIs typically receive specialized "search and seizure" training. Some agencies have also provided additional customer relations and community policing training to officers involved in the PSI programs.

BASS

While practically all agencies have strict policies against racial profiling, some agencies have been conducting or planning to conduct behavioral profiling training. One hundred forty Massachusetts state troopers have been trained in BASS and have used it to observe and screen travelers as they patrol Boston's Logan Airport terminals. Boston's Logan Airport, the first U.S. airport to start using the BASS technique, implemented the program soon after the attacks of September 11, 2001. SPOT, a federal program based on behavior profiling, was initiated in 2003 and is being introduced at airports nationwide. Israel has had great success with BASS at airports and shopping malls, despite the high number of suicide bombers attempting to attack these facilities. Unlike U.S. workers, Israeli guards have received intensive training and go through a tough selection procedure. However, the SPOT program is still expected to significantly enhance security at U.S. airports.[95]

In addition to basic security-related training, covert testing and assessment of inspection staff are conducted by some agencies.

Agencies Not Planning to Conduct PSIs

Smaller interviewed agencies indicated that they would need funding from federal or other sources to consider the implementation of PSIs because they perceive that the risk of terrorism for their systems is relatively low. One agency stated that they would not implement a PSI program even if they received government funding because such a program is too risky in terms of privacy and civil rights–related issues.

It is interesting to note that smaller transit agencies were either nonresponsive or chose not to participate in this research. On the basis of this, it can be inferred that many of the smaller agencies are not conducting, or planning to implement, PSI programs.

Of the two agencies interviewed that are not conducting PSIs, the smaller agency operates only one mode—bus—and the larger one operates three modes—bus, light rail, and subway. The larger agency has gone through a risk assessment process and has implemented security measures such as access control, video surveillance, roving patrols, canine units (other than explosives detection dogs), interagency CCTV monitoring, and a chemical detection system.

The smaller agency has not performed a risk assessment of its system but has implemented security measures, including access control technology, video surveillance, and roving patrols.

Perception of Terrorist Risk

Of the two agencies not conducting PSIs, the larger agency does not believe that the risk of terrorism is low and does believe that many of their terrorism-related security measures can be implemented without specific federal directives requiring them. At the same time, the agency believes that its transit system and operations are already secure and that a good security program need not include PSIs. Therefore, this agency is not considering PSI implementation. In addition, the agency believes that screening passengers would create delays that would be unacceptable to its passengers and that the legal aspects of PSIs are a risk in terms of privacy and civil rights–related issues. Greater financial assistance from the government would cause them to increase their security staff rather than increase their level of passenger screening activities. The agency's customers are more concerned about "routine acts" of crime and lawlessness that impact safety and security than random acts of terrorism. At the same time, passengers might be tolerant of additional security-related delays or inconveniences to reduce the threat of terrorism.

The smaller agency does not, and is not planning to, conduct PSIs. In general, agency management is more concerned about their vulnerability to terrorism than their customers are. Reasons for *not* considering security inspections include the fact that the agency's customers have not expressed concerns about terrorist activity and that screening passengers would create unacceptable delays to transit service.

The smaller agency's customers are not demanding security-related improvements to reduce the threat of terrorism and would not be tolerant of additional security-related delays or inconveniences to reduce the threat of terrorism. Their customers are more concerned about "routine acts" of crime and lawlessness that impact safety and security than random acts of terrorism. The agency wished to stress that it does not consider the risk of an act of terrorism on their system to be low. If funding were available, the agency would add surveillance/video equipment and access control technologies before adding security staff and would consider initiating passenger screening activities.

[95] A. Beshkin, "U.S. Airport Screeners Look for Behaviors" (NewsVOAcom [Voice of America website], October 2, 2006). www.voanews.com/english/archive/2006-10/2006-10-02-voa40.cfm.

Size and Training of Security Force

The total number of security staff at the larger agency not conducting PSIs is 62; 45 of these staff members are transit police officers. The smaller agency has one staff member within its security division and no transit officers. However, the smaller agency receives assistance from the local city police department and community service interns when needed.

The smaller agency has provided NTI terrorism awareness training to all of its employees. The larger agency has provided FTA Transit Watch and NTI terrorism awareness training to its employees.

Security Measures

Technologies

There is a consensus among interviewees that despite the success of the PATH Exchange Place test of airport screening equipment in a transit environment, similar equipment would not be operationally or financially feasible for their systems. Operational issues include limited space in smaller stations, service delays, long queues, open systems needing to build artificial barriers, and lack of a sufficient number of trained personnel. Financial issues include the cost of the required personnel and their training and the equipment purchase and maintenance cost. In addition, constitutional and liability issues (including health concerns about the equipment) were a matter of concern for some interviewees. Agencies not directly affected by the attacks of September 11, 2001, strongly believed that customers would not tolerate the inconveniences and possible delays that would be caused by the screening technologies. These agencies were also concerned about their ability to justify instituting such strong measures when they may not be needed or may not be effective in detecting against certain threats. One interviewee stated that the ideal technology would be one that would screen the environment for all threats without impacting operations.

Security technologies—such as access control systems for control centers, railyards and bus depots, and other facilities, as well as video surveillance (CCTVs) to protect transit property and provide surveillance within transit vehicles—have been installed at many agencies. The largest agencies have been testing and installing CBRNE detection equipment and intelligent video systems. Radiological detection sensors are being developed for use in conjunction with intelligent video. If the sensor detects a threat, it communicates with the camera, which then tracks the source of the radiation. DHS also has a BioWatch program to evaluate biological detection equipment in transit stations. Interoperable communications and hotlines from control centers to local emergency responders have also been deployed by some agencies.

Specific technologies for buses include CCTVs, two-way radios connecting the bus operator to the control center, silent alarms, and AVL technology. Specific technologies for rail include call boxes along tracks, public address systems, passenger to station manager intercoms on trains and platforms, passenger to rail operator intercoms on trains, two-way radios connecting train operators and the control center, and automated electronic fire protection systems in stations and tunnels.

The Integrated Electronic Security System, Command, Communication, and Control (IESS/C3) program is being implemented by one of the largest multimodal agencies in the nation to enhance security throughout its transportation network and to provide incident management response and recovery capabilities. The IESS/C3 program will enhance monitoring, surveillance, access control, intrusion detection, and response capabilities and requires the installation of over 1,000 cameras and 3,000 motion and perimeter sensors. Command, communication, and control centers will be established and integrated into the agency's response and recovery management system and the police department's Mobile Command Center. One of its agencies plans to install cameras to record activity for post-incident analysis in its subway system and is also considering implementing video with real-time transmission capability in its rail cars. Cameras are also being installed on some of the agency's buses.

The agency is also implementing a statewide wireless-network-compatible communications system to improve coverage, promote interoperability, and establish a standardized system for internal and interagency communications. A neighboring state transit agency is implementing satellite communications in key buildings and its police vehicles as a backup system for its wireless network.

Another large multimodal agency has installed cameras within its buses that are capable of transmitting images to police vehicles that have GPS and an AVL system. It is possible to determine the location of each police car and also whether or not it is idling. A similar system is being planned for its interstate buses. Such a system should greatly enhance the response capability of transit police and emergency responders should a bus be hijacked or some other major incident occur. Also, buses that are not following their regular route can be flagged and investigated.

Personnel

Because the mere presence of security personnel acts as a deterrent against terrorism and common crime, many of the larger agencies have stepped up the size of their security forces since the attacks of September 11, 2001. The use of roving patrols to provide widespread presence and coverage is common among all transit agencies, regardless of size. In addition, the importance of frontline supervision should be

noted. In general, frontline supervisors are themselves former frontline workers and also union members, and, thereby, they have substantial influence on the behavior and performance of the frontline workers. Moreover, the supervisors are influenced by what transit management considers important, what the supervisors get feedback on. Transit management must therefore ensure that proper supervision, rewards, and discipline mechanisms are in place, and management must work in close coordination with the unions and their leadership to make certain that security measures have been appropriately implemented. Conflicting messages can easily be received by frontline transit employees because of the multiple and conflicting goals (e.g., on-time performance) being pursued by transit agencies.

Larger agencies use specialized security teams that have received special, targeted training. These teams perform special security activities. The following are descriptions of these security activities and some of the security teams:

- **Passenger fare inspections.** Open transit systems operating on the honor system do not have access control/fare collection methods such as turnstiles. Therefore, transit officers conduct random fare inspection. Their presence, or potential presence, acts as a deterrent.
- **Train order maintenance sweep (TOMS).** TOMS consists of one sergeant with several officers. The sergeant alerts the conductor to the sweep. The officers spread out on the platform, and each officer steps onto a train car and performs a visual sweep of the car. Sweeps take a matter of seconds and do not significantly impact subway operations. A TOMS is used as a security measure for larger subway and rail systems.
- **Atlas teams.** Atlas teams consist of one lieutenant, two sergeants, and sixteen officers. They are sent out to stations based on intelligence and Internet monitoring. High-profile stations are constantly monitored.
- **Critical response vehicles (CRVs).** The CRVs consist of a motorcade of 69+ police vehicles that travel a main thoroughfare. Each police vehicle with a team of two officers breaks off and proceeds to a subway station.
- **Hercules teams.** Hercules teams travel in unmarked vehicles and arrive unannounced at major transit stations, terminals, and transfer points. They exit the vehicle and enter the transit system. They perform train sweeps and may or may not travel to other stations.
- **Aerial surveillance.** A large multimodal agency conducts regular aerial surveillance of its infrastructure including bridges, tunnels, and substations.
- **HazMat team.** One multimodal agency has the largest certified HazMat team in its metropolitan region and trains local responders as backup. Some agencies have similar units with limited HazMat capability.
- **Explosives detection unit.** An explosives detection unit has a response vehicle with enhanced visuals, an X-ray, and robotics. The unit is specifically trained to work within the transit system operating environment. Similar units may focus on screening abandoned/suspicious bags or objects for explosives or other threat materials.

Other Security Measures

Other forms of security measures include the following:

- Explosives detection canine teams and other canine teams,
- Collaboration with local law enforcement and emergency response agencies,
- Employee training and education,
- Customer and community education and outreach, and
- An antiterrorism hotline.

Size of Security Force

Since the attacks of September 11, 2001, transit agencies have been increasing the number of officers and security staff, and some have created a Director of Security position. One of the largest domestic multimodal agencies has increased its officers by 42% since the attacks of September 11, 2001. Some of this multimodal agency's officers have also been assigned to counterterrorism operations. The part of this multimodal agency responsible for subway and bus service has over 400 security staff members and 2,500 dedicated transit officers within the city police department to protect its transit system. In addition, 100 train supervisors and managers have been trained for emergency work, including the operation of trains to transport emergency responders during emergencies. Also, National Guard soldiers have been providing security assistance at major transit hubs under the direct supervision of law enforcement officers. The multimodal agency also has 700 officers assigned to other modes and locations.

Collaboration with Local Law Enforcement, Emergency Responders, and the Community

Close collaboration with local law enforcement is important, especially for agencies with systems covering a large service area. In major incidents, having supplemental resources at hand will increase the response capability of the agency. In an effort to augment their forces in major emergencies, including terrorist attacks, one of the large multimodal transit agencies that serves a large geographic area has been training officers in 560 law enforcement agencies regarding its transit system and emergency response procedures.

The largest multimodal agency in the nation has a strong level of collaboration with the community, keeping it informed of the agency's inspection program and asking customers, through its outreach program, to inform transit police or personnel of any suspicious packages or activity. Another multimodal agency practices community policing by interacting with vendors and other community members within a certain radius of its stations and reminding them to report suspicious activity. Some agencies have also created a hotline to receive tips about suspicious activity from the public.

Immediately following the attacks of September 11, 2001, transit agencies in metropolitan areas began holding interagency discussions and started intensive information- and knowledge-sharing efforts with domestic, international, and federal agencies (DHS, TSA, and FBI, as well as British, French, Japanese, Israeli and other international police authorities). The agencies also developed and are continuing to develop strategies and plans to deal with a wide range of threats and scenarios. Agencies now partake in an Interagency Counterterrorism Task Force (ICTF) responsible for supervising and coordinating emergency drills, training, and intelligence sharing. The ICTF also provides a daily intelligence briefing on transit-related threats and terrorist activities to about 350 transit and security agencies worldwide.

Ferry Systems

The federal government (U.S. Coast Guard and federal legislation) has strictly regulated safety-related elements of ferry operations. The Maritime Transportation Security Act of 2002 has followed the safety model in establishing security-related regulations.

Four ferry systems were interviewed for this research. One is a large, passenger- and vehicle-carrying system on the West Coast of the United States. Three are smaller systems: one passenger-only system, also on the West Coast, and two passenger- and vehicle-carrying ferry systems on the East Coast.

The large system, operating in the northwestern United States, is actually the largest ferry system in the nation, the largest vehicle-carrying ferry system in the world, and the third largest in the nation in terms of passenger trips. Because there have been threats against the system, the agency considers its ferry system to be highly vulnerable and has implemented a vehicle inspection program. The U.S. Coast Guard's Marine Safety and Security Team members escort randomly selected ferries in boats to enforce a 500-yard security zone. The number of escorted ferries is increased when there is a special event. At the same time, the agency does not plan to institute additional security measures unless there are federal directives requiring them. With the many security and safety-related regulations that are now in place, it would be difficult for the agency to justify adding any additional measures. One of the three smaller systems conducts 100% inspection of foot traffic using an airport-style magnetometer (portal) and X-ray of carry-on bags that are supplemented by canines and hand-wands. Also, 100% of commercial vehicle traffic, 100% of recreational vehicle traffic, and 50% of passenger vehicles are inspected under the current MARSEC Level 2.

Perception of Terrorist Risk

As previously mentioned, the large ferry system believes that it is highly vulnerable to terrorist attack. This perception is due to federal reports indicating threats to the ferry system, the size of the system, and the large number of vehicles carried on its ferries. Terminals are located in a large metropolitan area and also in suburban and rural areas. This diversity in terminal location has influenced the views expressed by the agency's customers on the system's vulnerability to attack. According to the agency interviewees, customers who live in the metropolitan area believe that the system is vulnerable to terrorist attack and are more aware of and concerned about terrorism-related matters. Customers living in outlying areas are not as concerned. Also, commuters are more sensitive to the system's vulnerability than tourists and leisure riders. In general, however, ferry operators reported that most of their customers are primarily concerned about reliable ferry service and routine crime and lawlessness; therefore, they would not be tolerant of additional security-related delays or inconveniences to reduce the threat of terrorism.

All three of the small systems are also highly concerned about the threat of terrorism and believe their ferry operations are vulnerable to attack. However, with one exception, their passengers do not express the same concerns about the threat of terrorism.

Vehicle Screening Program (Large Ferry System)

The vehicle screening program at the large ferry system was established in July 2004 in response to regulations implementing the Maritime Transportation Security Act of 2002. The system uses a combination of canines and agency police officers conducting visual inspections to meet the regulatory requirements set forth in 33 CFR Part 104 and Part 105.

The visual inspection involves viewing any visible element of the vehicle. The canine inspection takes a matter of seconds (10 seconds on average) as the explosives detection canine team encircles a vehicle in the screening process. The agency has a written inspection policy, but it is not publicly available. The screening occurs 7 days a week and tends to be focused on peak periods, although screening occurs during all time periods.

Inspection Objective and Protocol

The objective of the vehicle screening is both deterrence and detection. Under the inspection protocol, terminals are randomly selected for screening. For selected terminals, all entering vehicles are screened. Major changes to the screening protocol are made at the command level. However, in unique circumstances, officers are allowed some discretion. If a passenger refuses the vehicle screening, he or she is not allowed to board the ferry. If the canine responds in a vehicle screening, it is interpreted as probable cause and allows officers to search the vehicle, its contents, and its occupants, if necessary. If a passenger refuses the search, they may be detained. Once passengers have boarded the ferry, they may not leave without permission of the captain.

Prohibited Items

Prohibited items are as follows:

- Unaccompanied freight shipments;
- Hazardous materials (49 CFR, Parts 170 to180);
- Explosives or incendiary devices (33 CFR, Part 6);
- Chemical, biological, or radiological agents or devices (33 CFR, Part 6);
- Unlawful or illegally possessed firearms;
- Illegal fireworks; and
- Acetylene tanks.

The restricted items are propane tanks, gasoline, and pressurized tanks. Some firearms are permitted on the large ferry system's ferries in accordance with state laws (ferries are considered a part of the state's highway system).

Customer Notice of PSI Program

Before the screening program began, a major media conference occurred, bulletins were issued, and information on the screening was posted on the agency's website.

Measures of Effectiveness

While the ferry system does not currently have measures of effectiveness for their vehicle inspection program, the system is in the process of developing them. In terms of the numbers of vehicles inspected, thousands of vehicles are screened on a daily basis, and tens of thousands of vehicles are inspected on a monthly basis.

PSI Program Using Airport-Style Screening (Small Ferry System)

This small ferry system that uses an airport-style PSI method is the only ferry system that has implemented an airport-style screening system. This ferry system has also implemented other security measures, including access control, video surveillance CCTV for restricted areas and other areas, and airborne patrol activities.

Policy and Protocol

The ferry operator's PSI policy is nondiscretionary and maintains that 100% of foot traffic must be screened. In addition, the PSI policy also mandates that 100% of commercial vehicle traffic (e.g., trailers, buses, and rental trucks), 100% of recreational vehicles, and 50% of privately owned passenger vehicles must be screened. However, consistent with MARSEC requirements, the Chief of Police reserves the authority to amend the screening process to increase or decrease the percentages based on the acquisition of threat-based intelligence information. There is a written inspection policy and protocol. Requests for copies can be directed to the agency. The system's inspection protocol began in 2003 in advance of the MARSEC regulatory requirements imposition. This system was the first operation in the United States to have its security plan approved by the Commandant of the Coast Guard.

Inspection Objectives and Inspection Location

The objectives of this ferry operator's PSI program are detection and prevention of a terrorist attack. PSIs for this ferry system are performed at the entranceways to the ferry facilities.

Inspection Method

Since its inception in 2003, the inspection protocol has included use of a magnetometer portal and X-ray conveyor to screen carry-on baggage. Canine inspection and hand wands have also been deployed. There is no perceptible difference between the operating environment at the ferry facilities and the operating environment at airport facilities that necessitates changes in screening equipment selection criteria. Equipment is selected based on performance criteria that place ease of use, accuracy, and operating life cycle above cost. Vehicle inspections are conducted in parking lot receiving areas. They are performed visually, with the assistance of canine explosives detection teams. Inspections teams are composed of a combination of police and security personnel. The number of officers on a team can range from 10 to 12, with a ratio of 3 police officers to 1 security officer.

Customer Notice of PSI Program

The ferry operator has taken measures to ensure that customers are fully aware of the PSI program. Signs are posted at

the facilities, and flyers describing the program have been distributed periodically. Those persons who do not wish to undergo screening are denied passage on the system.

PSI Program Using Behavioral Screening (Small Ferry System)

In this small ferry system, visual inspections using BASS began in early 2005, primarily in two of its three terminals. These inspections are based on behavior and are performed by ticket booth attendants and agents as part of routine operations under MARSEC Level 1. Ferry workers performing the visual inspections have undergone specialized behavioral training. A large portion of passengers are inspected in this manner. If the MARSEC level increases to 2, all passengers are visually inspected before entering the terminal, with two staff members stationed at the ferry terminal entrance. Also, bag searches for a certain portion of passengers would occur. If the MARSEC level is increased to 3, ferry operations may or may not continue. If operations do continue, a larger portion of bags would be inspected.

PSI Program Using Manual and Visual/Behavioral Screening (Small Ferry System)

At this small ferry system, random and targeted manual and visual security screening of vehicles, passengers, and baggage is conducted, including behavioral assessment, on its ferries. The policy and objective of the security screening were established at its onset in July 2004 in compliance with the requirements of the Maritime Transportation Security Act of 2002, 33 CFR, parts 101–105.

The primary decision makers were ferry agency staff and the U.S. Coast Guard. Policy development involved research on viable threats against ferry systems and inspection procedures utilized at similar facilities. Both legal and operational aspects were considered when establishing inspection policy, and terrorism experts were involved in the establishment process.

Vehicles, passengers, and baggage may be screened. The screening is both discretionary in terms of who (or which vehicle) to inspect and nondiscretionary. It is nondiscretionary in that vehicles are screened based on a set of random numbers provided to them on a daily basis. In addition to random screening, vehicles and/or persons may be screened based on observed suspicious activity (discretionary). Changes to inspection protocol are determined at the command level.

Objectives

The PSI objectives are deterrence and detection. Screening is expected to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of a similar nature. Screening, defined in 33 CFR § 101.105 as "a reasonable examination of persons, cargo, vehicle, or baggage for the protection of the vessel, its passengers, and its crew," is intended to ensure that dangerous substances or devices, or other items that pose a real danger of violence or a threat to security, are not present. Inspection rates and methods are dependent on the MARSEC level, which is set by the U.S. Coast Guard.

Prohibited Items

Dangerous substances or devices that have reasonable potential to cause a transportation security incident are prohibited. These substances and devices include explosives, incendiary devices (excluding fireworks), hazardous materials (placarded vehicles or containers), illegal weapons, and other items that could result in a significant loss of life, significant environmental damage, a significant disruption to the transportation system, or a significant economic disruption in a particular area.

Inspection Location and Time

Screening is conducted in the roadway prior to reaching the wharf at one location and on the wharf in the second location. Locations were chosen based on site limitations. Screening is conducted 7 days a week during all times of the day—peak and off-peak periods (including late-night periods).

Inspection Method

Visual/behavioral and manual inspection methods are used. Vehicles or passengers may be selected for screening based on both random and targeted criteria. The use of random criteria (set of random numbers generated by a computer) provided to the security staff on a daily basis is believed to reduce the impact of selection on particular socioeconomic and ethnic groups. Targeted screening is based upon "suspicious activity." Suspicious activity is defined as any activity regarding a person, vehicle, baggage, or cargo that a reasonably prudent person would consider materially out of the ordinary or unusual based on articulable facts and circumstances. Examples of abnormal or unusual activity are provided in the policy. Individuals exhibiting suspicious behavior may require further investigation. They may be asked a series of questions to verify their identity, intended destination, and the contents of their vehicle or baggage. Searches of suspicious individuals may be conducted at the discretion of the Facility Manager or supervisor. The officers are instructed not to detain anyone during the screening process. If criminal activity or suspicious activity is observed during the screening procedure, it is reported to the Facility Manager or supervisor, and law enforcement may be contacted.

Vehicles selected for screening are directed to pull into the screening area. The officer explains the random screening process, provides the driver with a screening information flyer, and asks the driver whether they agree to the voluntary screening. If the driver refuses, he or she is asked to exit the area. If the driver agrees to the screening, the officer requests that the vehicle be turned off and the hood, cargo doors, trunk lid, and other closures be opened so that a visual inspection may be performed.

Measures of Effectiveness

Although there are no measures of effectiveness for the program, in the small ferry system's manual and visual PSI program, 224,000 passengers have been screened to date. On average, 300 are screened on a daily basis, and 2,100 are screened on a weekly basis.

Customer Notice of PSI Program

Screening notices are posted on signs located approximately 1/2 mile prior to the screening station. The notices are strategically placed to allow individuals to change direction (and use an alternate route) to avoid the screening station. All passengers wishing to board the ferry must pass through the screening station and may be selected for random screening. Passengers are encouraged to arrive early, be patient with the security officers screening vehicles, and be prepared to open trunks and enclosed containers when selected for screening.

PSI Tests Using Electronic Equipment

TSA tested handheld trace detection units at the site of one of the small passenger- and vehicle-carrying ferry systems. These units were found to be moderately successful. TSA canine teams were also tested at this site and found to be successful. Funding constraints of the agency, however, prohibited the continued use of electronic equipment and explosives detection canines for vehicle and passenger screening. The average inspection time per customer was 45 seconds using the trace detection equipment. The security officers conducting the screening were contract workers, with eight officers per shift.

Trace detection equipment (a document scanner) was tested by TSA on the site of the small passenger-only ferry system. Because the testing was performed under the condition that no passenger would miss a scheduled ferry departure, not all passengers were inspected; however, about 80% were successfully inspected at 8 to14 seconds per passenger. The passengers were required to wait in a line outside of the waiting area to undergo the PSI. None of the passengers had complaints about the PSI. The U.S. Coast Guard has also performed a trial using a canine unit.

Legal Issues and Policy Drivers

The screening policy drivers for the large ferry system were primarily legal. Different federal and state laws concerning privacy levels and warrantless searches had to be addressed in the screening policy and protocol formulation. The screening methods that were selected, visual and canine, were considered the least intrusive screening methods. Canines, in particular, are nonjudgmental and respond only when there is a threat present. Also, canine detection is effective for inspecting vehicles without having officers enter the vehicle. In order to separate security inspections from ordinary law enforcement, explosives-only canines are used. However, if the officers find contraband or notice a license plate violation, they may issue a summons, and arrest or detain individuals.

The large ferry system has gone through a risk assessment process. Although customers have expressed concerns about terrorism and the agency believes that its system is vulnerable and at high risk for terrorist activity, screening passengers would create unacceptable delays to the service. Thus, the system would not implement passenger screening even with financial assistance from the government. In addition, the legal aspects of PSIs are deemed too risky in terms of privacy and civil rights issues because the state constitution has a very high standard of protection from warrantless searches. In addition, the legal aspects of PSIs using electronic equipment are considered too risky in terms of health-related issues. Finally, the agency believes that a good security program need not include passenger screening.

One of the small passenger- and vehicle-carrying ferry systems considered the following constitutional and tort issues in formulating policy and selecting methodology: invasion of privacy, injury and health effects, canine issues, and failure to exercise required level of care. To ensure that the protocol is related to the articulated purpose of the screening, the purpose of the screening is directly stated in the screening procedures. In order to minimize privacy intrusions, officers do not open enclosed containers (e.g., baggage or vehicle trunks). Screening officers do request that the owner of the vehicle/baggage open all enclosed containers. According to one ferry system official, to separate security inspections from ordinary law enforcement, inspection is conducted by contract security personnel who are screening vehicles for "dangerous substances and devices that have the potential to cause a transportation security incident." If a device is found, the vehicle/individual is prohibited from boarding the ferry. If illegal contraband is observed during screening, it is reported to law enforcement. The term "screening" is used in all policy and training documents so that the process cannot be confused with a law enforcement "search."

The other small passenger- and vehicle-carrying ferry system indicated that it is not immune from civil liability under state or local law. Legal issues of concern in formulating policy and methodology were constitutional. Tort issues were not a concern, and there have not been any lawsuits filed in conjunction with the PSI program.

Before implementing behavioral inspections, the small ferry system carrying only passengers considered a range of legal issues in formulating policy and methodology, including constitutional and tort issues. Also, behavioral training has been provided to staff members who perform visual inspections during the normal course of their duties. At the same time, there is a strict no-profiling policy at the system. There have been no complaints about these inspections.

Impact of Inspection Programs on Agency Image and Customer Satisfaction

As expected, the large ferry system's policy has had a positive effect on both its image and customer satisfaction because of enhanced security. Although thousands of inspections have been performed, there have been very few customer complaints. Furthermore, the complaints that have been submitted were minor ones.

Two of the small ferry agencies reported that there was a positive impact on both the agency's image and on customer satisfaction, and this outcome was expected. The third agency experienced a negative effect on its image; at the same time, however, there was a positive impact on customer satisfaction, which was also expected.

Collaboration with Local Law Enforcement, Emergency Responders, and the Community

For the large ferry system, the level of collaboration experienced with the state officers and the U.S. Coast Guard has been very high. The level of collaboration with local police and emergency responders has been high in terminals located in the major metropolitan area. For terminals located in outlying areas, the local police and emergency responders may not have the same resources or capability levels, and, therefore, the level of collaboration is lower in those areas. Also, the communities on the major commuter routes are more attuned to the threat of terrorism, and commuters on those routes are more alert and aware of their surroundings. Hence, the security-related collaboration is higher for the communities using the commuter routes.

One of the small ferry operators noted that it has not been experiencing a high level of collaboration with the community. However, the other two expressed a high level of collaboration with the community, and the level of collaboration that all of the operators have been experiencing with local police and emergency responders has been high.

Size and Training of the Security Force

For the large ferry system, the security division consists of three employees and seventy officers who patrol the ferry system and conduct vehicle screening. They have gone through specialized training, including ATF certification. While covert testing of the officers is not routinely performed, interagency training exercises are held.

The small ferry agencies have fewer security personnel—the passenger-only system has only 1 officer, while one passenger- and vehicle-carrying system has 12. One of the passenger- and vehicle-carrying systems has a total of 95 security staff. It is interesting to note that this operator is also the one that conducts airport-style screening.

Training for the small ferry system staff conducting manual and visual inspections was conducted by a contractor experienced in vehicle security screening. Contracted management staff attended a "Train the Trainer" session and now conduct initial and refresher training. Covert observation of inspection staff is being conducted. Training in behavioral assessment has also been provided to security staff so that they can conduct behavioral screening. The inspection teams for the small ferry system conducting airport-style PSIs receive both classroom and on-the job training and also undergo drills and exercises. While this ferry operator does not conduct covert testing, the U.S. Coast Guard does perform periodic unannounced security inspections at the ferry operator's facilities.

CHAPTER 4

PSI Decision-Making Model

Introduction

One of the important security decisions transit agencies face is whether to deploy PSIs as a countermeasure to protect their systems against terrorism. When used as a part of an overall systems security approach, PSIs can offer significant benefits that provide a more secure operating environment, even in the open access framework that typifies transit systems. Of course, transit agencies face security risks throughout their systems, not just to those assets that are routinely accessed by passengers. There are also security risks associated with the business activities of private entities providing goods or services at transit stations. For example, the delivery to vendors of foods and other retail products can create security problems at loading docks. Further, because such private businesses may have their own security functions or are able to set different security standards than those to which a public entity must adhere, transit agencies are encouraged to explore the options of coordinating security efforts with the private sector.

However, the types of threat that this chapter is focused on are those posed by would-be terrorists mingling with regular passengers as a means to attack a transit system. The decision model presented in this chapter is aimed at assisting agencies in deciding whether to institute PSIs to address such threats, and if PSIs are instituted, how to deploy them.

In this decision-making model, PSIs refer to inspections conducted without warrants or individualized suspicion. Generally, such inspections are legally permissible only if they can be justified under exceptions to the Fourth Amendment's warrant and individualized suspicion requirements. When individualized suspicion exists, inspections are subject to normal policing procedures, and such inspections are not covered by the decision-making model.

There are a number of tools and methods for carrying out PSIs, including the following:

- Behavioral assessments,
- Radiation detection pagers,
- Explosives detection canines,
- Visual/physical bag inspection,
- Visual/physical car inspection,
- Handheld detectors,
- Magnetometers,
- Walk-through detection portals (including puffer portals),
- Table-top detectors,[96]
- Baggage scanners,
- Explosives detection vans (for ferry operations), and
- Detectors integrated into ticket machines and turnstiles (under development/testing).

PSI methods can be divided into those that are based on technology and those that aren't. PSIs that are based on technology require assessment and selection of technology, which requires time and resources.

Technologies available for carrying out inspections include the following:

- Bulk detection technologies
  - X-ray
  - Backscatter X-ray
  - Millimeter wave imaging
  - Terahertz imaging
- Trace detection technologies
  - Ion mobility spectrometry (IMS)
  - Mass spectrometry (MS)
  - MS variants (emerging)
  - MS + chromatography, automated MS, environmental monitoring
  - Surface acoustic wave (SAW)
  - Optical sensors
  - Chemical luminescence

[96] Note that trace detection technologies can be housed in a table-top scanner often called a document scanner; however, samples can be obtained from any surface, including bags. Trace detection technologies can also be housed in a portable handheld detector.

- Intelligent video technology
  - Facial recognition
  - Gait/behavior detection (emerging)
  - Integrated with radiological detection (emerging)
- Liquid detection technologies (emerging)
- Biosensors
  - Canine
  - Molecular biology
  - Wasps (emerging)
- Micro-electro-mechanical systems (MEMS) sensor
- Lie detectors

At present, use of ionizing radiation is one of the key distinguishing features among technologies because members of the public may object to the use of ionizing radiation, and equipment using ionizing radiation may be subject to state and local regulation.

The technology-based methods can be further broken down by certain general characteristics that may be deemed critical for first instance evaluation: footprint, portability, use of ionizing radiation, and maturity of the technology.

Given the present state of technology and history of terrorist threats, the decision-making model is primarily focused on explosives as a means of attack, rather than radiological, chemical, or biological attacks. However, where relevant information about these other types of threats has been identified, references have been made to PSIs that address these other, overlapping attack risks. Similarly, although the PSIs considered here are primarily aimed at explosives detection, the capability of particular models to detect additional threat types is a significant consideration for deciding between specific equipment models.

Deciding whether to institute PSIs can involve a complex mix of political, economic, operational, and legal elements. The benefits of instituting PSIs, in addition to deterring terrorist attacks, may include an increased perception of security on the part of customers; this perception, in turn, has the potential secondary benefits of maintaining or increasing ridership and enhancing the general public's perception of the security of their community. Nonetheless, such additional benefits cannot on their own provide a legal rationale for conducting PSIs. The overarching rationale for determining when to deploy PSI countermeasures must be based on an assessment of the agency's risk of terrorist attack. The decision-making model presented here is designed to assist transit agencies in sorting through the complexities while maintaining a focus on risk reduction, elimination, or mitigation.

It is recommended that the PSI decision be made with the components of the transit agency's written security plan in mind. If the agency has not yet developed a written security plan, then the decision about whether to institute PSIs should be made in the context of developing an overall system security plan.

Fortunately, there are a significant number of transit systems that face a low risk of terrorist attack. For these agencies, conducting PSIs is probably not a good use of resources. In other cases, operational restrictions or limitations or budgetary constraints may cause transit agencies to determine that PSIs are either impossible to perform or inappropriate. When an agency makes this decision, a written record of the reasoning behind the decision not to conduct PSIs may prove useful—either to explain the decision to the public or to mitigate liability should some sort of terrorist event in fact take place. (See Appendix D for a discussion of the liability risks of not instituting a PSI program. In reality, there are *several* decision points at which a transit agency may determine that PSIs are not appropriate in its system. It is recommended that regardless of the decision point, the agency document that determination.)

However, even when an agency determines that the current risk of attack is low, it is recommended that a contingency plan be maintained that sets forth actions that could be taken in case of elevated risk, so that acceptable inspection parameters are known ahead of time. The activities that could be undertaken in support of the contingency plan include the following: conducting legal analysis to support inspections; identifying resources available for rapid deployment; and writing protocols for inspections that would take place at higher levels of alert or in the event of a specific threat of attack. In addition, it may be useful to identify promising technologies under development that could be deployed as they become available.[97] Furthermore, having such a plan may enhance the ability to access the resources of DHS.

When the decision is made to proceed with PSIs, the type of inspection chosen and how it is implemented will have further operational and legal ramifications. Protocols that are well thought out and appropriate training are crucial to smooth operations and mitigation of any potential liability.

Decision–Making Model

The methodology presented here provides an overarching model for decision-making. For ease of presentation, the model assumes a decision-making process with three phases:

1. Determining whether the risk of attack is sufficient to create a compelling government need for deterring or detecting attacks and, if so, further evaluating PSIs that could be used to address that need;

[97] Explosive detectors deployable on transit vehicles could be developed. See C. Bennett, "Senator Suggests Bomb Detectors for the Subway," MassTransit website. www.masstransitmag.com/article/article.jsp?siteSection=4&id=1199#.

2. If inspections are to be instituted, establishing the policy and developing accompanying protocols; and
3. Assessing inspection methods and alternatives for implementation.

If PSIs are to be instituted, the transit agency should conduct customer outreach before actual deployment. Outreach is not just a good customer relations strategy; in many instances, customer outreach is also necessary to ensure the constitutionality of the program. In addition, outreach can be used to develop additional passive surveillance through encouraging the local community to alert law enforcement to suspicious activity or to suspicious persons trying to gain access to the system. Finally, it is recommended that transit agencies conduct a review of their PSI determination annually to examine whether circumstances require commencing, modifying, or terminating PSIs.

The authors recognize that transit agencies may not follow the presented methodology step by step. Therefore, to facilitate understanding, certain steps—for example, prompts for legal analysis—are referred to and repeated more than once. Transit agencies can use these repeated references to assist them in working through the various phases of the decision-making model.

Overview of Phase 1—Risk Assessment

The Phase 1 sequence follows and is displayed graphically in Figures 1 and 2.

As a starting point, transit agencies should consider the risk of attack by asking the following questions:

- How likely are terrorists to attack the system?
- If the system were attacked, what are its most vulnerable assets?
- Of the most vulnerable assets, which are most critical to operations?
- How could the agency best protect those assets?

It is assumed that most transit agencies have previously answered these questions in whole or in part by conducting one or more prior risk assessments that have taken into account the risk analysis aspects of threat, vulnerability and criticality. Such an analysis is the necessary underpinning of a system security program (as discussed in the FTA's list of recommended top 20 security measures).[98] It is also vitally important that the risk assessment be maintained and updated on a continuing basis. "Resources for Conducting Risk Assessments" (see below) provides ready references for accomplishing risk analysis.

The risk assessment will generate a prioritized list of threats that need to be addressed. The transit agency should gather information through various sources regarding the current threat situation, especially any specific threats against its system or neighboring systems. The agency should then use this information to determine which countermeasures or combination of countermeasures to deploy. The PSI method chosen should be appropriate for addressing the threat, the perpetrator, and the threat material.

Perpetrators may be working alone, in coordination with others, or with a terrorist organization. Agencies should institute mitigation efforts against the lone perpetrator with a bomb in a backpack as well as against a terrorist cell seeking to target multiple transit locations simultaneously. Also, perpetrators' knowledge of transit operations and their level of sophistication regarding threat materials can vary significantly. Information about terrorist organizations and other perpetrators that may be operating within a particular region can be obtained by the transit agency from state and federal intelligence sources.

Because the threat environment is constantly changing, transit agencies need to keep in continuous contact with federal sources to obtain up-to-date intelligence information and ensure that their threat mitigation efforts are appropriate. Threats against transit systems can range from explosives to cyber attacks. The primary threats are identified and described in this section. While the bulk of PSI focus and effort has been directed at identifying explosives such as improvised explosive devices (IEDs), other threats must be (and are being) taken into account by transit agencies.

Major Threats Facing Transit Systems

The following the major threats facing transit systems are discussed in this section: arson, explosives, weapons of mass destruction (WMDs), violent confrontations/hostage situations, tampering, power loss, transit vehicle as a weapon, and network failure/cyber attack.[99]

Arson

Arson is an intentionally set fire. It can destroy transit assets within a facility, cause structural damage to the facility itself, cause electrical and mechanical systems failure, and cause

[98] FTA, "Top 20 Security Program Action Items for Transit Agencies." http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20.

[99] Research and Special Programs Administration, John A. Volpe National Transportation Systems Center, *Transit Security Design Considerations*, FTA-TRI-MA-26-7085-05, DOT-VNTSC-FTA-05-02 (prepared for FTA Office of Research Demonstration and Innovation and FTA Office of Program Management) (Washington, DC: FTA, November 2004). http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/default.asp.

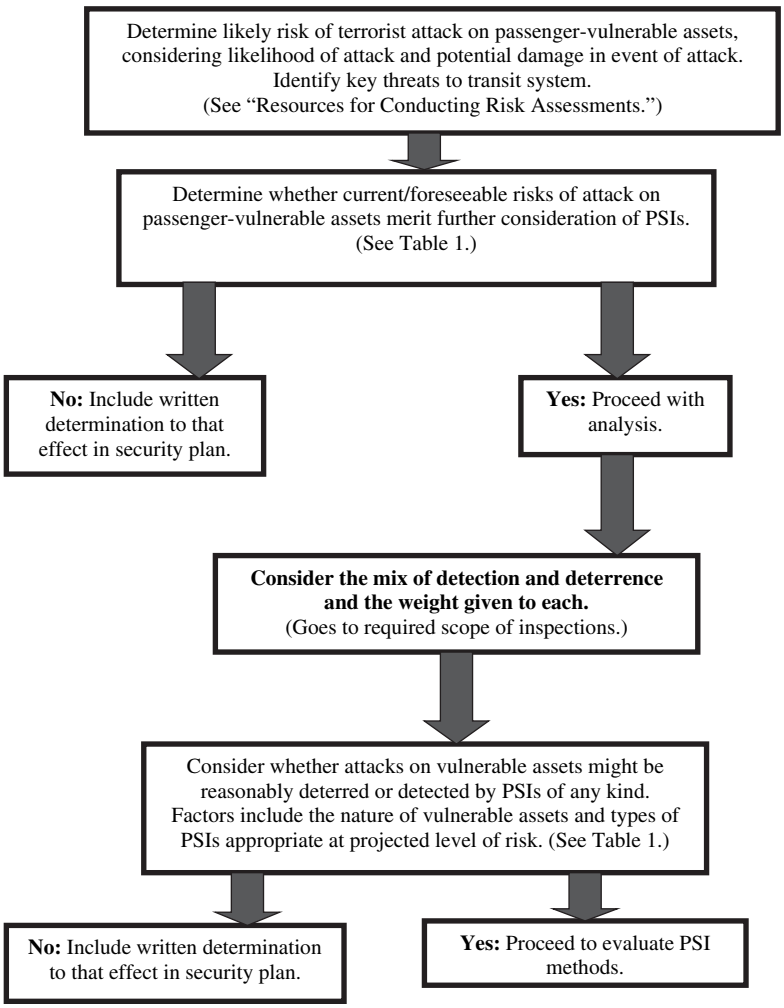

Figure 1. Risk assessment.

injuries or fatalities. Toxic fumes produced by burning fuel, oil, plastics, and some paints are a serious health threat and may cause death. Smoke can reduce visibility, obscuring exit pathways and making escape more difficult for victims. Fires may be intentional or accidental, and countermeasures for either will be relevant for both types. Arson and explosion-related fires, however, may cause more severe damage because they tend to target or cluster around critical systems and equipment.

Explosives

An explosion is an instantaneous or almost instantaneous chemical reaction resulting in a rapid release of energy. The energy is usually released as rapidly expanding gases and heat, which may be in the form of a fireball. The expanding gases compress the surrounding air, creating a shock wave or pressure wave. The pressure wave can cause structural damage to a structure while the fireball may ignite other building materials, leading to a larger fire. Explosives can cause the destruction of assets within a facility, structural damage to the facility itself, and injuries or fatalities. Explosions may start a fire, which may inflict additional damage and cause additional injuries and fatalities. The type and amount of explosive material used and the location of the explosion will determine the overall impact of the explosives.

WMDs

WMDs are nuclear, radiological, chemical, and biological weapons capable of inflicting mass casualties. Radioactive materials and other contaminants in forms such as powders, liquids, gases, and dirty bombs that are intended to harm large numbers of people are also examples of WMDs.

The hazards of WMDs are fatalities, negative health effects, and permanent or temporary contamination of a facility. Because many WMD materials have few discernable physical characteristics, symptoms are the first sign of an attack. In addition, some chemical and biological agents will not produce symptoms for hours or days after the attack has occurred.

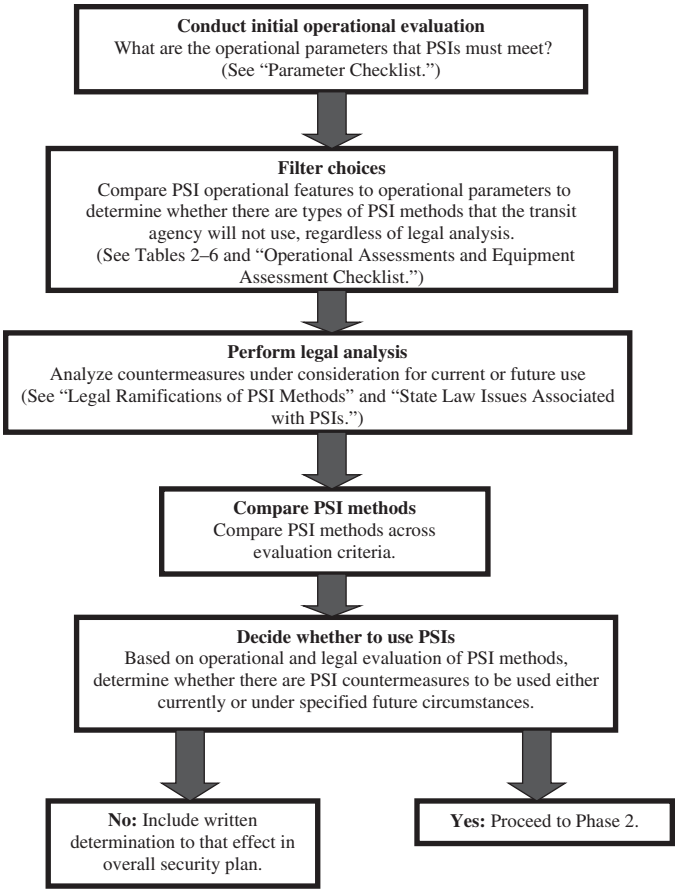

Figure 2. Evaluation of PSI methods.

Violent Confrontations/Hostage Situations

Violent confrontations and hostage situations are common on transit systems throughout the world. These confrontations include assaults and robberies within transit vehicles or at transit facilities, which may result in casualties, property loss and damage, and hostage taking. Easy access, remoteness of the vehicle, and available civilians make transit vehicles especially vulnerable to hostage situations. Attackers may use a variety of weapons, including small arms, assault rifles, shoulder-mounted rocket-propelled grenades, knives or other bladed weapons, and small explosives.

Tampering

Malicious tampering can facilitate the accomplishment of an attack; for instance, tampering with subway track can cause derailment. Transit infrastructure may be damaged by a truck, boat, or airplane carrying explosives to induce structural damage and fatalities and injuries to transit users. Tampering with electrical systems can cause power loss, wreaking havoc on transit operations (especially subway/rail operations, which rely on electrical power).

Power Loss

Local or regional loss of, or disturbances to, electrical power can significantly disrupt transit service and operations by causing diminished or suspended operations control and signal systems, computer-aided dispatch, and radio systems. Loss of power may be caused by an intentional or unintentional event aimed at the transit system or nearby targets. Power losses can affect not only transit operations but also other activities in the vicinity.

Transit Vehicle as a Weapon

Transit vehicles can become weapons as well as targets. For instance, terrorists may steer a transit vehicle into a building, bridge, or transit infrastructure, or they may plant explosives in a transit vehicle in the storage yard in hopes of detonating it at a later time. A retired transit vehicle may also be an attractive weapon or vehicle for carrying out terrorist operations because of its familiar and innocuous nature.

Network Failure/Cyber Attack

Network failures and cyber attacks can cause major disruptions to transit service and operations. As more and more transit systems deploy ITS technologies such as AVL and traveler information, the consequences of even small-scale cyber attacks can be serious and cause significant economic damage. There has been more than one case of hackers illegally accessing a transit agency's control center network and altering displays on electronic message signs. Network failure may also be caused by faulty or damaged internal components and a general computer virus.

In any event, to assess the need for and usefulness of PSIs, agencies will often be required to consider factors not previously taken into account. These additional factors relate specifically to identifying operation-critical assets that could be threatened by passengers. As the agency conducts this assessment, the intrusion posed by the PSI under consideration must be balanced against the severity of the threat to be guarded against. The intrusion and duration of the inspection itself must be taken into account (how extensive is the inspection? How long does it take?) as well as the intrusion such inspections pose throughout the transit system (Will they be conducted daily or only keyed to fixed indicators? Will they occur everywhere in the system or at fixed points only?). Thus, when an agency determines that assets throughout the entire system face a high risk of attack by passengers, they may choose to conduct PSIs daily throughout the system (as is done in New York City). When an agency determines that specific assets face a high risk of attack by passengers for

a limited time, that agency may consider conducting PSIs in a limited range of stations for a limited period of time (as in Boston in 2004).[100]

Following the initial risk assessment, the transit agency may determine that the risk to passenger-vulnerable assets is so low—both currently and under any reasonably foreseeable future circumstances—as to warrant no further action concerning PSIs. If so, it is recommended that the agency include information about that determination in its overall security plan.

Unless it has been determined that PSIs do not need to be considered, it is recommended that the agency move on to a preliminary evaluation of whether any PSI methods would protect the identified assets by detecting, deterring, or apprehending would-be terrorists. If it conducts such a review, the agency should make a written determination of the circumstances, if any, under which PSIs might be appropriate in its system.

In conducting this preliminary assessment, the agency should keep in mind the primary purposes of conducting PSIs: detection and deterrence. The assessment should anticipate that a PSI program aimed at detection will demand continuity and a pervasive presence (e.g., inspections throughout the system all the time). Such a program could be established using a single PSI method throughout the system or a combination of methods—for example, using explosives detection equipment in some areas of the system, officer inspections in other areas, and canine teams in still other areas.

On the other hand, the New York City Transit model (assuming other federal courts adopt the reasoning of the Second Circuit Court of Appeals) suggests that a PSI program aimed at deterring attacks need not have inspections everywhere in the system all the time, so long as the presence is routine yet unpredictable (see Appendix D). Thus, a deterrent program could strategically locate a mix of resources throughout the system, varying locations and times for inspections. Accordingly, it is recommended that the transit agency consider the number of vulnerable assets and the types of spaces it needs to protect first in evaluating the usefulness of PSIs as a tool and again in evaluating particular PSI methods.

Once the determination is made that there are circumstances under which PSIs may be appropriate, the transit agency must examine whether there are specific PSI countermeasures that should be deployed and the operating conditions associated with their use. Aside from legal analysis, the transit agency may determine that specific countermeasures are unacceptable from an operational perspective or, alternatively, that none of the PSIs are acceptable.

However, assuming that operationally appropriate PSI countermeasures are identified, the agency must then conduct a legal analysis of those methods. The agency can then determine whether there are PSI methods that it can deploy to guard against terrorist attack.

Overview of Phase 2—Policy/Protocol Development

Once the transit agency has determined that there is sufficient justification to deploy PSIs as a countermeasure to combat terrorism, the next step is to establish a policy to govern inspections. The agency should also develop protocols and procedures for personnel to follow in implementing the policy.

In the event that the agency decides not to implement inspections immediately, the agency should identify particular threat levels or other indicators that will control when inspections will take place. As a part of this contingency planning, those countermeasures that can be rapidly deployed in response to changing conditions should be prioritized. Indicators will also be identified for intensifying existing inspection methods. Figure 3 shows the steps in the policy/protocol development process.

Policy and protocol will specify how the set of people or objects to be inspected will be selected for primary inspections and whether there will be varying inspection levels based on passenger volumes. Policy and protocol should also specify how decisions on inspection dates, times, and locations will be made. Additionally, the agency also must specify who is in charge of the inspection process, who will make the required decisions, and who has the authority to make changes to the protocol.

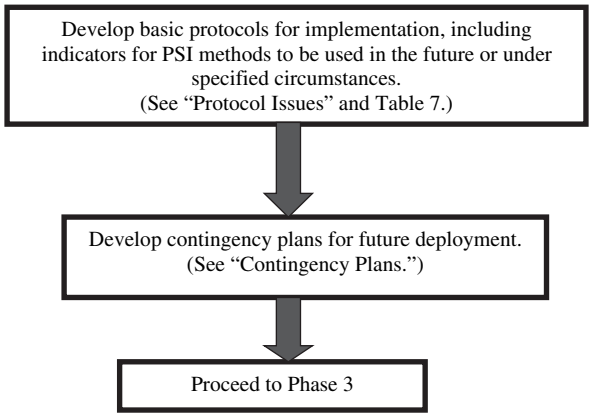

Figure 3. Policy/protocol development.

[100] The Mineta Transportation Institute (MTI) has suggestions for different threat conditions. See B. M. Jenkins and B. R. Butterworth, *Selective Screening of Rail Passengers*, MTI Report 06-07 (San Jose, CA: Mineta Transportation Institute, February 2007), 47–51.

The PSI method to be used for primary inspections and the PSI method to be used for secondary inspections should be described in detail in the agency's policy and protocol. Primary and secondary inspections may or may not include PSI technologies. If PSI technologies are to be used, technology description, specification, usage guidelines, and required training will be described. If applicable, any steps that can be taken to minimize radiation-related risks to transit personnel and customers should be clearly indicated. The protocol will state how alarms will be handled if they are not resolved after a secondary inspection or if threat material or contraband is found. In addition, if there is the possibility of innocuous but valid substances triggering an alarm, a list of those materials should be provided in the protocol. If a person leaves the area on encountering the inspecting personnel, a decision on whether or not to follow or detain the person needs to be made. This issue should also be addressed in the protocol.

The number of transit security personnel and their duties as well as the number of units of detection equipment and the number of canines that will be required for each inspection station should be specified in the protocol. It is also recommended that training information (e.g., training content, how security staff will be trained, and how many hours), performance evaluation, and monitoring procedures be included.

Overview of Phase 3—Assessment of PSI Methods

Once the transit agency identifies PSI countermeasures deemed appropriate on operational and legal grounds, it must consider whether there are further options for deployment (see Figure 4). For example, if the agency selects canine inspections, it will have to determine what opportunities exist for receiving assistance and support from DHS and/or TSA or whether to acquire the canines through other means. If the canines are not acquired through DHS or TSA, the agency will have to decide between in-house and contracted provision of services, which will require evaluation of training methods and procurement sources. Should the agency select a technology-based method, such as trace detection, it will have to evaluate different models of the equipment. In the case of officer inspections, there may be options in terms of whether to contract with outside security firms to perform the inspections.

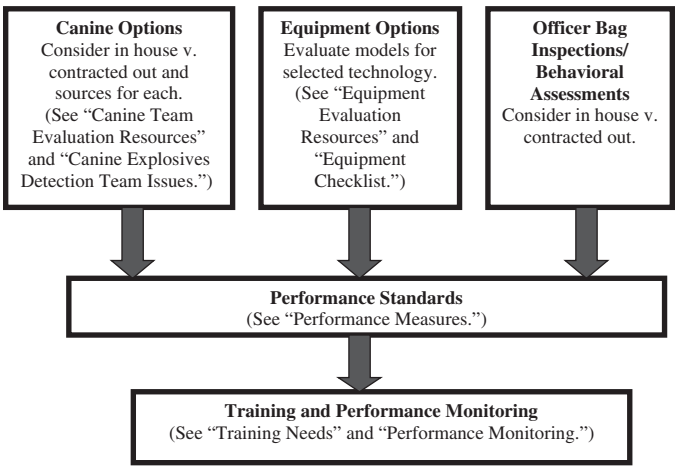

Figure 4. Selecting deployment options.

These additional options may necessitate refinements in the protocols developed in Phase 2.

Once deployment options are selected, the agency will have to finalize its performance standards and plan a training curriculum.

Phase 1—Risk Assessment

The first step is to consider the likelihood that terrorists will attack the system, the features most vulnerable to attack, the most operation-critical vulnerable features, and how best to protect those operation-critical vulnerable features. The results of such considerations should identify the risk of attack by passengers to vulnerable features and include an assessment of the extent to which vulnerable features are operation critical. Important factors in assessing risk are the number of potential casualties and the scope of potential damage. Thus, multimodal facilities and facilities with significant ancillary functions, such as movie theatres or retail stores, should be considered as being at higher risk of attack than small stations. Risk should be considered both for current conditions and reasonably foreseeable future conditions. For example, the agency may determine that there is no current risk of attack, but that the system's particular profile (e.g., the size of the city in which it is located, the importance of the transit system to local and national economy, or the impact of a terrorist attack), could make it a likely target in the future. It is also important to consider whether an identified risk is ongoing or of limited duration.

Resources for Conducting Risk Assessments

Resources are available to assist a transit agency in conducting such a risk assessment. Some of these resources are the following:

- TSA/FTA Security and Emergency Management Action Items for Transit Agencies. (http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/ActionItems/default.asp)
- "Risk Management: An Essential Guide to Protecting Critical Assets" (November 2002). (http://transit-safety.volpe.dot.gov/security/securityinitiatives/top20/2%20–%20security%20problem%20identification/8%20–%20

threat%20and%20vulnerability%20assessment/additional/nipc_risk_management_process.pdf)
- Jenkins, B. M. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*. MTI Report 01-14. Mineta Transportation Institute, October 2001. (http://transweb.sjsu.edu/mtiportal/research/publications/summary/0114.html)
- TSA Security Analysis and Action Programs, TSA technical assistance for risk assessments, and TSA security training. (http://www.tsa.gov/approach/risk/assessment_tools.shtm)
- Sandia National Laboratories. (http://www.sandia.gov/mission/homeland/factsheets/index.html)
- Parsons Brinckerhoff (D. B. Ham and Stephen Lockwood) and Science Applications International Corporation. "National Needs Assessment for Ensuring Transportation Infrastructure Security." Prepared for the AASHTO Transportation Security Task Force. AASHTO, October 2002. (http://www.transportation.org/sites/security/docs/NatlNeedsAssess.pdf)
- Homeland Security Comprehensive Assessment Model (HLS-CAM). (https://www.dhssaver.info/actions/document.act.aspx?type=file&source=view&actionCode=submit&id=3079)
- Transportation Research Board, security publications. (www.TRB.org/SecurityPubs)
- Department of Energy Information Bridge. (http://www.osti.gov/bridge/basicsearch.jsp)
- Department of Homeland Security—Transportation Risk Assessment and Vulnerability Evaluation Tool (http://www.tsa.gov/approach/risk/editorial_1733.shtm)
- NCHRP Project 20-59(17), "Guide to Risk Management of Multimodal Transportation Infrastructure" (scheduled for completion November 2007). (http://www.trb.org/TRBNet/ProjectDisplay.asp?ProjectID=637)

Following the risk assessment, the agency should consider the types of inspections that may be appropriate to its particular level of risk. When the risk of attack is low, inspections should be minimally intrusive, have a low impact on passenger operations, pose few (if any) risks of civil liability, and be relatively inexpensive. At the other end of the scale, when the risk of attack is higher, agencies should assess the need for inspections to be more intrusive. In general, when the risk of terrorist attack is higher, passengers are likely to be more willing to tolerate delays or inconveniences, the agency may be willing to run greater legal liability risks, and there may be a willingness to devote more resources to the inspection method. From a constitutional perspective, when the risk of attack is higher, more intrusive inspection methods can be justified. This applies to the absolute intrusiveness of the PSI method and its duration (a continuing threat is more likely to justify continuing inspections).

The first decision that must be made is whether there are any circumstances under which PSIs should be used as a countermeasure to protect operation-critical assets. If the agency determines that no such circumstances exist, it should include that written determination in its overall security plan. However, even when an agency identifies little or no current risk of terrorist attack, it should consider PSI methods that can be quickly and easily deployed to meet future threats.

If the agency determines that there may be circumstances under which PSIs may be appropriate, it should evaluate PSI methods to determine their appropriateness for deployment. This determination should depend primarily on a consideration of the assets identified as vulnerable and the particular purpose of the inspections, for instance, detection or deterrence. In the latter case, it is important for the agency to consider that PSIs need not—and indeed, under many circumstances, should not—be performed daily throughout its system. The list below shows what kinds of inspection are appropriate for low, medium, and high levels of risk, respectively (see also Table 1):

- **Low level of risk**—Use of radiation detection pager, environmental monitors, screening of suspicious or abandoned packages.

Table 1. Types of inspection to consider for high, medium, and low risk of terrorist attack.

Low	Medium	High
• Passive measures • Contingency plan for heightened alert/specific intelligence	• Passive measures • Low-level inspections • Contingency plan for heightened alert/specific intelligence	• Passive measures • Visual/physical inspections • Technology-based inspections • Plans for intensified screening in case of heightened alert/specific intelligence

Note. When the risk of terrorist attack is low, it may still be appropriate to deploy numerous noninspection security measures, such as CCTV and customer awareness programs.

- **Medium level of risk**—Use of canine teams; behavioral assessments by trained security personnel and transit staff (e.g., token booth clerks, bus operators, and cleaners); intelligent video, including facial recognition; abandoned package recognition; and atypical behavior recognition.
- **High level of risk**—Use of random manual and electronic inspections. (The inspection percentage and number of locations should be adjusted based on the actual level of risk; if the level of risk is very high at a particular location, the inspection procedure may be changed from random to more frequent or to screening of all passengers. However, it is important to avoid counterproductive operating conditions by conducting inspections at such a high percentage that crowds are formed.) Equipment that may be used for the inspections includes portals, trace detection in ticket machines or turnstiles, handheld devices, desk-top trace detectors, and baggage scanners.

Assessing Operational Parameters

In order to evaluate PSI methods, the transit agency should first assess its operational parameters. If the particular system contains more than one mode of transit, the agency is likely to have to assess parameters for each mode. The parameter checklist below may be useful in assessing operational parameters. Note that the priority of the checklist questions may vary. One of the analytical steps is to prioritize the questions. This will help with later steps in the analytical process.

Parameter Checklist

The parameter checklist includes assessment in five areas: equipment, personnel, passenger services impact, cost considerations, and miscellaneous issues.

Equipment

Issues to consider regarding equipment are the following:

- What locations in the system are available for deploying inspections?
- What space is available for inspection equipment?
- What are the portability aspects of inspection equipment?
- What facilities are available to secure and store inspection equipment?
- Is there a preference for technology-based or non-technology-based methods?
- Is the operating environment clean or dirty from an equipment maintenance perspective? Are there concerns about use of ionizing radiation?
- What is the administrative tolerance for managing emerging technologies?

Personnel

Issues to consider regarding personnel are the following:

- How many personnel are available to perform inspection duties?
- Who will supervise and manage the inspection programs?
- What is the level of technical knowledge required to operate the equipment?
- How much training would be required to maintain operator proficiency?
- What operational or administrative support will be required to conduct the inspections?
- What duration of inspections can be maintained based on staffing levels?

Passenger Services Impact

Issues to consider regarding passenger services impact are the following:

- What is the maximum time to inspect that can be tolerated?
  - Consider peak and off-peak tolerance
  - Consider operational perspective and passenger perspective[101]
  - Consider difference between day-to-day delays and delays for inspections done during a limited period of time in order to meet a specific threat
- What space is available for passengers waiting to go through a PSI?
- Are there inspection alternatives available for persons with disabilities?

Cost Considerations

Issues to consider regarding cost are the following:

- What is the budget for inspection methodologies (consider acquisition, training, operation [including labor], and maintenance)?
- Is there an opportunity cost associated with the inspections?

Miscellaneous Issues

Miscellaneous issues to consider are the following:

- What operational trade-offs will be necessary?
  - Performance versus operational feasibility

[101] The agency may want to survey customers concerning their perceptions of the threat of terrorism, their tolerance for security-related delays at present, and their tolerance for security-related delays in the event of a specific threat of attack.

Table 2. Location criteria for PSI methods.

	Requires significant space for inspection	Can be deployed virtually anywhere in system	Best deployed at entry-point to system	Easily moved to different points in system
Canines	No	Yes	Not necessarily	Yes
Detection pagers	No	Yes	Not necessarily	Yes
Visual/physical bag inspections by officers	No	Yes	Not necessarily	Yes
Ticket scanners	No	No	Not necessarily	No
Handheld scanners	No	Yes	Not necessarily	Yes
Desktop equipment	No	Yes (assuming availability of power)	Not necessarily	Yes
Magnetometers	Yes	No	Yes	No
Portals	Yes	No	Yes	No

Note. The criteria in Table 2 do not reflect legal considerations.

  - Performance versus customer acceptance
  - Operational feasibility versus customer acceptance
- Are there defined access points for the system at which inspection personnel or devices can be stationed?
  - Systems that operate on the honor method do not have turnstiles and could have difficulty implementing certain PSI methods.

Operational Assessments and Equipment Assessment Checklist

Once operational parameters have been assessed, the transit agency should compare its parameters to the location criteria of various inspection methods (see Table 2). There are a number of factors that an agency should consider, such as where in its system PSIs could be conducted, whether there are types of inspection that are unsuitable because of space limitations, and how easily PSI methods can be redeployed. *Ability to redeploy is of interest because it is possible to construct a deterrence model that deploys PSIs in varying, selected portions of the system (i.e., it is not always necessary to inspect everywhere every day).*

While it is recommended that the initial assessments focus on operational issues, legal considerations relevant to determining where to deploy PSIs may be of interest even at this early stage. In some cases, the location of the inspection may affect its intrusiveness, an important factor in assessing constitutionality. More specifically, location may affect both randomization (reduces intrusiveness) and the ability of passengers to decline inspection (reduces intrusiveness)—important constitutional factors.

Randomness is important from legal, operational, and security standpoints. To reduce legal liability, it is better to inspect either all passengers or to inspect passengers at random. Operationally, for most transit systems, inspecting all passengers is not feasible; therefore, random inspections would be the most logical choice. Inspections that are random both in terms of *who* will be inspected and *where* the inspections will take place are a strong deterrent to terrorists, who try to avoid uncertainty.

Accordingly, before deploying a non-suspicion-based[102] PSI method that may result in Fourth Amendment concerns, an agency should consider whether the inspection could be carried out in a random, nondiscretionary manner, and whether passengers have an ability to decline the search. If the answer to either question is no, the risk of the inspection method being held unconstitutional will increase. In some cases, whether a passenger understands that he or she is free to leave the scene may also be constitutionally significant. Table 3 shows the effect of location on the relative ability of a passenger to decline an inspection and leave the scene, as well as the effect of location on the randomness of the inspections. Randomness is also relevant to preventing racial profiling.

PSI methods can be divided into those that are not based on technology and those that are (see Table 4). Most of the technology-based methods will require resources for testing

[102] Behavioral assessments, which are based on suspicion of prohibited behavior, require a different sort of analysis. See "Legal Ramifications of PSI Methods" below.

Table 3. Effect of inspection location on significant constitutional issues.

	Ability to decline search	Ability to leave scene	Ability to ensure randomness
At entry point	High	High	High
Within terminal	Medium	Medium-Low	Medium-Low
On platform	Medium	Medium-Low	Medium-Low
At interior bus stop	Medium	Medium-Low	Medium-Low
At exterior bus stop	Medium	Medium-Low	Medium-Low
On conveyance	Low	Low	Low

and evaluation of particular models before actual deployment, which may make it difficult to deploy those methodologies quickly. It is highly recommended that even technologies that are proven in airports and other environments be tested under the agency's specific operating conditions. For some agencies, the use of technology may be viewed as a strong positive or strong negative; thus, dividing methods into technology-based and non-technology-based categories may serve as an initial means of sorting them.

Technology-based PSI methods can be further categorized by several general characteristics that can be easily ascertained and that may eliminate them from further consideration. These categories are footprint, portability, use of ionizing radiation, and maturity of the technology (see Table 5). Radiation is particularly significant, as technologies used in airports are not necessarily deployable in all states; use of radiation in transit environments is subject to state health regulations. (See Appendix D.)

Once the agency has evaluated a location, taking into consideration operational and legal issues and the previously mentioned health regulations, it may proceed to do a more general operational assessment of any PSI method not already eliminated. Table 6 lists various operational criteria that should be considered in the adoption of a PSI method. As discussed in "Phase 3—Assessment of PSI Methods," there are additional criteria that should be considered in selecting equipment models.

Once the agency has compared PSI operational features to the agency's operational parameters, it may be useful to then evaluate targeted inspection methods using the Equipment Assessment Checklist. The Equipment Assessment Checklist, which can be used to perform an operational assessment of technology types, includes the following criteria:

- Space requirements
- Impact on passenger throughput
- Power
  - Power source requirements
  - Availability of appropriate power source
- Environmental effects on equipment
  - Fumes produced by commuter railroad trains and subways
  - Dust or vapors from construction work
  - Cleaning fluids
- Accessibility to disabled passengers
- Accuracy (see Appendix A in for a description of differences among trace technologies)

Table 4. Non-technology-based and technology-based PSI methods.

PSI method	Non-technology-based	Technology-based
Behavioral assessments	X	
Radiation detection pagers		X
Ticket-machine scanners		X
Explosives detection canines	X	
Visual/physical bag inspection	X	
Handheld detectors		X
Desktop detectors		X
Portals		X
Baggage scanners		X
Z backscatter vans		X

Table 5. Technology-based PSI methods categorized by four characteristics.

	Footprint	Portable	Uses ionizing radiation	Mature technology[1]
Radiation detection pagers	Small	Yes	No	No
Ticket-machine scanners	Small	No	Yes	No
Handheld trace detectors	Small	Yes	IMS/MS[2]-based do	IMS, yes, otherwise no
Handheld metal detectors	Small	Yes	No	Yes
Desktop trace detectors	Medium	Yes	IMS/MS-based do	IMS, yes, otherwise no
Puffer portals	Large	No	IMS/MS-based do	IMS, yes, otherwise no
Magnetometers	Large	No	No	Yes
Z backscatter vans	Large	Yes	Yes	No
Backscatter X-ray scanners	Large	No	Yes	No
Baggage scanners	Large	No	Yes	Yes

[1]"Mature technology" here means a technology that has been well tested in both laboratory and field settings and has been available for deployment for explosives detection use for at least several years.
[2]IMS=Ion mobility spectrometry. MS=Mass spectrometry. Airports appear to be experiencing difficulty with this technology. See E. Lipton, "Faces, Too, Are Searched at U.S. Airports," *New York Times*, August 17, 2006, Late Edition—Final, sec. A, p. 1, col. 3, www.nytimes.com/2006/08/17/washington/17screeners.html (article available for purchase at this URL).

  - False acceptance rate
  - False alarm rate
- Health issues
  - Whether equipment emits any radiation or in any way affects health of operators or persons inspected
  - Whether state law allows nonmedical use of radiation equipment on people
  - Whether state law requires licensing of technicians to operate the type of equipment being evaluated
  - Whether state law requires certification and subsequent inspections of the type of equipment being evaluated
- Cost
  - Unit cost
  - Installation
  - Life cycle
  - Operation and maintenance
  - Labor
  - Training
  - Infrastructure modification
- Maintenance requirements
  - Ease of use, including number of personnel required for operation and training required for proficiency

Based on the parameter assessment and review of the operational ramifications of various PSI methods, the agency may then determine whether certain types of PSI methods should be eliminated from consideration. Such methods need not be subject to legal analysis, although it is recommended that the agency document its reasons for eliminating methods from consideration.

Analysis of Legal Ramifications

After the operational assessments have been conducted, it is important to analyze the legal ramifications of deploying various PSI methods. As noted in Appendix D, significant constitutional and tort issues may come into play in deploying PSIs. (Agencies should conduct analysis of specific PSI methods of interest under relevant state laws, with particular attention to potential health restrictions. In the transit environment, state and local laws concerning deployment of devices that use ionizing radiation may also be controlling. See "State Law Issues Associated with PSIs" below.) Finally, the protocols for deploying the PSI methods may affect legal liability. (See Table 3 and "Protocol Issues" below.)

Table 6. General operational criteria for assessing PSI methods.

Method	Acquisition cost[1]	Operation and maintenance costs[2]	Inspection (analysis) time[3]	Effectiveness/ accuracy[4]	Amount of training required[5]	Reliability[6]	Accessible to individuals with disabilities
Canines	Medium	Medium	Low	High[7]	High	High[7]	N/A
Behavioral assessment	N/A	N/A	N/A	High	High	N/A	N/A
Radiation detection pagers	Low	Low	N/A	High	Low	High	Yes
Officer visual/ physical bag search	N/A	Low	Low	High	Medium	N/A	N/A
Ticket-machine scanners	Unknown	Unknown	Designed to be low	Unknown	Unknown	Unknown	Possibly not
Handheld trace detectors	Low	Low	Low	High	Relatively low	High	Yes
Handheld magnetometers	Very low	Low	Low	High	Low	High	Yes
Desktop scanners	Low	Low	Low	High	Low - medium	High	Yes
Magnetometers	Medium	Medium	Low	High	High	High	Possibly not
Puffer portals	Medium	Medium	Low	Medium-high	High	N/A	Possibly not
Backscatter X-ray	Medium	Medium	Low	N/A	High	N/A	Possibly not
Car-bomb screener	High	High	Low	N/A	High	N/A	Possibly not
Baggage scanners	High	High	Low	High	High	High	N/A

[1] Based on the following definitions: Very low ≤ $25,000, Low = $25,000–$70,000, Medium = $70,000–$300,000, High > $300,000. Handheld and portable metal and trace detectors are typically low in acquisition costs while trace and bulk detection portals are moderate and bulk detection conveyor equipment is expensive.
[2] Operation and maintenance costs are generally estimated to be 5–10% of the acquisition cost. The estimates in this table are based on this rule-of-thumb; however, because precise operation and maintenance costs differ by vendor, additional cost-related research should be performed by the decision-maker. The cost per passenger trip will depend on the total number of daily trips. In New York City, canines, X-rays, and metal detectors would cost about $0.40 cents per trip, while in Cleveland, which provides far fewer trips, the cost would amount to $3.45 per trip.
[3] Based on the following definitions: Low ≤ 10 sec, Medium = 10–30 sec, High > 30 sec. Analysis time is generally low, 10 sec or less for most technologies; however, the total transaction time (including the time needed for officers to explain the procedure to the passenger) can vary.
[4] Bulk detectors experience lower rates of "nuisance" alarms because they do not sound an alarm for residues that could have been from an innocuous source. Another benefit of bulk technology is that new explosive materials would not be detected by trace detectors, while bulk technologies make it possible for operators to identify suspicious items. Threat material may be more difficult to detect if sampling misses an area contaminated with traces of explosive. At the same time, false alarms and innocuous true positives may occur more frequently when trace detection equipment is used. Effectiveness and accuracy are higher for MS than IMS technology and higher for backscatter X-ray than X-ray. False acceptance rates and false rejection rates should typically be in the range of 1–5%. Finally, it should be noted that these manufacturer-stated accuracy rates should be backed up with operational testing in the transit environment.
[5] While all equipment requires calibration and understanding start-up and testing procedures, the portable metal and trace detectors are easier to operate than the larger equipment. Portable equipment would require a minimum of 1 day of training, while other equipment would require longer training periods. To operate trace detectors (including handheld trace detectors) the operator must know what areas and how to sample. Bulk detection equipment that relies on images would also require quite a bit of training—operators need to know what images look suspicious and what images do not.
[6] Tests have shown no major differences in reliability among the technologies. Even the handheld detectors were shown to be reliable in both indoor and outdoor temperature ranges and varying humidity levels.
[7] Canines tend to tire easily; some become ineffective after 30 min. Therefore, canines will require frequent breaks. Further, it is not always possible to tell when they are "off-duty."

Below, in "Legal Ramifications of PSI Methods," general potential legal liability for each potential PSI method and ways to mitigate such exposure are summarized. For each method, training on necessary protocols is likely to mitigate liability. For each suspicionless method, Fourth Amendment liability is likely to be mitigated by tying the inspections to clearly articulated threats, providing adequate notice, affording the opportunity for persons to avoid inspection, and limiting the scope of the inspection to the threat. "Notice" refers to announcing that passengers may be subject to inspection.

Notice does not include divulging operational aspects of the program, such as precisely when inspections will take place or the standards the agency uses to set inspection intervals or locations. Even for suspicion-based inspections, tying the inspections to clearly articulated threats and limiting the scope of the inspection to the threat should serve to mitigate Fourth Amendment liability.

The summaries in "Legal Ramifications of PSI Methods" highlight legal issues relevant to the deployment of PSI countermeasures. However, the list is not intended to be all inclusive. Each agency will have to individually assess its own inspection program activities based on applicable federal and state laws and its own tolerance for risk. The deployment of PSI countermeasures may result in the apparent detection of a suspicious substance that turns out to be innocuous after secondary screening. Thus, there is always the potential for a passenger claiming that he or she has been treated in an unfair/unlawful manner. This risk is mitigated by training inspecting officers on the appropriate response to the apparent need for secondary screening. However, certain PSI methods are more susceptible than others to producing false/innocuous positives, and those methods are identified in "Legal Ramifications of PSI Methods."

Legal Ramifications of PSI Methods

The legal ramifications of several PSI methods are discussed below. For each method, potential constitutional issues, tort issues, and Americans with Disabilities Act (ADA) issues are described. Major risks are also listed, as well as strategies for mitigating major risks. Some PSI methods discussed also include consideration of other ramifications.

Behavioral assessments. Police officers can be trained to assess behavior to identify potential terrorists, just as they can be trained to identify potential drug traffickers. On the basis of their training in identifying potential terrorists, police officers can stop and ask questions of passengers who meet the protocol indicators to either dispel or confirm reasonable suspicion. Ramifications of this method are the following:

- Constitutional—There is no Fourth Amendment impact to merely striking up a conversation or requesting identification, so long as it is clear that the person subject to request is free to decline (or merely ignore the request). At bus stops, in terminals, and on platforms it should be relatively clear that the person subject to the request is not being detained. But there may be greater risk of constitutional violation should the request be made on the conveyance itself. The Fourth Amendment (and state constitutions, which may have more stringent requirements) requirement of reasonable suspicion must be met absent clear consent. In at least some states, the use of racial/ethnic characteristics as behavioral assessment indicators is likely to be deemed illegal.
- Tort—Potential basis for constitutional tort claim (Fourth and Fourteenth Amendment and, where permitted under state law, corollary state provisions). Potentially basis for invasion of privacy claim, risk extremely low. No apparent health risks.
- ADA—No apparent ADA ramifications.
- Major risk—Risk of claims of constitutional violations, including unlawful detention (constitutional and tort). Potential for claims of racial profiling. Risk may vary depending on state law governing racial profiling.
- Mitigation of major risks—Protocol that relies on objective indicators to extent feasible, does not rely exclusively on racial/ethnic characteristics, clearly delineates behavior required to establish reasonable suspicion, reasonably circumscribes officer's discretion in conducting behavioral assessment. Protocol requiring that absent reasonable suspicion, if person declines to provide ID or answer questions, officer will take no further action. Training on protocol and racial profiling.

Radiation detection pagers. These pagers are small enough to be worn on a belt clip and sensitive enough to detect radiation without being in close proximity to passengers; thus, no active inspection occurs unless the pager alarms. Ramifications of this method are the following:

- Constitutional—Possibly not an inspection for Fourth Amendment purposes, because passengers are not individually approached unless the device alarms, at which point reasonable suspicion is present.
- Tort—Potentially a basis for an invasion of privacy claim, although the risk is extremely low. Possible claims based on treatment following false positive/innocuous true positive.
- ADA—No apparent ADA implications.
- Major risk—Passengers detained based on inaccurate/misleading results may file suit.
- Mitigation of risks—Protocol requiring positive results as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening. Awareness of possibility that medical treatment may set off radiation detection pagers.

Trace detector integrated into ticket machine. This screening occurs during the ordinary course of business, prior to passenger entry into the transit system. Ramifications of this method are the following:

- Constitutional—Possible Fourth Amendment concerns exist. Given that the scanner only checks for prohibited substances and that it does so in the course of a passenger-

initiated transaction, this kind of inspection should be considered minimally intrusive for Fourth Amendment purposes.
- Tort—Potentially basis for invasion of privacy claim, risk extremely low. Possible claims based on treatment following false positive/innocuous true positive. Scanners employing IMS/MS technology may pose health risks.
- ADA—Need to ensure that machine is ADA-compliant or must provide secondary screening.
- Other—Scanners employing IMS/MS technology may be illegal in some states; may require certification, licensing of inspectors in some states.
- Major risk—Passengers detained based on inaccurate/misleading results may file suit. Claims based on health risks.
- Mitigation of risks—Protocol requiring positive results as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening. Provide notice that the ticket machine contains a scanner in order to allow passengers the option of avoiding even minimally intrusive inspection. Scrupulously maintain radiation components.

Nonintegrated (desktop) document scanner. Passenger is asked to touch a card that can capture traces of explosives; the card is then scanned and analyzed. For some models, the operator swabs the surfaces of objects that may have come into contact with the passenger, and the swab is analyzed by the scanner. Ramifications of this method are the following:

- Constitutional—Possible Fourth Amendment concerns exist, but as officer does not inspect contents of bag, and scanner only checks for prohibited substances, inspection should be considered minimally intrusive for Fourth Amendment purposes. More intrusive than scanner integrated into ticket machine, as it does require that the passenger stop activity for inspection.
- Tort—Potentially basis for invasion of privacy claim, risk low. Possible claims based on treatment following false positive/innocuous true positive. Scanners employing IMS/MS technology may pose health risks as all desktop trace detection models use ionizing radiation.
- ADA—No apparent ADA ramifications.
- Other—Scanners employing IMS/MS technology may be illegal in some states; may require certification, licensing of inspectors in some states.
- Major risk—Passengers detained based on inaccurate/misleading results may file suit. Claims based on health risks.
- Mitigation of risks—Protocol requiring positive results as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening. Scrupulously maintain radiation components.

Explosives detection canines. Dogs patrol/are stationary and alert when they detect explosives. They are also used frequently for secondary screening inspections. Ramifications of this method are the following:

- Constitutional—Virtually no federal constitutional impact on bag inspections, particularly if passengers are not stopped in order to conduct inspection. (Compare with *Illinois v. Caballes*,[103] where the issue was whether the motorist had been detained. See discussion in Appendix D.) When a passenger is stopped so that a canine may sniff either the passenger or the passenger's bag, the stop may be considered a seizure under the Fourth Amendment, thus requiring constitutional justification. Even detection of explosives on passenger (rather than in bag) is likely to be deemed minimal intrusion outweighed by compelling government need. Absent faulty training or officer misconduct, no danger of racial profiling. Cross training for explosives and drug detection could give rise to pretexting claims, which, depending on the factual situation, could also give rise to racial profiling claims.
- Tort—Possible basis for claims related to canine behavior. Possible claims based on treatment following false positive/innocuous true positive. No apparent health risks.
- ADA—No apparent ADA ramifications.
- Major risks—Passengers attacked by canines may file suit; passengers detained based on inaccurate/misleading results may file suit.
- Mitigation of major risks—Appropriate training, certification (e.g., TSA certification). Protocol requiring that passenger stops for purposes of allowing canine to sniff be conducted according to inspection protocol and that positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.

Visual/physical bag search. Officers inspect passenger bags by looking inside and possibly physically manipulating bag contents for better visibility. Ramifications of this method are the following:

- Constitutional—Significant Fourth Amendment ramifications to this PSI method. Justified where government need is compelling, intrusion is minimized, and protocol design is effective.
- Tort—Potentially basis for invasion of privacy claim, risk relatively low. No apparent health risks.
- ADA—No apparent ADA ramifications.
- Major risks—Fourth Amendment challenges, invasion of privacy claims.
- Mitigation of major risks—Efforts to minimize intrusion by limiting scope particularly critical for mitigating Fourth Amendment liability for this method. Directing officers

[103] 543 U.S. 405 (2005).

not to read any material in passenger bags will minimize privacy claims as well as intrusiveness.

Handheld trace detectors. A sample is taken from the outside of a bag by swipe or vapor analysis. Ramifications of this method are the following:

- Constitutional—Fourth Amendment implicated, but should be considered to be a minimally intrusive inspection, as officer does not inspect contents of bag.
- Tort—Potentially basis for invasion of privacy claim, risk extremely low. Scanners employing IMS/MS technology may pose health risks.
- ADA—No apparent ADA ramifications.
- Other—Scanners employing IMS/MS technology may be illegal in some states; may require certification, licensing of inspectors in some states.
- Major risks—Fourth Amendment challenges, invasion of privacy claims, health claims.
- Mitigation of major risks—Scrupulously maintain radiation components.

Handheld magnetometers. Officers inspect passengers/bags with a wand that detects the presence of metal. Ramifications of this method are the following:

- Constitutional—Possible Fourth Amendment concerns exist. Inspection considered more intrusive than magnetometer because of physical proximity between officer and passenger. Wand inspection of bag less intrusive than visual/physical bag inspection because officer does not inspect contents of bag, wand inspection of passenger arguably more intrusive than visual/physical bag inspection because of physical proximity between officer and passenger.
- Tort—Potentially basis for invasion of privacy claim, risk relatively low.
- ADA—No apparent ADA ramifications.
- Major risks—Fourth Amendment challenges.
- Mitigation of major risks—Using as secondary PSI method should mitigate intrusiveness of physical approach to passenger, as there would be some grounds for suspicion.

Backscatter X-Ray machine. When the passenger steps onto the machine, backscatter signals interact with explosives, plastics, and metals and present the shapes of the objects to screeners. Ramifications of this method are the following:

- Constitutional—Fourth Amendment concerns exist. Likely to be considered far more intrusive than magnetometer because of revealing nature of image.
- Tort—Potentially basis for invasion of privacy claim, risk possibly higher than for any other inspection method detailed in this report. Possibly significant health risks.
- ADA—Machine must be ADA-compliant or agency must provide secondary screening.
- Other—May be illegal in some states; may have certification, licensing requirements where legal.
- Major risks—Fourth Amendment challenges, invasion of privacy claims, health risks.
- Mitigation of major risks—Privacy claims may be mitigated by concealing sensitive body areas or reducing image details and also by ensuring that images are not displayed to anyone but the inspectors. Destroying images once they are reviewed for security purposes should also mitigate risk of privacy claims. Health claims may be mitigated by proper maintenance and operation.

Millimeter wave imaging scanners. Millimeter wave holographic imaging systems are capable of imaging through clothing to detect contraband, metal, plastic, or ceramic weapons. Ramifications of this method are the following:

- Constitutional—Possible Fourth Amendment concerns exist. Not as intrusive as backscatter X-ray machine.
- Tort—Possible claims arising from false positives. Possible health risk, relatively low risk.
- ADA—Machine must be ADA-compliant or agency must provide secondary screening.
- Major risks—Fourth Amendment challenges.
- Mitigation of major risks—Health claims may be mitigated by proper maintenance and operation, as well as protocol to ensure appropriate handling of positive results.

Puffer portals. The portal uses puffs of air to dislodge any residue on the passenger; the residue is then analyzed using an ionizing radiation source. Ramifications of this method are the following:

- Constitutional—Should be considered search for Fourth Amendment purposes. Not as intrusive as backscatter X-ray machine.
- Tort—Possible claims arising from false positives. Health risk.
- ADA—Machine must be ADA-compliant or agency must provide secondary screening.
- Other—May be illegal in some states; may require certification, licensing in some states.
- Major risks—Fourth Amendment challenges, health claims.
- Mitigation of major risks—Health claims may be mitigated by proper maintenance and operation and protocol to ensure appropriate handling of positive results.

Baggage X-Ray scanners. Carry-on bags are put through machines that screen for explosives using X-rays. Ramifications of this method are the following:

- Constitutional—Certainly considered search for Fourth Amendment purposes. In airport context this has been considered a minimally intrusive search.

- Tort—Potentially basis for invasion of privacy claim; risk relatively low. Possible health risks.
- ADA—Machine must be ADA-compliant or agency must provide secondary screening.
- Other—May have certification requirements in some states.
- Major risks—Fourth Amendment challenges, health risks.
- Mitigation of major risks—Health claims may be mitigated by proper maintenance and operation.

Z backscatter van. The van contains explosives detection technology using backscatter X-rays. This technology is suitable for use in ferry terminals, where the van can move alongside vehicles waiting to board the ferry. Ramifications of this method are the following:

- Constitutional—Should be considered search for Fourth Amendment purposes.
- Tort—Possible health risk, particularly if van used on vehicles with passengers in them.
- ADA—No apparent ADA ramifications.
- Other—May require certification in some states. To extent it exposes passengers to X-rays may be illegal in some states.
- Major risks—Fourth Amendment challenges.
- Mitigation of major risks—Health claims may be mitigated by proper maintenance and operation and ensuring that van only inspects vehicles without passengers in them.

State Law Issues Associated with PSIs

It is imperative that the transit agency research the law of its own jurisdiction on the legal issues associated with any particular PSI. (See Appendix D.) The following checklist of jurisdictional laws, legal definitions, and legal issues may prove helpful with this research:

- Racial profiling;
- Search and seizure law;
- Whether canine sniff of person is a search;
- Whether canine sniff of property is a search;
- Whether an agency can be subject to tort liability;
- Exceptions to tort liability (governmental/proprietary or discretionary/ministerial);
- Tort implications of purchase of liability insurance;
- Public duty rule;
- Tort liability for state constitutional violations;
- Tort liability for invasion of privacy;
- Duty of care owed to prevent terrorist attack, including duty to warn of danger of attack;
- Tort liability for dog exposure;
- Tort liability for health hazards of screening equipment;
- Tort liability for false/innocuous true positives; and
- Restrictions on use of particular technologies (whether humans may be exposed to ionizing radiation for non-medical purposes, possible restrictions on millimeter wave imaging scanners, and whether equipment must be registered or technicians licensed).

Comparing Methods across Evaluation Criteria

When compared with each other across a set of criteria, inspection methods will differ. One method may be minimally intrusive, but pose more than minimal tort risks. Another may be minimally intrusive but expensive. Once the transit agency has considered both the operational and legal aspects of specific PSI methods, it may find it useful to compare particular methods across various legal and operational criteria. The criteria that the agency may want to consider include intrusiveness of the PSI, risk of liability for invasion of privacy, risk of liability for health hazards, risk of liability for false/innocuous true positives, state law requirements for certification/licensing (including whether a particular technology is legal for proposed use), effect on passenger throughput, capital cost to acquire, operational costs, maintenance costs, and training costs.

Based on the foregoing operational and legal assessments, the transit agency can determine whether it would be appropriate to deploy any PSI methods either currently or under specified future circumstances. If the agency determines that it is not appropriate to deploy any PSI methods, a determination to that effect should be included in its overall security plan. If the agency determines that it could appropriately deploy one or more PSI methods in its system, the agency should proceed to "Phase 2—Policy/Protocol Development."

Phase 2—Policy/Protocol Development

Once the transit agency has determined that it could appropriately deploy PSI methods as a measure to combat terrorism, it is highly recommended that the transit agency's PSI policy be put in writing, including a clear articulation of both the legal and operational purposes of conducting PSIs.

In order for an agency to deploy a non-suspicion-based inspection method that does not create a concern about a potential violation of Fourth Amendment rights, the risk of terrorist attack must be great enough to create a compelling government interest in deterring or detecting such an attack. It is advisable that the agency's legal analysis demonstrate the government need/danger faced, the need to proceed without individualized suspicion, and the minimal nature of the privacy intrusion created by the inspection method chosen.

It is critical to note that the purpose need not be the actual apprehension of terrorists. The New York City Container Inspection Program (CIP)—the most sweeping PSI program to date and the first to be reviewed at the federal appellate court level—was designed primarily for deterrent purposes. Carrying out inspections in an unpredictable yet routine fashion, the program design obstructs the terrorist goal of hitting predictably vulnerable targets. In other words, a deterrent effect may be obtained even though inspections are not carried out continuously, so long as they occur regularly and in patterns not predictable to someone planning an attack. TSA also emphasizes unpredictability (see www.tsa.gov/approach/unpredictability.shtm).

In addition, the policy should describe—and limit—the scope of the inspections. The risk assessment should have identified the type of threat the agency thinks is possible and wants to guard against; the scope of the inspection should relate to that threat, that is, the policy should tie inspection parameters to factors likely to deter or detect the threat. For example, if the threat requires looking for 20-pound explosives, the protocols might prohibit inspecting small bags and small pockets in big bags.

Having articulated both the purposes of conducting PSIs and the preferred PSI countermeasures to deploy, the agency should develop protocols for implementation, including indicators for PSI methods to be used in the future or under specified circumstances. For example, the agency may develop a protocol for inspecting passenger bags at various intervals of time. Intervals may ordinarily vary according to passenger traffic and available personnel, and may vary at a specified number of stations depending on station layout and operating characteristics. The protocol should specify under what conditions intervals and numbers of stations might increase.

The agency should also consider what countermeasures could be taken to rapidly respond to newly developed intelligence information or to a change in threat levels. Possible indicators include transportation-related terrorist attacks elsewhere in the world or specific intelligence regarding one of the agency's own transit systems. It is critical that selection criteria not violate applicable law concerning racial profiling. (See Appendix D for legal background.) Major issues that a transit agency may want to take into account in formulating its policy, including protocol development, follow.

Protocol Issues

Purpose of the PSI Program

Clearly the PSI program must advance a substantial government interest separate from general crime control efforts. If the inspections are too closely interwoven with general law enforcement, they could be held invalid. For example, coordination with narcotics units could be problematic. Similar concerns may exist when officers engaged in behavioral assessments pursue general law enforcement while conducting antiterrorism assessments.

Keying PSIs to articulated threat warnings or other articulated indicators (see "Contingency Plans," below) could help to differentiate them from routine law enforcement, provided that the type of threat warning is in fact related to a relatively specific danger. Similarly, employing an inspection method that targets only terrorism-related threats, such as explosives, should also help distinguish the policy from general law enforcement.

Calibrating the Inspection to Discover the Identified Threat

The scope of the inspection should be no broader than required to discover the identified threat, but must, at the same time, be broad enough to discover the identified threat. For example, assume that the identified goal of the policy is to prevent terrorists from bringing enough explosives into a system to cause significant injury or death or to prevent the breech of the hull of a moving conveyance. In such a case, the selected inspection countermeasure should be designed, if possible, to determine the likely bulk or weight of the explosives that would be required to inflict such damage, and the protocol should limit inspections to containers, or portions of containers, large enough or heavy enough to contain that quantity of explosives.

Credible Support for Program Design

It does not appear that statutory authority is required to design and implement a PSI program. However, some credible source attesting to the validity of program design is advisable. For example, evaluation by counterterrorism experts as to the effectiveness of a design aimed at deterrence could be helpful.[104] Alternatively, when agencies are considering the use of behavioral assessment, it may be advisable to ensure that the protocol is consistent with expert advice concerning the efficacy and accuracy of such assessments for identifying potential terrorists.

Implementing the Policy as Written

The PSI selected should be deployable as set forth in the policy/protocol. The resources cited should indeed be available. It is important to keep in mind that, for example, a method that can be constitutionally deployed in one area of the system may not be constitutional if deployed elsewhere.

Procedural Safeguards

There are a number of procedural safeguards that may, depending on state law, minimize the intrusiveness of the

[104] Agency counsels are urged to review MacWade v. Kelly, Docket No. 05-6754-cv (2d Cir. August 11, 2006).

inspections and thereby enhance their constitutionality. These include the following:

- Having a designated screening area—a separate, but open, clearly visible area (courts should consider that such an arrangement reduces passengers' apprehension and the stigma of being searched);
- Having at least two officers present, including a supervisor;
- Documenting all inspections; and
- Providing a complaint procedure for deviations from the protocol.

Determining the Inspection Protocol

Where the protocol is defined (at the command or line level) and how it is executed (ministerially or with discretion) will have enormous implications for its constitutionality. The inspection policies upheld in Boston and New York were defined at the command level and executed ministerially.

In order to be executed ministerially, a policy must have guidelines on what to inspect, how to inspect, and what constitutes prohibited items. This does not mean that the inspecting officers must be totally devoid of discretion, but there should be reasonable limits on any exercise of discretion. For example, the protocols could specify that different inspection methods be deployed depending on the number of passengers waiting in line. In the case of behavioral assessment, the more subjective the indicators, the greater the risk that there will be allegations of abuse of discretion, if not actual occurrences of abuse of discretion. For example, indicators such as "appears nervous" require more subjective assessment than "photographing transit system features" (which may be legitimate) or "attempts to access restricted areas."

Generally the number of, and location of, inspections may be determined daily based on the anticipated volume of passengers, DHS alerts, and specific threat intelligence. Occurrence of special events, such as political conventions, may also justify instituting inspections, varying inspection methodology, or varying inspection frequency for the duration of the event.[105] It is possible to use computer software to generate random numbers for selecting passenger inspection intervals, which enhances the randomness of the intervals. Decisions about the conduct of inspections should be made by supervisors following written policy. These decisions should then be communicated to inspecting officers.

[105] See, for example, M. Fickes, "Preventing Mass Transit Terror Attacks," *Government Security: Technology Solutions in Defense of the Homeland*," October 1, 2005. http://govtsecurity.com/mag/preventing_mass_transit/.

Inspecting People versus Inspecting Packages

In some cases, the decision about whether to inspect people or packages may be made when the PSI method is selected. However, to the extent that the selected PSI method could be deployed to inspect passengers or their packages, the transit agency should keep in mind that inspecting passengers will be considered more intrusive than searching packages and thereby may require greater justification—including, but not limited to, reasonable suspicion. Inspecting passengers, as opposed to their packages, on a nonrandomized basis may be considered profiling, and, to the extent that it focuses on the characteristics of any protected class, will be subject to intensified scrutiny.

Inspecting packages may raise some Fourth Amendment/state constitution concerns, but it is subject to lower standards than inspecting passengers. Targeting packages based on size, weight, or some other factor related to the purpose of the inspection should not have the same constitutional implications as selectively inspecting passengers.

When the policy requires baggage inspections only, the protocol could provide for exempting passengers not carrying baggage from passing through security checkpoints.

Inspection Location

Some questions about location are answered when the PSI method is selected, as some methods can be deployed only in certain locations. Nonetheless, inspection location remains an important issue in structuring the protocol. To the extent that the PSI method allows for various inspection locations, an initial decision must be made as to whether inspections will be conducted within the system or at entrances to the system only. As noted above, inspections within the system may be more difficult to conduct in a truly randomized, nonarbitrary fashion, which of course has implications for the constitutionality of the inspections and could require a different standard for justifying them. Even behavioral assessments, which are not random, may be less susceptible to challenge if they occur before passengers enter the system, or at least before they board conveyances.

Even a policy that only allows inspections at entrances to the system is likely to have selection issues, either as to location or time of day. Concerns include not creating a pattern discernible to a potential terrorist (which goes to the efficacy of the policy) and not disproportionately affecting certain segments of the population (which may raise equal protection issues, as conducting inspections may have an effect on transit service). If the threat is not confined to a particular part of the system, or time of day, the agency should examine whether the checkpoint selection is randomized except as to the objective threat. Further, as noted above, building sufficient unpredictability into the protocol is key to establishing deterrence. Clearly, the protocol must specify criteria for selecting and

changing inspection locations and not leave that decision to the inspecting officers' discretion.

Providing Adequate Notice/Opportunity to Avoid Inspection

Notice of the inspection and opportunity to avoid it will enter into an assessment of the reasonableness of the inspection. Two aspects to consider are timing, whether notice of the policy is adequate to allow people to make other plans, and prominence, whether notice is clearly visible in the system before payment is required. The protocol may provide that once passengers proceed past a certain designated point, they may no longer decline the inspection. If so, notice of that requirement should be clearly provided in advance. In addition, passengers should be provided with notice that re-entry after declining inspection is prohibited.

Secondary Inspections

The protocol should specify when an initial (apparent) presence of a prohibited substance or a behavioral assessment indicator calls for secondary inspections. Such inspections may consist of verbal questioning or more intrusive inspections, including, in some instances, searches of the passenger. The protocol should specify the conditions under which such secondary inspections occur, such as the indicators for such inspections, how the secondary inspections are to be carried out (which may be dictated by the indicators), when to request additional officers, and so forth. Secondary inspections may be a recurring issue when the PSI method is susceptible to false positives or innocuous true positives. For example, radiation pagers may react to passengers undergoing radiation treatment. In order to minimize liability, it is important not only that the protocol be clear regarding how such passengers are to be treated, but that officer training (see "Performance Monitoring" below) emphasizes the possibility of such initial results.

Invasion of Privacy

Despite the difficulty in most jurisdictions of a plaintiff mounting a successful invasion of privacy action arising from a PSI (see Appendix D), it is recommended that the protocol mandate steps to ensure against invading a passenger's privacy more than necessary to accomplish the purpose of the inspection. For example, a protocol governing visual/physical inspections by officers could direct inspecting officers not to read any material in bags selected for inspection. When the PSI method involves potentially revealing images or other sensitive information, it is recommended that the protocol specify who shall have access to the information and whether and for how long the transit agency shall retain the information. Protocols governing the use of handheld devices, which require the officer to be in close physical proximity to passengers, could include guidance for minimizing any unnecessary physical contact with passengers.

Accessibility

The PSI protocol should account for the accessibility of any technology-based inspection method. The deployment of any technology that is not accessible to disabled passengers will require the use of secondary screening to accommodate those passengers. Allowing all disabled passengers to avoid inspection because inaccessible inspection technology would not only undermine the inspection's operational effectiveness but also its legal rationale.

Other

It is further recommended that the agency develop policies for the following:

- Dealing with passengers who decline screening and attempt re-entry;
- Explaining when the inspection crosses the threshold from administrative inspection to suspicion-based search (still allowed);
- Handling the discovery of contraband; and
- Announcing threats to the public.

Contingency Plans

Transit agencies may determine that while current or immediately foreseeable circumstances do not warrant conducting PSIs, there are reasonably foreseeable future circumstances—such as changes in operations or special events—that warrant PSIs. If that is the case, it is advisable to develop contingency plans. Such plans will be similar to a current PSI policy, with less attention to operational detail and more attention to how to deploy resources rapidly. The following is a checklist for agencies developing a contingency plan:

- Identify circumstances under which PSIs would be necessary and/or advisable (e.g., attack on surface transportation anywhere in the world, attack on transportation system in the United States, preplanning surveillance detected at U.S. transportation systems, high terror alert for U.S. transportation systems, and specific intelligence about the system being analyzed);
- Prioritize inspection needs/measures that would be desirable based on operational compatibility;
- Conduct a legal analysis of desirable inspection methods;
- Finalize a list of contingency inspection methods;
- Develop protocols for conducting PSIs;
- Identify possible sources for quick deployment such as TSA, FTA, and/or a loan from another transit system; and

- Specify training that could be delivered in a cost-effective way before the need to deploy inspection.

Mitigation Measures

As indicated above, in developing its protocols, the transit agency should consider measures that will mitigate any potential legal liability. Table 7 summarizes suggested mitigation measures for the primary risks posed by various PSI methods. In all cases, training on the PSI protocol is suggested to enhance mitigation measures. Also, it is important to recognize that Fourth Amendment liability is likely to be mitigated by linking inspections to clearly articulated threats, providing adequate notice, affording the opportunity to avoid the inspections, and limiting the scope of the inspection to the threat being addressed. (See Appendix D.) Notice refers to announcing that passengers may be subject to inspection. It does not include divulging operational aspects of the program,

Table 7. Mitigation measures.

	Mitigation of intrusion	Mitigation of privacy concerns	Mitigation of claims with respect to unreasonable detention, etc.	Mitigation of health risks
Behavioral assessments	Use, to extent feasible, of objective indicators; reasonable limitations on officer's discretion; extreme caution in using racial/ethnic characteristics.	Same as for intrusion.	Same as for intrusion.	N/A
Radiation detection pagers	Not a primary risk.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Not a primary risk.
Trace detector integrated into ticket machine	Provide notice that ticket machine contains a scanner to allow passengers option of avoiding even minimally intrusive inspection.	Not a primary risk	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Non-integrated (desktop) scanner	Minimally intrusive for Fourth Amendment purposes.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Explosives detection canine	Not a primary risk.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	N/A
Visual/physical bag search	Protocols and inspection policies and procedures must be documented and followed. Inspections are based on compelling government need.	Directing officers not to read any material in passenger bags will minimize privacy claims as well as intrusiveness.	Not a primary risk.	N/A
Handheld trace detector	No additional measures.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Handheld magnetometers	Use as secondary PSI method should mitigate intrusiveness of physical approach to passenger, as there would be some grounds for suspicion.	Not a primary risk.	Not a primary risk.	Not a primary risk.
Backscatter X-ray	Conceal sensitive body areas or reduce image details. Also ensure that images are not displayed to anyone but the inspectors. Destroying images once they are reviewed for security purposes should also mitigate risk.	Conceal sensitive body areas or reduce image details. Also ensure that images are not displayed to anyone but the inspectors. Destroying images once they are reviewed for security purposes should also mitigate risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Millimeter wave imaging scanner	Not a primary risk.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Puffer portal	Not a primary risk.	Not a primary risk.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components.
Baggage X-ray	Not a primary risk.	Not a primary risk.	Not a primary risk.	Scrupulously maintain radiation components.
Z backscatter van	Avoid scanning vans with passengers.	Avoid scanning vans with passengers.	Require positive results be treated as cause for suspicion, not evidence of guilt, and process accordingly in conducting secondary screening.	Scrupulously maintain radiation components; avoid scanning vans with passengers.

such as precisely when inspections will take place or the standards the agency uses to set inspection intervals or locations. Deploying explosives detection canines also poses the risk that the canine may attack a passenger. This risk may be mitigated by appropriate training of canines and officers, as well as by certification by a recognized authority such as TSA.

It is recommended that the agency carefully evaluate its chosen mitigation measures under state law to determine if they will work in its particular circumstances and if additional mitigation measures are advisable.

Phase 3—Assessment of PSI Methods

Once the transit agency identifies PSI countermeasures deemed appropriate on operational and legal grounds, it must consider whether there are further options for deployment. For example, should the agency select canine inspections, it will have to determine whether to apply to receive assistance from the TSA for its deployment or to acquire the canines through other means. If the canines are acquired through other means, the agency will have to decide between in-house and contracted provision of services, requiring evaluation of training methods and procurement sources. Should the agency select a technology-based method, such as trace detection, it will have to evaluate different models of the equipment.

Canine Inspections

In addition to TSA, transit agencies with established canine explosives detection teams may be an excellent resource to consult on the question of whether to outsource canine inspections, training, and performance standards. See "PSI Using Canines" in Chapter 2 of this report for more information.

Issues to consider in selecting a vendor include the trainer's experience with canines and explosives, whether the canines supplied have been cross-trained for patrol and explosives detection, whether the trainer focuses exclusively on explosives detection canines (which suggests a greater degree of expertise), and whether the trainer has worked with canines in a transit environment as opposed to airport or other security environments (as differences in environments can be significant to the canine).

Canine Team Evaluation Resources

Several resources are available for those agencies interested in exploring the use of a canine explosives detection team:

- TSA's National Explosives Detection Canine Team Program (provides dog and training, www.tsa.gov/lawenforcement/programs/editorial_1886.shtm)
  - Training is located at Lackland Air Force Base in San Antonio, Texas
  - Training takes 10 weeks
  - Training includes partial funding for handler salaries, care and feeding of the canines, and veterinary costs and other costs associated with canines on teams' return to home base
- Transit agencies that have completed the TSA canine program
  - Massachusetts Bay Transportation Authority (MBTA)
  - San Francisco Bay Area Rapid Transit District (BART)
  - Southeastern Pennsylvania Transportation Authority (SEPTA)
  - Washington Metropolitan Area Transit Authority (WMATA)
  - Port Authority Trans-Hudson Corporation (PATH)
  - Chicago Transit Authority (CTA)
  - Los Angeles County Metropolitan Transportation Authority (Metro)
  - Maryland Transit Administration (MTA)
  - San Francisco Municipal Railway (Muni)
  - San Diego Trolley, Inc. (SDTI)
- Transit agencies that have non-TSA-trained canine teams
  - New York City Transit (NYCT)
  - New Jersey Transit (NJ TRANSIT)
  - Metropolitan Atlanta Rapid Transit Authority (MARTA)
  - Metropolitan Transportation Authority of Harris County (Houston METRO)
  - Niagara Frontier Transportation Authority (NFTA)
  - Tri-County Rail
  - Amtrak
- Associations
  - International Police Work Dog Association (offers certification) (www.ipwda.org)
  - North American Police Work Dog Association (offers workshops) (www.napwda.com/)
  - National Narcotics Detector Dog Association (offers certification for explosive detection) (www.nndda.org/)
- Examples of private vendors (these vendors have not been evaluated)
  - American K9 Interdiction, Inc. (www.ak9i.com/)
  - Explosive Countermeasures International, Inc. (www.nobombs.net/expl_dog.shtml)
  - Detection Support Services (www.dssbombdogs.com/)
  - Explosive Labs K-9 Services (www.xlk-9.com)
  - GSS Security Services K9 Division (www.nybombdogs.com)
  - Michael Stapleton Associates (www.mikestapleton.com/index.html)
  - Work Dogs International (www.bombdogdetection.com/index.html)
- Literature
  - *TCRP Report 86: Public Transportation Security—Volume 2: K9 Units in Public Transportation: A Guide for*

Decision Makers (includes recommendations for putting together proposals for outsourcing canine teams and sample standards)[106] (http://www.trb.org/news/blurb_detail.asp?id=900)
  - "Observations and Recommendations Regarding Training, Record Keeping, and Deployment of Explosive Detection Canine Teams" (www.fiu.edu/~ifri/Observations%20and%20Recommendations.pdf#search=%22Canine%20%2B%20%22explosive-detection%22%20%2B%20report%22)

Canine Explosives Detection Team Issues

It is recommended that agencies instituting a canine explosives detection team consider the following issues:

- Liability for injuries caused by canines
  - State dog bite laws should be reviewed
  - In-house program generally has greater liability than contracted service
  - Meeting federal certification and training standards may reduce risk of liability
  - Steps taken to establish reasonableness of canine search policy may affect liability—be sure to clearly state the authority for the program, document performance standards, and establish use-of-force and bite policies
- Constitutional
  - To preserve reasonableness of inspections under Fourth Amendment, care should be taken in associating explosives detection canines with regular law enforcement
- Standards for team qualifications
  - Trainer or vendor qualifications and accreditations
  - Dog selection policy
  - Dog breeder qualifications
  - Handler selection policy
  - General orders for canine unit
  - Reports and assignments
  - Basic training
  - In-service training
  - Substances trained to detect
- Unique canine issues
  - Feeding
  - Housing
  - Sanitation

[106] J. Balog, J. Strongin, A. Boyd, and D. C. Mitchell, *TCRP Report 86: Public Transportation Security—Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers* (Washington, DC: Transportation Research Board of the National Academies, 2002).

Equipment Assessment

If a transit agency has identified a preferred PSI method or several methods that involve the use of specific equipment, the transit agency must select specific models. As noted earlier, vendor-quoted accuracy levels and other performance levels should be viewed circumspectly. Equipment should be tested in an operational setting for a sufficient period of time to establish actual performance (end-to-end performance) as well as performance of the actual device. Factors such as vendor assistance in training should also be taken into consideration. See "PSI Technologies" in Chapter 2 and Appendix B.

Equipment Evaluation Resources

Some resources for agencies evaluating PSI technologies include the following:

- *Evaluation of a Test Protocol for Explosives Trace Detectors Using a Representative Commercial Analyzer* (NIJ Report 100-99)[107] (www.ncjrs.gov/pdffiles1/nij/178261.pdf),
- *Guide for the Selection of Commercial Explosives Detection Systems for Law Enforcement Applications* (NIJ Guide 100-99)[108] (www.ncjrs.gov/pdffiles1/nij/178913.pdf), and
- *TCRP Report 86: Public Transportation Security—Volume 6: Applicability of Portable Explosive Detection Devices in Transit Environments*[109] (http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_rpt_86v6.pdf).

Equipment Checklist

The following criteria can be used to assess competing types of technology:

- Space requirements
- Impact on passenger throughput
- Accessibility to disabled passengers
- Accuracy
  - False acceptance rate
  - False alarm rate

[107] G. A. Eiceman, C. M. Boyett, J. E. Parmeter, *Evaluation of a Test Protocol for Explosives Trace Detectors Using a Representative Commercial Analyzer*, NIJ Report 100-99, prepared for the National Institute of Justice (Washington, DC: U.S. Department of Justice, September 1999).

[108] C. L. Rhykerd, D. W. Hannum, D. W. Murray, J. E. Parmeter, *Guide for the Selection of Commercial Explosives Detection Systems for Law Enforcement Applications*, NIJ Guide 100-99, prepared for the National Institute of Justice (Washington, DC: U.S. Department of Justice, September 1999).

[109] S. G. Haupt, S. Rowshan, W. C. Sauntry, *TCRP Report 86: Public Transportation Security—Volume 6: Applicability of Portable Explosive Detection Devices in Transit Environments* (Washington, DC: Transportation Research Board of the National Academies, 2004).

- Availability (reliability)
  - Mean-time-between-failure and is calculated by using the following formula: uptime/(uptime + downtime)
  - Downtime would include critical and noncritical failures and any recalibration procedure that is needed to restart the equipment
- Cost
  - Unit cost
  - Installation
  - Life cycle
  - Operation and maintenance
  - Labor
  - Training
  - Infrastructure modification
- Maintenance requirements
- Ease of use
  - Number of personnel required for operation
  - Training required for proficiency
    - Level of complication
    - Assistance provided by manufacturer
- Portability
  - Dimensions
  - Weight
  - Typically considered portable if one person is able to transport
- Power
  - Capabilities
    - Necessity for electrical or other power sources
    - Battery needs
  - Loss recovery capability (if there is a power disruption, equipment should be able to store, retrieve, and recalibrate itself to correct setting)
  - Needs
    - Input power should have adequate voltage and frequency tolerance
    - Power and data cables should be secured and protected from tampering
    - Portable equipment should have batteries capable of extended operation
- Controls and displays
  - Access to operator controls should be secure
  - Power and device status information should be clearly displayed
  - User interface should be intuitive
- Test function (built-in test function should be activated during start-up of equipment)
- Safety (equipment should comply with all applicable safety requirements including electrical and ergonomic safety)
- Alarm capability
  - Type of alarm (audio and/or visual)
  - Effectiveness
- Detection states
  - Vapor
  - Aerosol
  - Liquid
- Start-up time (time required to set up equipment including calibration requirements, if any)
- Resistance to interferants (substances able to deactivate the detection capability of the equipment by implementing some type of countermeasure). System should also be resistant to attempts by terrorists and criminals to hide threat materials
- Substances detected (high number of detected threats increases the usefulness and cost-effectiveness of the system)
  - Types of explosives
  - Biological agents
  - Chemical agents
- Operational environment
  - Environment under which equipment is able to operate
  - Conditions that could affect detection capability include excessive moisture (rain, high humidity), temperature extremes, presence of diesel fuel, smoke, and other vapors.
- Durability (ability of the equipment to tolerate rough usage, including shock event, impact, and bumps). This is particularly relevant for frequently moved equipment
- Potential health issues
  - Equipment that emits any ionizing radiation or in any way affects health of operators or persons inspected
  - State laws governing nonmedical use of ionizing radiation equipment on people
  - State laws governing licensing of technicians to operate ionizing radiation equipment
  - State law requiring certification and subsequent inspections of ionizing radiation equipment

Once PSI methods have been determined and specific models, delivery options, etc. have been selected, the agency must consider training needs and performance standards. These will vary by PSI method.

Performance and Training

Performance Measures

Canines. Professional associations such as the International Police Work Dog Association (www.ipwda.org) and National Narcotics Detector Dog Association (www.nndda.org/) provide certification standards. TSA also provides standards. Washington State Police Canine Association provides performance standards for canine handlers (www.wspca.com/Explosive_Standards_4-23-06.pdf#search=%22Canine%20%2B%20%22explosive-detection%22%20%2B%20report%22).

Physical inspections. NYCT and NJ TRANSIT have experience with measuring performance. The Massachusetts Bay Transportation Authority and TSA have experience in training officers in behavioral assessment.

Equipment operators. TSA performance measures provide points of comparison to what may be needed in the transit environment. These measures include the following: percentage of screeners achieving a specific score on their annual recertification testing on their first attempt; the percentage of screeners scoring above the national standard level on threat image projection (TIP) performance; and the number of passengers screened, by category. As a matter of comparison, the 1996 GAO goal for airport screening was 6 passengers per minute; currently, airport screening operates at 7 to 10 passengers per minute, or 6 to 9 seconds per passenger.

Transit agencies may wish to establish standards for time to inspect per passenger. There should also be a planned system for responding to complaints or criticisms associated with the conduct of inspections. A record of the type and number of complaints received should be maintained by the agency.

Equipment standards. General performance measures for the equipment itself include the number of false negative rate/percentage of threats detected, false positive rate for innocuous–valid and innocuous–not valid materials, uptime, and average scan time. These measures are as follows:

- False positive rate, innocuous–valid materials;
- False positive rate, innocuous–not valid materials;
- Percentage of time the equipment is operational;
- Average transaction time per passenger, primary inspections; and
- Average transaction time per passenger, secondary inspections.

Other measures, such as start-up time, may be based on the assessment criteria listed in Appendix B.

A number of organizations have established, or are attempting to establish performance standards for explosives detection equipment. See, for example, *The InterAgency Board (IAB) 2005 Annual Report and 2006 Standardized Equipment List* (SEL) (www.iab.gov/download/AnnualReport2005.pdf#search=%22Canine%20%2B%20%22explosive-detection%22%20%2B%20report%20%2B%20%22performance%20standard%22%22).

In addition, FAA standards for EDSs can be used. The National Research Council has made numerous recommendations at the behest of the FAA on the certification of EDSs and the verification of performance levels of new and existing systems; these recommendations can be applicable to transit systems.

The recommendations include configuration management guidance. Configuration management involves change control and documentation and ensures that any changes made to the equipment are evaluated before implementation and then tracked so that the configuration of the equipment is known at all times. Performance verification tests the equipment to ensure that performance does not degrade due to the changes that have been made.

According to *Configuration Management and Performance Verification of Explosives-Detection Systems*:

> A quality system that adheres to quality standards, such as the ISO 9000, is recommended. The system should have the following attributes:
>
> - A definition of the critical parameters and the tolerances, procedures, and processes to be monitored
> - Documented evidence of an internal quality system
> - A definition of the methods for controlling and verifying changes to procedures and processes
> - A definition of an internal audit program
> - A provision for a third-party audit of conformance with the quality system.[110]

Configuration Management and Performance Verification of Explosives-Detection Systems recommends that the FAA ensure that the equipment is the product of an implemented and documented manufacturing quality system. Also, subsequent units must be produced according to the same quality. It is recommended that the FAA have its own quality system for pre-certification, certification testing, standards development and maintenance, and testing for maintaining certification. Each manufacturer should receive a periodic audit including a configuration audit.[111]

In order to make changes to the equipment, configuration control boards would be established to determine which changes should be implemented and the implementation and testing conditions that will be imposed.[112]

The panel for *Configuration Management and Performance Verification of Explosives-Detection Systems* recommended seven types of testing:

- Precertification to determine if the technology is ready for certification testing;
- Certification to determine if the technology performance is at certification level;
- Qualification to verify the performance of a unit to qualify for deployment (it would take place at the manufacturing site);

[110] Panel on Technical Regulation of Explosives Detection Systems, Commission on Engineering and Technical Systems, National Materials Advisory Board; *Configuration Management and Performance Verification of Explosives-Detection Systems*; NMAB-482-3 (Washington, DC: National Research Council, National Academy Press, 1998) 47.
[111] Ibid., 48.
[112] Ibid., 40.

- Verification to verify the performance of a deployed unit (it would be performed in the airport);
- Monitoring to verify critical system parameters (monitoring would be done at specified intervals using test articles to ensure that unit performance is unchanged); and
- Self-diagnosis to verify that subsystem parameters are operating according to specifications.[113]

Standard sets of bags are used for testing purposes—one with explosives to measure detection performance and another without explosives to measure false alarm rates. Other types of bags are also used to test specific equipment models.[114]

According to *Configuration Management and Performance Verification of Explosives-Detection Systems*:

> For trace detection devices, a performance verification testing protocol would ideally consist of the following:
>
> - Sample collection—determines if, during normal operation, the operators adequately sample simulated carry-on luggage that has known amounts of explosives placed on specific areas of the luggage.
> - Sample transfer—determines the efficiency with which the sample collection techniques transfer the material for detection from a surface known to be contaminated with a known amount of explosive.
> - Sample analysis—determines if the trace detection device adequately maintains the required detection limit while functioning continuously.[115]

Training Needs

In the transit industry, the development of security training standards and a certification and recertification system are essential. Consistency of security training content and quality and appropriate and effective training delivery mechanisms are needed to maintain the highest levels of competence and preparedness among transit personnel. A system of certification and oversight is also important in ascertaining that the expected level of learning has taken place for each transit employee. Recertification, along with refresher training, will provide transit personnel with up-to-date security-related information and motivate personnel to keep using their knowledge of applicable security-enhancing techniques. Additional measures to ensure continued operationalization of the techniques can be taken by transit agencies, including the covert observation of transit staff and announced and unannounced exercises.

The absence of standards and a certification system creates additional challenges for transit agencies in determining what kind of training to provide to their personnel, how much training to deliver, and the methods of providing the instruction. Transit agencies may look at training programs for airport screeners, maritime workers, and commercial drivers for guidance in establishing appropriate standards. In addition, transit agencies may look to other transit agencies that have successfully established training programs.

In addition, National Incident Management Systems (NIMS) and Incident Command System training would provide a thorough working knowledge of the communications procedure, chain of command, and protocol during major incidents.

Training needs are addressed below. Training needs that apply generally are listed first, and specific needs based on the inspection method follow.

General training needs. In general, inspection personnel will need training in the following:

- Customer selection procedure;
- Response to alarm;
- Secondary inspection procedures;
- Response to apparent discovery of prohibited items;
- Response to discovery of other contraband;
- Recordkeeping procedures; and
- Customer relations training, including communicating the purpose of PSIs to customers and addressing typical questions.

Practice runs are essential. Written exams can be used to test trainees' knowledge of the training material. Performance monitoring is also important in determining a trainee's understanding and whether or not a trainee has been able to put course materials into operation. (See "Performance Monitoring" below.)

Canines. If the canine team is in house, there will be initial training needs for both the officers and the dogs, which can be met by working with TSA, commercial vendors, or possibly other transit agencies that have experienced teams. TSA training takes 10 weeks on site at the TSA facility. (See "Canine Team Evaluation Resources.") It may take several weeks for the trainer and canine to become accustomed to each other. TSA training may need to be supplemented with additional in-house or contracted-out training focusing on a specific transit environment because TSA training is geared toward the airport environment. The program should include dog care and handling guidance and customer relations guidance, including the steps to be taken if a customer displays anxiety or if the dog becomes agitated because of the

[113] Ibid., 35.

[114] Ibid., 43.

[115] Ibid., 47.

presence of another dog. Once trained, the team will need to continue in-service training and also conduct training exercises to maintain proficiency and certification.

Officers conducting physical inspections. In addition to the general requirements noted above, officers conducting visual/physical bag inspections will need to be trained on the protocol for conducting safe inspections and on inspection procedures.

Personnel conducting behavioral assessments. In addition to the general requirements noted above, personnel conducting behavioral assessments will need to be trained on the protocol for behavioral analysis, with an emphasis on avoiding racial profiling unless specifically allowed under protocol. Nonsecurity staff conducting behavioral assessments will need to be trained in when and how to call for security personnel.

Equipment. In addition to general requirements noted above, operators will need to be trained to operate the equipment. Training on operating the equipment is usually conducted by the manufacturer. Because there are no existing transit security training standards, vendor training and refresher training are especially important. Different technologies and equipment models will require different types of training; for instance, trace detection using the swab method will require knowledge of the prime areas where explosives residue may be found. The training standards for airport screeners are a useful point of reference for determining the amount of equipment training necessary for transit screening equipment operators: airport screeners must undergo 40 hours of classroom instruction, 60 hours of on-the-job training, 3 hours (on average) per week of refresher training, and remedial training if an operational test is failed. Licensing may also be required.

Equipment operators will need to be assessed. Once again, the standards for airport screeners can be instructive: airport screeners are subject to proficiency reviews, covert testing, and use of the TIP system.

Technicians will need to be trained to maintain equipment. Training on maintaining the equipment is usually conducted by the manufacturer. Because there are no existing transit security training standards, vendor training and refresher training are especially important. Equipment should be monitored for number of breakdowns and other reliability issues.

Performance Monitoring

Covert testing is an important aspect of performance monitoring. While the percentage or number of deterred attacks can never be measured, the covert use of realistic threat simulants can be used to monitor the performance of transit security personnel. Related measures include the number of covert tests conducted and the results of covert tests (the number of false negatives as a percentage of threats detected).

Covert observations of transit security personnel are also recommended. Weak performance may be corrected through additional training or discussions with the personnel. Measures that can be generated from the observations include the number of security-related violations by PSI staff/officers (an example of a security-related violation that may also be a procedural violation is disregarding an alarm and not performing secondary inspections when warranted) and the number of procedural violations by PSI staff/officers (an example of a procedural violation is disregarding random number criterion).

To ensure that sufficient training has occurred, training-related measures include training hours per PSI staff/officer and scores obtained on written exams and trial runs.

Customer surveys and complaint analysis may assist agencies in determining the effectiveness of their customer relations training programs and the performance of individual security personnel. The following measures may be useful:

- Number of complaints (total, and per transit staff member);
- Number of commendations (total, and per transit staff member); and
- Customer satisfaction (overall, and specifically with the PSI program).

To ensure that racial profiling is not taking place, records of the ethnicities of searched passengers may be examined for irregularities.

In addition, to ensure the efficiency of the PSI process, records of the number of passengers being screened should be examined.

APPENDIXES

The following appendixes have been published as *TCRP Web-Only Document 38* and are available in on the TRB website at http://www.TRB.org/SecurityPubs:

- Appendix A: PSI Technologies
- Appendix B: Technology Assessment Criteria and Field Tests
- Appendix C: Aviation Screening
- Appendix D: Legal Implications of Performing Passenger Security Inspections
- Appendix E: Contact List

Abbreviations and acronyms used without definitions in TRB publications:

AAAE	American Association of Airport Executives
AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
ACI–NA	Airports Council International–North America
ACRP	Airport Cooperative Research Program
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	Air Transport Association
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
NASA	National Aeronautics and Space Administration
NASAO	National Association of State Aviation Officials
NCFRP	National Cooperative Freight Research Program
NCHRP	National Cooperative Highway Research Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
SAE	Society of Automotive Engineers
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century (1998)
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation