

Transit Security Update

DETAILS

152 pages | | PAPERBACK

ISBN 978-0-309-41881-2 | DOI 10.17226/23058

AUTHORS

BUY THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at NAP.edu and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

TCRP

SYNTHESIS 80

TRANSIT
COOPERATIVE
RESEARCH
PROGRAM

Transit Security Update

Sponsored by
the Federal
Transit Administration



A Synthesis of Transit Practice

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

TCRP OVERSIGHT AND PROJECT SELECTION COMMITTEE*

CHAIR

ROBERT I. BROWNSTEIN
AECOM Consult, Inc.

MEMBERS

ANN AUGUST
Santee Wateree Regional Transportation Authority

JOHN BARTOSIEWICZ
McDonald Transit Associates

MICHAEL BLAYLOCK
Jacksonville Transportation Authority

LINDA J. BOHLINGER
HNTB Corp.

RAUL BRAVO
Raul V. Bravo & Associates

GREGORY COOK
Veolia Transportation

TERRY GARCIA CREWS
StarTran

NATHANIEL P. FORD, JR.
SF Municipal Transportation Agency

KIM R. GREEN
GFI GENFARE

JILL A. HOUGH
North Dakota State University

ANGELA IANNUZZIELLO
ENTRA Consultants

JOHN INGLISH
Utah Transit Authority

JEANNE W. KRIEG
Eastern Contra Costa Transit Authority

DAVID A. LEE
Connecticut Transit

CLARENCE W. MARSELLA
Denver Regional Transportation District

GARY W. MCNEIL
GO Transit

MICHAEL P. MELANIPHY
Motor Coach Industries

FRANK OTERO
PACO Technologies

KEITH PARKER
Charlotte Area Transit System

JEFFREY ROSENBERG
Amalgamated Transit Union

MICHAEL SCANLON
San Mateo County Transit District

BEVERLY SCOTT
Metropolitan Atlanta Rapid Transit Authority

JAMES S. SIMPSON
FTA

JAMES STEM
United Transportation Union

FRANK TOBEY
First Transit

EX OFFICIO MEMBERS

WILLIAM W. MILLAR
APTA

ROBERT E. SKINNER, JR.
TRB

JOHN C. HORSLEY
AASHTO

THOMAS J. MADISON, JR.
FHWA

TDC EXECUTIVE DIRECTOR

LOUIS SANDERS
APTA

SECRETARY

CHRISTOPHER W. JENKS
TRB

*Membership as of November 2008.

TRANSPORTATION RESEARCH BOARD 2009 EXECUTIVE COMMITTEE*

OFFICERS

Chair: *Debra L. Miller, Secretary, Kansas DOT, Topeka*
Vice Chair: *Adib K. Kanafani, Cahill Professor of Civil Engineering, University of California, Berkeley*
Executive Director: *Robert E. Skinner, Jr., Transportation Research Board*

MEMBERS

J. BARRY BARKER, *Executive Director, Transit Authority of River City, Louisville, KY*
ALLEN D. BIEHLER, *Secretary, Pennsylvania DOT, Harrisburg*
JOHN D. BOWE, *President, Americas Region, APL Limited, Oakland, CA*
LARRY L. BROWN, SR., *Executive Director, Mississippi DOT, Jackson*
DEBORAH H. BUTLER, *Executive Vice President, Planning, and CIO, Norfolk Southern Corporation, Norfolk, VA*
WILLIAM A.V. CLARK, *Professor, Department of Geography, University of California, Los Angeles*
DAVID S. EKERN, *Commissioner, Virginia DOT, Richmond*
NICHOLAS J. GARBER, *Henry L. Kinnier Professor, Department of Civil Engineering, University of Virginia, Charlottesville*
JEFFREY W. HAMIEL, *Executive Director, Metropolitan Airports Commission, Minneapolis, MN*
EDWARD A. (NED) HELME, *President, Center for Clean Air Policy, Washington, DC*
WILL KEMPTON, *Director, California DOT, Sacramento*
SUSAN MARTINOVICH, *Director, Nevada DOT, Carson City*
MICHAEL D. MEYER, *Professor, School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta*
MICHAEL R. MORRIS, *Director of Transportation, North Central Texas Council of Governments, Arlington*
NEIL J. PEDERSEN, *Administrator, Maryland State Highway Administration, Baltimore*
PETE K. RAHN, *Director, Missouri DOT, Jefferson City*
SANDRA ROSENBLOOM, *Professor of Planning, University of Arizona, Tucson*
TRACY L. ROSSER, *Vice President, Corporate Traffic, Wal-Mart Stores, Inc., Bentonville, AR*
ROSA CLAUSELL ROUNTREE, *Consultant, Tyrone, GA*
HENRY G. (GERRY) SCHWARTZ, JR., *Chairman (retired), Jacobs/Sverdrup Civil, Inc., St. Louis, MO*
C. MICHAEL WALTON, *Ernest H. Cockrell Centennial Chair in Engineering, University of Texas, Austin*
LINDA S. WATSON, *CEO, LYNX—Central Florida Regional Transportation Authority, Orlando*
STEVE WILLIAMS, *Chairman and CEO, Maverick Transportation, Inc., Little Rock, AR*

EX OFFICIO MEMBERS

THAD ALLEN (Adm., U.S. Coast Guard), *Commandant, U.S. Coast Guard, Washington, DC*
REBECCA M. BREWSTER, *President and COO, American Transportation Research Institute, Smyrna, GA*
PAUL R. BRUBAKER, *Research and Innovative Technology Administrator, U.S.DOT*
GEORGE BUGLIARELLO, *President Emeritus and University Professor, Polytechnic Institute of New York University, Brooklyn; Foreign Secretary, National Academy of Engineering, Washington, DC*
SEAN T. CONNAUGHTON, *Maritime Administrator, U.S.DOT*
CLIFFORD C. EBLY, *Acting Administrator, Federal Railroad Administration, U.S.DOT*
LEROY GISHI, *Chief, Division of Transportation, Bureau of Indian Affairs, U.S. Department of the Interior, Washington, DC*
EDWARD R. HAMBERGER, *President and CEO, Association of American Railroads, Washington, DC*
JOHN H. HILL, *Federal Motor Carrier Safety Administrator, U.S.DOT*
JOHN C. HORSLEY, *Executive Director, American Association of State Highway and Transportation Officials, Washington, DC*
CARL T. JOHNSON, *Pipeline and Hazardous Materials Safety Administrator, U.S.DOT*
DAVID KELLY, *Acting Administrator, National Highway Traffic Safety Administration, U.S.DOT*
SHERRY E. LITTLE, *Acting Administrator, Federal Transit Administration, U.S.DOT*
THOMAS J. MADISON, JR., *Administrator, Federal Highway Administration, U.S.DOT*
WILLIAM W. MILLAR, *President, American Public Transportation Association, Washington, DC*
ROBERT A. STURGELL, *Acting Administrator, Federal Aviation Administration, U.S.DOT*
ROBERT L. VAN ANTWERP (Lt. Gen., U.S. Army), *Chief of Engineers and Commanding General, U.S. Army Corps of Engineers, Washington, DC*

*Membership as of January 2009.

TRANSIT COOPERATIVE RESEARCH PROGRAM

TCRP SYNTHESIS 80

Transit Security Update

A Synthesis of Transit Practice

CONSULTANT

YUKO NAKANISHI

Nakanishi Research and Consulting, LLC

Rego Park, New York

SUBJECT AREAS

Public Transit

Research Sponsored by the Federal Transit Administration in Cooperation
with the Transit Development Corporation

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.

2009

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 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 Academy of Sciences, 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 TRB. 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 SYNTHESIS 80

Project J-7, Topic SF-13

ISSN 1073-4880

ISBN 978-0-309-09824-3

Library of Congress Control Number 2008910980

© 2008 Transportation Research Board

COPYRIGHT PERMISSION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

Cooperative Research Programs (CRP) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply TRB, AASHTO, FAA, FHWA, FMCSA, FTA, or Transit Development Corporation endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from CRP.

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 Transit Development Corporation, the National Research Council, 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 Transit Development Corporation, the National Research Council, 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 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. 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

TCRP COMMITTEE FOR PROJECT J-7

CHAIR

DWIGHT A. FERRELL
Metropolitan Atlanta Rapid Transit Authority

MEMBERS

DEBRA W. ALEXANDER
Capital Area Transportation Authority, Lansing, MI

MARK W. FURHMANN
Metro Transit, Minneapolis–St. Paul, MN

ROBERT H. IRWIN
Consultant, Calgary, AB, Canada

DONNA KELSAY
San Joaquin Regional Transit District, Stockton, CA

PAUL J. LARROUSSE
Rutgers, The State University of New Jersey, New Brunswick

WADE LAWSON
South Jersey Transportation Authority, Atlantic City

DAVID LEE
Connecticut Transit, Hartford

FRANK T. MARTIN
PSB&J, Tallahassee, FL

DAVID PHELPS
LTK Engineering Services, Moneta, VA

HAYWARD M. SEYMORE, III
Q Straint, University Place, WA

PAM WARD
Ottumwa Transit Authority, Ottumwa, IA

JOEL R. WASHINGTON
Washington Metropolitan Area Transit Authority, Washington

FTA LIAISON

LISA COLBERT
Federal Transit Administration

TRB LIAISON

PETER SHAW
Transportation Research Board

Cover figure: MBTA Transit Police Department SWAT Team Drill (*Courtesy: MBTA*).

COOPERATIVE RESEARCH PROGRAMS STAFF

CHRISTOPHER W. JENKS, *Director, Cooperative Research Programs*

CRAWFORD F. JENCKS, *Deputy Director, Cooperative Research Programs*

GWEN CHISHOLM SMITH, *Senior Program Officer*

EILEEN DELANEY, *Director of Publications*

TCRP SYNTHESIS STAFF

STEPHEN R. GODWIN, *Director for Studies and Special Programs*

JON M. WILLIAMS, *Program Director, IDEA and Synthesis Studies*

DONNA L. VLASAK, *Senior Program Officer*

DON TIPPMAN, *Editor*

CHERYL KEITH, *Senior Program Assistant*

TOPIC PANEL

COLIN H. ALTER, *Federal Emergency Management Agency*

JOEDY W. CAMBRIDGE, *Transportation Research Board*

DWIGHT A. FERRELL, *Metropolitan Atlanta Rapid Transit Authority*

GARY GEE, *San Francisco Bay Area Rapid Transit District*

VICKI GLENN, *Vanasse Hangen Brustlin, Inc., Vienna, VA*

BRIAN HEANUE, *Washington Metropolitan Area Transit Agency*

CHRISTOPHER A. KOZUB, *Rutgers, The State University of New Jersey*

PAUL MACMILLAN, *Massachusetts Bay Transportation Authority*

RONALD J. MASCIANA, *Metropolitan Transportation Authority*

HARRY SAPORTA, *PB World, Washington, D.C*

RICHARD GERHART, *Federal Transit Administration (Liaison)*

GREG HULL, *American Public Transportation Association (Liaison)*

FOREWORD

Transit administrators, engineers, and researchers often face problems for which information already exists, either in documented form or as undocumented experience and practice. This information may be fragmented, scattered, and unevaluated. As a consequence, full knowledge of what has been learned about a problem may not be brought to bear on its solution. Costly research findings may go unused, valuable experience may be overlooked, and due consideration may not be given to recommended practices for solving or alleviating the problem.

There is information on nearly every subject of concern to the transit industry. Much of it derives from research or from the work of practitioners faced with problems in their day-to-day work. To provide a systematic means for assembling and evaluating such useful information and to make it available to the entire transit community, the Transit Cooperative Research Program Oversight and Project Selection (TOPS) Committee authorized the Transportation Research Board to undertake a continuing study. This study, TCRP Project J-7, “Synthesis of Information Related to Transit Problems,” searches out and synthesizes useful knowledge from all available sources and prepares concise, documented reports on specific topics. Reports from this endeavor constitute a TCRP report series, *Synthesis of Transit Practice*.

This synthesis series reports on current knowledge and practice, in a compact format, without the detailed directions usually found in handbooks or design manuals. Each report in the series provides a compendium of the best knowledge available on those measures found to be the most successful in resolving specific problems.

PREFACE

*By Donna Vlasak
Senior Program Officer
Transportation
Research Board*

This synthesis updates an earlier synthesis and addresses terrorism that had not been included in the original study, along with ordinary crime. Counterterrorism and anti-crime security measures and practices, crime and security incident trends, and other related issues, including major issues and obstacles to security and policing management are covered.

This report was accomplished through a review of the relevant literature in the field and surveys of transit agencies. Interviews were conducted with industry experts, along with a review of the National Transit Database.

Yuko Nakanishi, Nakanishi Research and Consulting, LLC, Rego Park, New York, collected and synthesized the information and wrote the paper, under the guidance of a panel of experts in the subject area. The members of the Topic Panel are acknowledged on the preceding page. This synthesis is an immediately useful document that records the practices that were acceptable within the limitations of the knowledge available at the time of its preparation. As progress in research and practice continues, new knowledge will be added to that now at hand.

CONTENTS

1	SUMMARY
5	CHAPTER ONE INTRODUCTION
	The Terrorist Threat, 5
	Project Background and Objectives, 8
	Report Organization, 9
10	CHAPTER TWO PASSENGER PERCEPTION OF CRIME AND TERRORISM
	Passenger Perception of Crime, 10
	Passenger Perception of Terrorism, 10
	Performance Measures, 10
	Crime and Security Data, 12
	Crime Trends, 13
	Suspicious Activity, 14
	Data Issues, 14
	Characteristics of Crime Victims and Offenders, 15
16	CHAPTER THREE SECURITY MEASURES
	Technology Issues, 17
	Access Control, 18
	Crime Prevention through Environmental Design, 19
	Patrols, Plainclothes, and Visual Surveillance, 22
	Video Surveillance, 22
	Passenger Security Inspections, 24
	Threat Detection Technologies, 25
	Tunnel Security, 26
	Other Measures, 26
	Cyber Security, 27
	Communications Security and Redundancy, 28
	Interoperable Communications, 28
	Collaborative Transportation Imagery Project, 28
29	CHAPTER FOUR SECURITY PRACTICES
	Security and Policing Management, 29
	Security Resource Allocation, 30
	Risk Management and Security Planning, 30
	Regional Coordination, Cooperative Relationships, and Intelligence Information, 31
	Customer Outreach, Education, Training, and Awareness, 32
	Employee Security and Policing Training, 33
	Youth Outreach Strategies, 35
	Evaluation Procedures, Drills, and Covert Testing, 35
	Ferry Security, 36
37	CHAPTER FIVE CONFLICT MITIGATION STRATEGIES
	Techniques, 38
	Information Sources, 39
	Prevention Strategies, 39

40	CHAPTER SIX CASE STUDIES
	Massachusetts Bay Transportation Authority (Boston, Massachusetts), 40
	Bay Area Rapid Transit (San Francisco, California), 45
	Capital District Transportation Authority (Albany, New York), 52
	Capital Metro (Austin, Texas), 55
	Washington Metropolitan Area Transit Authority (Washington, D.C.), 58
60	CHAPTER SEVEN CONCLUSIONS
	Project Findings, 60
	Transit Security Practices, 60
	Problems and Obstacles, 63
	Research Needs, 64
66	ABBREVIATIONS AND ACRONYMS
68	REFERENCES
71	BIBLIOGRAPHY
74	GLOSSARY
84	APPENDIX A SUPPORTING MATERIAL
87	APPENDIX B LITERATURE REVIEW
114	APPENDIX C SURVEY QUESTIONNAIRE
132	APPENDIX D LIST OF SURVEY RESPONDENTS
133	APPENDIX E SUMMARY OF SURVEY RESULTS

TRANSIT SECURITY UPDATE

SUMMARY This report, an update of the original *TCRP Synthesis of Transit Practice 21: Improving Transit Security* (1997), addresses terrorism, which was not included in the original study along with ordinary crime. Counterterrorism and anticrime security measures and practices, crime and security incident trends, and other related issues are covered in this report. Major issues and obstacles to security and policing management, as well as further research needs, have been identified and presented. The key elements of this Synthesis study include a survey of 120 transit agencies, with a 38% response rate, case studies, and a literature review along with input from industry experts and National Transit Database (NTD) analysis.

Since the publication of the last report in 1997, significant improvements have been made to mitigate ordinary crime, and significant progress has been made to secure transit systems from terrorism. After September 11, 2001 (9/11), securing public transportation systems against the terrorist threat became an important and complex issue for U.S. transit operators and continues to be a prime concern of both domestic and international transit operators. For many decades, transit systems outside of the United States have been a target of terrorist activity, which has resulted in significant losses of life, injuries, infrastructure damage, disruptions to transit service, and economic losses to the affected regions.

With almost 10 billion public transportation trips taken in 2006, U.S. transit systems offer many important benefits to their ridership, the community and its residents, regional and state economies, and the environment. The following characteristics of transit systems and their assets—vehicles, infrastructure, communications, and personnel—make them especially vulnerable to terrorist attacks:

- Large numbers of passengers contained within enclosed spaces,
- Ease of access to the general public,
- Symbolic nature of transit terminals,
- Economic significance to a region, and
- Psychological impact on a community and even the nation.

Synthesis survey results revealed that the terrorist threats of primary concern to multimodal, rail-only, and ferry systems were explosives, chemical and biological threats, hijackings and shootings, and sabotage. The terrorist threats of primary concern to bus agencies were hijackings, shootings, explosives, and sabotage. Transit agencies are well aware of many other possible terrorist threats, such as radiological attacks, cyber crime, and transit vehicles used as weapons, but these threats are considered to be of secondary importance.

To counter these threats and better protect their transit systems, transit agencies have invested more than \$2.5 billion on security and emergency preparedness programs and technologies to better protect their customers and systems, and have made changes to their security and policing management techniques to address terrorism as well as ordinary crime. The primary post-9/11, changes in security practices include the implementation

of Transit Watch, or a similar employee and passenger awareness and outreach program; provision of security training to frontline employees and counterterrorism training to police and security personnel. Transit agencies have increased the number and hours of security personnel; conducted threat and vulnerability assessments; received intelligence information from federal agencies; and increased local and regional coordination and outreach efforts through counterterrorism committees and intelligence information sharing with local responders and neighboring transit agencies. Human resource practices have changed, particularly regarding background checks. The guidance on background checks most recently issued by the TSA helps transit agencies conduct more robust background checks and makes the process more consistent across agencies by identifying the factors to consider and the recommended scope of the checks and procedures. In terms of planning, many transit agencies have up-to-date security and emergency management plans, including a Continuity-of-Operations Plan.

According to survey respondents, post-9/11 security investments have had a positive impact on terrorism deterrence and detection capabilities, general crime mitigation, and the public, passenger, and employee perception of security. Agencies report that their public outreach efforts have contributed to increased passenger and employee awareness, improved employee preparedness, and increased security in terms of both deterrence and detection. The greatest obstacle in security and policing management was reported to be the lack of resources to implement desired security measures.

The following effective counterterrorism practices, anticrime practices, and practices applicable to both counterterrorism and anticrime were identified by the Synthesis survey, case studies, literature review, and input from industry experts.

- Counterterrorism Practices
 - *Identity management* prevents unauthorized physical access of sensitive transit facility areas or virtual access to agency networks and its databases.
 - *Intelligence information* is an important security practice and includes gathering and identifying agency-specific, actionable information; analyzing intelligence information to determine its reliability and relevance to a particular agency; and sharing information. Intelligence sharing between the agencies and their federal, state, and local partners is further facilitated through TSA's Mass Transit Security Information Network's interagency communication and information-sharing protocols. The Homeland Security Information Network Public Transit Portal has been integrated into this network to provide a one-stop security information sources and outlets for security advisories, alerts, and notices.
 - *Passenger Security Inspections (PSIs)*, including random baggage inspections, canine patrols, and behavioral assessment, are practiced by several agencies. Behavioral assessment practiced by both transit officers and transit employees is a relatively cost-effective PSI method that is readily deployable and effectively expands the reach of the police force.
 - *Public education and outreach campaigns* inform passengers about the importance of reporting suspicious activities, persons, or items, and enlist them to become the eyes and ears of the agency. Public education and outreach efforts are being enhanced further by such programs as Play Your Part through which TSA, in joint efforts with mass transit and passenger rail agencies, advances security awareness among the traveling public as well as public and private partners. TSA Transportation Security Inspectors–Surface, supported by the Mass Transit Division, form partnerships with the agencies in high-visibility public awareness campaigns, altering the normal activities at terminals or stations and enhancing passenger awareness of and vigilance for suspicious activities and items as possible indicators of terrorist preparations for, or execution of, an attack.

- *Regional coordination* among transit agencies, emergency responders, local departments of transportation, and other relevant agencies enhances security initiatives and agency preparedness.
- *Training transit police and security personnel* enhances the preparedness of transit systems. Initially, a range of security training materials for transit workers was developed through programs sponsored by the FTA to assist transit agencies. To further assist these agencies, TSA, in consultation with FTA and other public and private security partners, developed and published the Mass Transit Security Training Program. This program presented on TSA's website provides detailed guidelines for mass transit and passenger rail agencies to develop and implement security training programs, and specifies the subject areas in which particular categories of employees should receive training. These guidelines are implemented under the Transit Security Grant Program. Course options include programs funded by FTA/TSA (transit-specific terrorism prevention and response) and the Federal Emergency Management Agency (general terrorism prevention and response).
- *Trace detection technology* detects residues from explosives and is available in portable devices suitable for transit environments. *Radiological pagers* are used by transit agencies to detect nuclear threats. *Chemical detectors* are being tested at major transit systems. *Biological threat detectors* are also being developed for use in transit systems.
- Anticrime Practices
 - *Codes of conduct* are rules that passengers must follow within the transit system. Enforcing codes of conduct can assist agencies in detecting and deterring crime and in enhancing the perception of security within their transit systems.
 - *Crime statistics maps* are valuable visual tools for transit police and are useful for the strategic deployment of officers. Providing passengers with access to up-to-date crime data through interactive, user-friendly crime statistics maps increases their perception of control over their transit trip.
 - *Plainclothes officers* within the transit system are used to catch perpetrators in the act of committing a crime. The use of *unmarked vehicles* is also an effective practice in transit park-and-ride or other parking facilities.
 - *School outreach* programs enlist the assistance of schools to enforce passenger codes of conduct and discourage disorderly behavior in juvenile populations.
 - *Training bus drivers* in customer relations, conflict mitigation, and gang-related violence provides bus drivers with increased confidence and knowledge in dealing with the public.
- Counterterrorism and Anticrime Practices
 - *Crime Prevention through Environmental Design* principles enhance security by hardening transit facilities and vehicles and making the transit environment less conducive to criminals.
 - *The Collaborative Transportation Imagery Project* is a joint endeavor by TSA and its partner agencies to produce detailed mapping and interactive imagery of key assets and systems. The project informs and enhances the quality of operational activities and addresses threats and security incidents, security plans, training programs, and exercises. The product, provided on digital disc, incorporates multiple types of imagery, satellite maps, schematics, and related materials to provide a comprehensive view of the transit system, detailing significant infrastructure and security apparatus.
 - *Transit police and security personnel*, which include high-visibility patrols and specialized counterterrorism teams, perform sweeps of transit terminals, stations, and trains and buses. These efforts enhance the visibility of transit employees, which is an effective security practice.

- *TSA's Visible Intermodal Prevention and Response* teams have been deployed at hundreds of transit systems throughout the country. These teams augment security in the systems, expanding the agencies' capabilities to implement random, unpredictable security activities to deter both terrorism and crime.
 - *Video technology* has multiple uses, and its scalable, analytical capability has been rapidly increasing. Recordings of incidents and accidents can be used to identify perpetrators, verify crime occurrences, and provide postincident analysis. Criminal or atypical behaviors can be identified by intelligent video technology. Video cameras can be linked with other detection systems such as intrusion detectors and chemical detectors.
- Other Findings
 - *Crime trends*: According to the Bureau of Justice Statistics, a nationwide decline in crime and a concomitant decrease in transit crime were seen in the United States starting in the mid-1990s. Transit crime dropped significantly from 1997 to 2002 and then began to plateau. Concerns were raised by industry experts about the reliability and accuracy of NTD data; however, the following conclusions can be made based on the NTD data analysis: There were many more minor than serious crimes within public transit systems, and the numbers of the most violent crimes—homicide and rape—were extremely low. For serious Part I offenses, the most problematic was theft, and for less serious Part II offenses, the most predominant was fare evasion, with a majority of the citations occurring on light rail systems.
 - *Major incidents, suspicious activity, and threats*: Transit agencies report an increase in suspicious activities, persons, and items in the period after 9/11. In general, these reports have diminished and have plateaued over the past few years.
 - *Passenger perception of crime and terrorism*: Although violent crimes in transit systems are generally low in actual numbers, public perception is different. Media coverage and the entertainment industry intensify public fears. Minor crimes and disorder (e.g., unruly juveniles) affect passenger perceptions even if the actual consequences of these incidents are minimal. These findings may influence how agencies measure security, because of the disparity between actual and perceived levels of crime. Regarding the perception of terrorism, public perception differs greatly between the east and west coasts, with east coast passengers more aware of the threat of terrorism and tolerant of terrorism-related security measures.
 - *Performance metrics*: Performance metrics are important in monitoring the performance of security systems, practices, and measures as well as the overall security of a transit system. Metrics can be used to communicate the benefits of security to management and the general public and convince decision makers as to the value and relevance of security investments.

CHAPTER ONE

INTRODUCTION

Before September 11, 2001 (9/11), a foreign terror attack on U.S. soil was deemed unlikely by many and unimaginable by others. On 9/11, transportation vehicles were turned into weapons that killed thousands of innocent civilians and emergency responders. 9/11 became the defining moment when the face of transit security changed and counterterrorism became one of the highest priorities of transit management. U.S. transit agencies, with FTA support, took immediate measures to enhance the security of their systems.

The key actions taken by the United States after 9/11—to establish the TSA and DHS, reorganize the intelligence community and create a Director of National Intelligence—have strengthened interagency collaboration and the government architecture against terrorism. Before 9/11, the FTA and the FRA had the primary federal responsibility for transit security. In response to the 9/11 attacks, TSA was created by Congress through an enactment of the Aviation and Transportation Security Act. Upon its creation in November 2001, TSA undertook primary responsibility for protecting all modes of transportation, including public transportation systems. Although originally within the U.S.DOT, TSA and other agencies were transferred to DHS after passage of the Homeland Security Act of 2002.

Countering terrorism threats has been a major challenge for transit agencies, because it requires a transfer of skill sets and a knowledge base along with specialized counterterrorism knowledge. Terrorists have different objectives and motives than criminals. They seek to maximize deaths, injuries, and property damage. The frequency and consequences of criminal and terrorist activity are disparate as well. Less serious crimes such as fare evasion and theft occur daily, pervade the entire system, and increase passenger perception of fear. Terrorist attacks occur infrequently and unpredictably but, when successful, can have a catastrophic impact on the transit system, a region's economy, and the psychology of entire nations.

Unfortunately, transit systems are attractive targets for terrorists: Large numbers of passengers are contained within enclosed spaces; transit terminals and stations are often visible, symbolic expressions of a city or a region; and transit, especially in urban areas, is central to regional commerce. Significant psychological trauma to a community or even the entire nation can be inflicted by a terrorist attack on a transit system.

Transit agencies, with the technical assistance provided by DHS/TSA and FTA, have been striving to meet these challenges and have, in varying degrees, enhanced the preparedness of their police force and security personnel, educated their passengers, and hardened their transit systems as terrorist targets. Immediately after September 11, counterterrorism efforts were implemented in a reactive and piecemeal manner, but more recently transit agencies have been incorporating security practices into their core mission, strategic plans, and daily operations. Although transit agencies have invested more than \$2.5 billion to enhance security and preparedness, transit security needs, according to APTA, are approximately \$6 billion (Hull 2007).

Transit agencies have had to balance security needs with the innate attributes of public transportation—accessibility to the public, reliability of service, convenience, and smooth operations—and address difficult issues such as privacy, tort law and constitutionality, and employee and public acceptance.

THE TERRORIST THREAT

Terrorists justify and even glorify violence against innocent civilians. Significant harm can be inflicted with relatively minor expenditure by terrorists. For instance, improvised explosive devices (IEDs), one of the primary threats to transit systems, can be assembled with commonly available items.

The principal international terrorist threat is from the al-Qaeda network, which has been evolving constantly in response to the counterterrorism efforts initiated by the United States and other nations. In 2006, authorities uncovered a plot by eight al-Qaeda terrorists to plant explosives on a Port Authority Trans-Hudson Corporation (PATH) train connecting New Jersey and Manhattan and hoped to blow up the underwater tunnel under the Hudson River (CNN 2006). In India, on May 13, 2008, bicycles and rickshaws were attacked in a well-planned series of explosions that killed at least 60 people and wounded 150 others in a top tourist destination. Although bicycles and rickshaws are not typical modes of public transportation in the United States, this type of attack illustrates the adaptability of terrorists and their capacity for planning and successfully executing simultaneous attacks.

Some of the other new challenges include a more dispersed network in multiple locations and nations; an increased and more sophisticated use of the Internet to communicate, recruit, proselytize, raise funds, and gain access to and disrupt government sites; and an increasing interest in weapons of mass destruction (WMD) (*National Strategy for Combating Terrorism* 2006).

A variety of international terror groups have been targeting U.S. assets and citizens, and homegrown terrorists have also exacted loss of life and psychological damage on innocent civilians on U.S. soil; however, the primary focus has been and continues to be on the al-Qaeda threat.

Multimodal, rail-only, and ferry operators naturally consider a greater range of threats to be applicable to their systems than bus agencies. Synthesis survey results revealed that the terrorist threats of primary concern to multimodal systems, including rail-only and ferry operators, were as follows:

- Explosives
- Chemical and Biological (tied)
- Hijacking and Shootings (tied)
- Sabotage.

The terrorist threats of primary concern to bus agencies were as follows:

- Hijackings
- Shootings
- Explosives
- Sabotage.

Cyber crimes have been on the rise in the United States with frequent hackings of government sites and databases, and large amounts of sensitive information being compromised. The potential for sophisticated hackers to damage or disrupt the computer network, communications systems, operations of control centers, and Intelligent Transportation Systems (ITS) technologies of transit systems is indisputable.

Potential Transit Targets

Transit targets include transit vehicles, transit and related infrastructure, communications systems, and transit personnel. Internationally, all modes including ferries have been the target of terrorist attacks, with attacks on rail systems being the most severe in terms of casualties and injuries. The attacks on Madrid's commuter rail system took the lives of 191 persons in 2004, and 200 persons died in the attack on Mumbai's commuter rail system in 2006. In 2005 in London, 52 people were killed on London trains and buses. On Israeli buses, IED attacks often carried out by suicide bombers have been less severe in terms of lives lost but the attacks have been much more frequent. Although no major terrorist

attack in the United States has occurred since 9/11, these events reflect the continued persistence and desire of terrorists to inflict harm on innocent civilians and their proclivity to choose transit systems as targets.

Transit Vehicles

Transit vehicles are primary targets because they contain large numbers of passengers and also can damage surrounding or nearby infrastructure. A series of attacks on a train proceeding through an underwater tunnel potentially can cause the destruction of the tunnel along with the death of the occupants of the tunnel and the train. An attack on a bus traveling under a building can not only destroy the bus along with its passengers and driver but also potentially cause the collapse of the building. The extensive and open nature of many commuter and light rail systems and their infrastructure make the assurance of passenger security particularly challenging. Vehicle-carrying ferries and high-capacity ferries are considered to be especially vulnerable. During emergencies, ferries may be the only viable mode of transportation for both victims and emergency responders and an important evacuation mode as well.

Transit Infrastructure

Transit infrastructure includes passenger terminals, stations, and stops; tunnels, bridges, and elevated structures; ferry terminals; rail yards and bus depots; rail right-of-way (ROW), tracks, and signals; control centers and communications; administrative facilities; and parking lots and structures that may or may not be owned by the transit authority (see Figures 1 and 2 for examples of a station and terminal). All of these transit infrastructure elements are potential targets (FTA 2004).

Passenger terminals such as Union Station in Washington, D.C., and Grand Central Terminal in New York City are typically large intermodal stations with high passenger and pedestrian volumes, provide critical links within a region's transit network, and hold symbolic significance to a city or region. Transit tunnels allow the passage of transit vehicles along with passenger and commercial vehicles and may be located underwater or underneath various structures, making them attractive targets. These tunnels are essential for goods and people movement, and repairing tunnels is costly and time-consuming. Because control centers and communications systems are essential for transit operations, they are vulnerable to physical or cyber attack.

Rail yards and bus depots are susceptible to attack because they contain many transit vehicles, maintenance areas with exposed vehicles, fuel storage, and revenue collection and storage mechanisms. Rail ROW, tracks, and signals can be targets because damage to these elements can

cause accidents and derailments. Parking lots and structures are potential targets, especially when they are located beneath or above a transit terminal or station.



FIGURE 1 Heavy Rail Station (Source: Dr. Yuko J. Nakanishi).



FIGURE 2 Grand Central Terminal (Source: Dr. Yuko J. Nakanishi).

Transit Personnel

Transit personnel, essential to a system's safe and secure operation, are viewed as an important first line of defense against terrorism and are vital during emergencies. Transit personnel are vulnerable to theft of their uniforms, theft of their identification, and impersonation; they are also vulnerable to hijackings and blackmail. The potential also exists for a terrorist to gain access to a transit system as an employee, contractor, or vendor to use a vehicle as a weapon or to commit other types of sabotage. Disgruntled employees are a concern because they can easily access transit vehicles and facilities.

TSA Security Initiatives

TSA's efforts to assist public transit agencies and passenger rail carriers to deter terrorism and reduce the effects of terrorist attacks continue to be guided by five principles (TSA 2008):

1. Expanding partnerships for security enhancement through regional coordination and liaison, notably engagement with federal and mass transit and passenger rail security partners through the Government Coordinating Council and Sector Coordinating Council framework, the Transit Policing and Security Peer Advisory Group and multiagency coordination forums in regional areas throughout the country: To address the first principle, TSA has been conducting regional security forums and workshops, collaborative efforts with public and private partners, and international outreach.
2. Elevating the security baseline through the Baseline Assessment for Security Enhancement (BASE) program and the analysis and application of results to drive the development of security programs and resource allocations that most effectively produce security enhancement: The BASE program assesses and aims to elevate the TSA's security posture in 17 Security and Emergency Management Action Items. Also, numerous security assessments have been conducted. Particular attention is paid to the transit agencies posture in five fundamental areas:
 - Protection of other high-risk assets that have been identified through systemwide risk assessments;
 - Use of visible, unpredictable deterrence;
 - Targeted counterterrorism training for key front-line staff;
 - Emergency preparedness drills and exercises; and
 - Public awareness and preparedness campaigns.

TSA has produced a compilation of Smart Security Practices derived from the BASE results, with the implementing mass transit or passenger rail agency and a point of contact identified, to enable mass transit and passenger rail security officials to network and discuss how the particular practice has been developed and implemented and to consider how it may be adapted to the operational circumstances of other systems.

3. Building security force multipliers through security training of employees and law enforcement, terrorism prevention and response exercises and drills, and public awareness campaigns: Well-trained employees are a force multiplier for security efforts implemented by transit agencies. To assist transit agencies in improving their training, in 2007, TSA developed and published the Mass Transit Security Training Program and is creating a national counterterrorism exercise program. The Visible Intermodal Prevention and Response (VIPR) program augments security by sending TSA teams to selected transit systems. The TSA teams provide random security activities as a terrorism deterrent.

4. Leading information assurance by building information-sharing networks integrating federal security partners with mass transit and passenger rail agencies and state and local entities to facilitate timely exchange of intelligence products and security implications at both classified and unclassified levels: TSA's Mass Transit Security Information Network ensures timely development and distribution to mass transit and passenger rail security officials and federal government decision makers of security information products, recommendations, and guidelines during periods of heightened threat or security incidents. Joint DHS/TSA and Federal Bureau of Investigation (FBI) threat and analysis briefings are held for mass transit security partners and other stakeholders quarterly.
5. Protecting high-risk assets and systems through development, testing, and deployment of new technologies and targeted application of security grants to achieve the most substantial mitigation of risk: Protecting high-risk underwater and underground assets and systems in mass transit is a top priority. The tunnel security working group formed by DHS and department of transportation (DOT) continued to bring together subject matter experts from a range of relevant fields to identify, assess, and prioritize the risk to mass transit systems with underwater tunnels. The National Explosives Detection Canine Team Program (NEDCTP) has continued to augment the explosives-detection capability of critical transit agencies by providing partial funding, training, certification, and management assistance. TSA's Office of Security Technologies, Transportation Sector Network Management (TSNM) Mass Transit is developing multiple technologies to advance capabilities to detect and deter terrorist activity and prevent attacks.

PROJECT BACKGROUND AND OBJECTIVES

This report is an update of *TCRP Synthesis of Transit Practice 21: Improving Transit Security* (Needle and Cobb 1997). The report incorporates terrorism-related issues, up-to-date information on security measures and practices, perception of crime and terrorism, and other related issues. The primary objectives of the updated Synthesis study were to identify (1) the state of the practice and the many security-related changes made by transit agencies since September 11, 2001; (2) the nature and perception of crime, incidents, and suspicious activity since 9/11; (3) counterterrorism and anticrime security measures and practices implemented by transit agencies; and (4) effective or innovative measures and practices. Secondary objectives included the identification of issues and obstacles to security and policing management and the identification of further research needs.

Technical Approach to the Project

The objectives of the project were met by the following tasks:

- Conducting a literature review of relevant materials,
- Developing and distributing a survey to 120 large and small transit agencies in various geographic regions of the United States,
- Conducting case studies,
- Seeking and receiving input from industry experts, and
- Analyzing National Transit Database (NTD) security and incident data.

Literature Review

A literature review of relevant materials on security and policing practices and transit counterterrorism strategies was performed by consulting FTA reports, TSA products, TCRP and NCHRP studies, books, journal and magazine articles, and online sources. The literature review is located in Appendix B of the report, and the key portions of the review were synthesized into the report text.

Survey

The objective of the survey was to obtain information about post-9/11 crime-prevention and counterterrorism measures; effective or innovative security and policing practices; and information about crime, incidents, threats, and suspicious activity trends. In addition, the survey sought to identify issues and obstacles to security and policing management. The expanded objectives of the survey necessitated a longer questionnaire format.

The survey was distributed through the online survey site, electronically, or by mail to 120 multimodal and modal transit operators. The goal of the selection process of the survey recipients was to ensure diversity in terms of agency size, geography, and service area as well as modes operated. Of the 120 operators contacted for the survey, 45 (or 38%) responded. Because there was variability in terms of responses to individual questions, this was taken into account in the data reporting process. The survey questionnaire, list of survey respondents, and the survey results are presented in Appendixes C, D, and E.

The categories of questions included in the survey were security and policing management; primary threats to transit systems; security measures being used or planned for use; the most effective measures and innovative practices; threats or incidents including cyber breaches; post-9/11 changes in security practices and changes in threats and suspicious activity, criminal offenses, and incidents; system security data and analysis; customer outreach; and employee security and policing training.

Because many transit agencies expressed significant concern regarding the provision of highly sensitive information and requested complete anonymity, agencies were afforded the opportunity to submit survey responses by fax without their contact information.

Case Studies

The objectives of the case studies were to obtain in-depth coverage of both crime and terrorism-related security challenges faced by the selected transit agencies and to take a closer look at the security practices and measures used by the agencies to address those challenges. The case study question categories included post-9/11 changes in security, policing, policy, and practices that had been made by the agency; the technologies and other security measures that were implemented and details regarding the implementation; changes in crime, incident, and suspicious activity trends; training and personnel issues; security data collection and analysis practices and concerns; and other information relevant to the study.

Input from Industry Experts

In addition to the Synthesis study's panel members, relevant input was received from industry experts, including the TSA, FTA, other federal agencies, and the private sector.

National Transit Database Security and Incident Data

NTD security and incident data were analyzed for the years 2002 to 2007, although much of the analysis results were not incorporated into the report because of concerns about the reliability and accuracy of the data.

REPORT ORGANIZATION

This report is organized into seven chapters, including this introductory chapter. Chapter two focuses on the passenger perception of crime and terrorism along with performance metrics and data issues. Chapters three and four cover the security measures and practices being used or those that are available for use by transit agencies. The information for these chapters is based on the survey analysis and literature review. Conflict mitigation strategies are presented in chapter five. Chapter six presents the results of the four case studies and an agency profile. The concluding chapter, chapter seven, summarizes the findings of this project, provides highlights of transit security practices, describes obstacles to transit policing and management, and presents recommendations for further research. Supporting material on security awareness, emergency evacuation, and rules and codes of conduct literature examples are provided in Appendix A. The literature review is presented in Appendix B.

CHAPTER TWO

PASSENGER PERCEPTION OF CRIME AND TERRORISM

Within transit systems, both serious and minor crimes affect passenger perceptions of security. Serious crimes are exaggerated by the media and intensify passenger fears. Minor offenses and disorder are also disconcerting to passengers and provoke the perception that the transit agency is not in control of its transit system. Perceptions of passenger and system vulnerability could embolden criminals and terrorists.

PASSENGER PERCEPTION OF CRIME

A study performed by the Metropolitan Transportation Authority (MTA) showed that the majority of its passengers overestimated the number of felony crimes committed within the subway system (Johnson 1988). Industry experts agree that this phenomenon is a widespread problem that persists in the transit industry.

Although violent crimes within transit systems are generally low in actual numbers, public perception is different. When a violent crime does take place within transit systems, media coverage is intense and has a significant impact on public perceptions about their transit system. McDonald noted that “for some passengers, fear evoked by media coverage of a single violent event was sustained for a long period of time” (2001, p. 7). The media and the entertainment industry have exaggerated the dangers of public transportation systems and have compounded public fears about mass transit. According to Nelson, “crimes that might barely merit mention otherwise become headline news if they occur on a mass transit system. Selective media coverage perpetuates the myth that public transportation is unsafe” (Nelson 1997).

The landmark effect also has a negative impact—even though a crime did not occur within the transit system, the media may refer to a crime as having occurred near a specific transit station because it serves as a readily recognizable landmark. Furthermore, public fears generally increase when any violent crime occurs in or in proximity to the transit system, even though a crime such as one originating from a domestic dispute may have little to do with the transit system itself. Nontransit crimes occurring outside of one’s own community do not have a similar psychological impact on the public.

Minor crimes and disorder have a greater impact on the perception of security when it occurs within the transit sys-

tem environment. For instance, an aggressive panhandler blocking a narrow hallway invokes more fear in passengers than the same panhandler on a public street. In addition, the unruly behavior of juveniles can be disconcerting to transit customers even though no crime is committed. This is particularly true when large numbers of youths congregate in the system, as cited in the Massachusetts Bay Transportation Authority (MBTA) Youth Study. The study found that 75% of afternoon riders were intimidated or unnerved by the overwhelming presence of school-age children within the transit system (MBTA 2000).

PASSENGER PERCEPTION OF TERRORISM

In terms of passenger perceptions of terrorism, Synthesis findings concurred with the *TCRP Report 86, Volume 13* (2007), which revealed that the mentality of east coast transit customers is thought to be different than those on the west coast and other parts of the nation because of the tragic events of 9/11, which took place in New York City, Washington, D.C., and Boston. Transit agency interviewees from agencies serving large metropolitan areas along the east coast reported that their customers take the threat of terrorism more seriously and are more tolerant of terrorism-related security measures, whereas smaller agencies reported that generally their customers do not demand security-related improvements to reduce the threat of terrorism and instead are more concerned with routine acts of crime and lawlessness.

PERFORMANCE MEASURES

Transit agencies have developed and implemented performance measures to improve their transit operations; to instigate changes in policy, planning, and procedures; to conduct performance comparisons; and to communicate and report results. Performance measures are usually aligned with the agency’s mission, goals, and objectives. In addition to the agency perspective, performance measures can reflect the perspectives of the transit customer, the transit vehicle or driver, and the community (*TCRP Report 88* 2003). Performance measures can reflect outcomes or outputs. *Outcomes* are the actual results that are visible or experienced by the agency, its customers, its personnel, and the community.

Outputs are the intermediate steps or products generated to produce the outcomes. Comparing changes in outputs to changes in outcomes can help determine whether a specific tactic is useful in producing a desired outcome.

Security metrics and targets can be established for all aspects of transit security. Crime outcome metrics can address a system's overall crime rate and the crime rate for specific stations, routes and lines, or parking facilities. Terrorism metrics reflecting outcomes are more difficult to develop because terrorist events are rare and deterrence levels cannot be measured. However, performance metrics related to the results of system testing (e.g., the detection rate of a particular security measure) and relevant incidents (e.g., response time) may be useful. Also, output measures such as the number of vulnerability assessment recommendations implemented or coverage and deployment metrics (e.g., the ratio of patrols to the number of transit vehicles) may be used to assess different aspects of a transit agency's counterterrorism efforts.

Passenger perceptions about their agency's ability to control the transit environment are an important indicator of the level of passenger security. Customer perceptions of security about their transit ride can be obtained through customer surveys. The specific attributes that influence passenger perceptions of security can be identified through analysis of customer survey or focus group data. Evaluation of these critical attributes could highlight weak attributes that then may be targeted for improvement. In addition, output measures can be established for specific security measures and practices.

Security performance measures can be used for multiple purposes, including the following:

- To evaluate overall system security,
- To compare present versus past performance,
- To identify trends,
- To determine progress toward performance goals,
- To identify vulnerabilities and security needs, and
- To motivate police and security personnel.

The BASE program assesses the TSA's security posture in 17 Security and Emergency Management Action Items. The assessments results have produced timely action to address identified weaknesses in different areas and can be used effectively in the development of performance measures.

The benefits and value of security investments and measures can be conveyed to the agency management, transit police, security personnel, and the public using these metrics. The benefits of specific security measures and practices can be determined by performing pre- and postimplementation evaluations. A primary benefit of security investments is believed to be the reduced risk of attack:

Risk of attack—although terrorism risk and deterrence level are difficult to calculate, testing the security system can determine the decrease in the detection rate after the measure or system is installed; for locations with many incidents of a certain type, the pre- and postimplementation assessment can determine whether and to what extent a specific security measure succeeds in meeting its security objectives.

Cost-related performance is important in demonstrating the cost-effectiveness and cost-related benefits of security investments (Campbell 2008). The following are possible cost-related measures:

- Cost of security incidents, including costs associated with lawsuits,
- Cost of compliance with regulations and insurance,
- Security cost as a percentage of overall agency budget or expenses,
- Audit findings from security defects,
- Downtime in transit service,
- Labor intensity of security activities owing to technology, and
- Overall costs of security operations.

Only a few survey respondents indicated that they use security performance measures. These respondents stated that they use the following measures: crimes per 100,000 passengers or crimes per 100,000 unlinked trips; security personnel per 1 million unlinked passenger trips; and percent of front-line personnel who have completed transit security training. The MBTA Transit Police Department publishes detailed Part I and Part II crime statistics by subway line and produces an interactive online map that displays crime statistics for each station. The San Francisco Bay Area Rapid Transit District (BART) Police Department provides data on crimes against persons, vehicle-related crimes, and police emergency-response times that are published in a quarterly report to the transit agency's board of directors. Additional information on MBTA and BART's crime statistics are included in the case studies (see chapter six). The New York Police Department (NYPD) website also contains information about its performance measures and the results. Information about CompStat (computer-driven crime statistics), the NYPD's crime control model, has been provided in the literature review in Appendix B. Transit agencies that did not report the use of performance metrics, however, did report the collection and use of the following security data: threats, suspicious activity, persons, and items; results of threat and vulnerability assessments; number of security personnel by location; number of security checks by location and average response time of security personnel; ingress and egress at all facilities; calls for service data by location; and training data.

To determine progress toward goals and objectives, appropriate targets should be set for performance measures. Sources of information on performance measures include

TCRP Report 88: A Guidebook for Developing a Transit Performance-Measurement System (2003), the Royal Canadian Police Departmental Performance Report (2007), and Campbell's *Measures and Metrics in Corporate Security* (2006):

- *TCRP Report 88: A Guidebook for Developing a Transit Performance-Measurement System* contains relevant information about effective performance measures and how they may best be implemented within transit systems as part of a performance-measurement system (2003).
- Guidelines for setting up an effective performance measurement program are described in chapter 4 of the Royal Canadian Police Departmental Performance Report (2007), which explains how the Royal Canadian Police Department's performance measurement system is linked to its strategic priorities and outcomes, and the specific metrics within its measurement system that reflect these outcomes.
- Campbell's *Measures and Metrics in Corporate Security* workbook provides 375 real examples of security metrics aggregated into 13 categories, covers how to start a security metrics program, explains how to present findings to senior management, and contains many examples of presentation techniques (2006).

CRIME AND SECURITY DATA

The FBI's Uniform Crime Reporting (UCR) Program, initiated in 1929 by the International Association of Chiefs of Police, collects offense data categorized into serious or Part I offenses and minor or Part II offenses (FBI-Uniform Crime Reports, published annually). Transit agencies categorize crime data similarly and often further parse the data into more specific categories.

The transit industry's centralized reporting mechanism for transit data is the FTA's NTD. The NTD contains data on UCR offenses and other major and nonmajor incidents. Beneficiaries of FTA formula funds are required to report these incidents to the FTA through a secure online reporting method. Although safety and other NTD data are considered to be more reliable, industry experts raised concerns about the accuracy and completeness of NTD crime and security-related incident data and agreed that these data issues need to be addressed.

The FTA expanded its collection of transit crime statistics in 2002 and has been categorizing incidents into major and nonmajor incidents: major incidents involve fatalities and injuries and are much fewer in number than nonmajor incidents. *Major incidents* are defined as those incidents and offenses involving a fatality other than a suicide, injuries requiring immediate medical attention away from the scene for two or more persons, property damage equal to or

exceeding \$25,000, an evacuation owing to life safety reasons, or a mainline derailment. Although homicide is always considered a major incident, other Part I and Part II offenses may or may not be "major" depending on the severity of the offense. *Nonmajor incidents* are defined as those incidents not already reported on the Major Incident Reporting form. In addition to Part I and Part II data, the FTA collects information about bombings, bomb threats, chemical or biological releases, sabotage, and cyber incidents.

The glossary provides definitions of major and nonmajor incidents and offenses. Data on the characteristics of crime victims and offenders are not available from the NTD, and few responses were provided for questions related to this topic on the survey. Therefore, national crime data were consulted to obtain data about the attributes of victims and perpetrators.

The following are Part I offense categories and definitions in the NTD:

- Homicide—always categorized under major incidents, is defined as the killing of one or more human beings by another, including the following:
 - Murder and nonnegligent manslaughter—the willful (nonnegligent) killing of one or more human beings by another.
 - Negligent manslaughter—the killing of another person or persons through gross negligence.
- Rape—the carnal knowledge of a person forcibly and against that person's will.
- Aggravated Assault—an unlawful attack by one person upon another wherein the offender uses a weapon in a threatening manner or the victim suffers obvious severe or aggravated bodily injury.
- Robbery—the taking or attempting to take anything of value under confrontational circumstances from the care, custody, or control of another person by force or threat of force or violence or by putting the victim in fear of immediate harm. The use or threat of force includes firearms, knives or cutting instruments, other dangerous weapons (clubs, acid, explosives), and strong-arm techniques (hands, fists, feet).
- Larceny/Theft—the unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another person. This includes pocket picking, purse snatching, shoplifting, thefts from motor vehicles, thefts of motor vehicle parts and accessories, theft of bicycles, theft from buildings, theft from coin-operated devices or machines, and all other theft not specifically classified.
- Motor Vehicle Theft—the theft or attempted theft of a motor vehicle. A motor vehicle is a self-propelled vehicle that runs on the surface of land and not on rails.
- Arson—to unlawfully and intentionally damage, or attempt to damage, any real or personal property by fire or incendiary device.

The following are Part II offense categories and definitions in the NTD:

- Fare Evasion—the unlawful use of transit facilities by riding without paying the applicable fare.
- Nonviolent Civil Disturbance—nonviolent public demonstrations that may or may not be disruptive.
- Other Assault—an unlawful attack or attempt by one person upon another where no weapon was used or that did not result in serious or aggravated injury to the victim.
- Trespass—to unlawfully enter land, a dwelling, or other real property.
- Vandalism—the willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without consent of the owner or person having custody or control by cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law.

The following are other security incident categories in the NTD:

- Bombing is the unlawful and intentional delivery, placement, discharge, or detonation of an explosive or other lethal device.
- Bomb Threats: Credible written or oral (e.g., telephone) communication to a transit agency threatening the use of an explosive or incendiary device for the purpose of disrupting public transit services or to create a public emergency.
- Chemical, biological, or nuclear release is the unlawful and intentional delivery, placement, discharge, or detonation of a biological, chemical, or nuclear lethal device.
- Cyber Incident—involves the targeting of transit facilities, personnel, information, computer, or telecommunications systems associated with transit agencies. Proscribed activities include the following:
 - Denial or disruption of computer or telecommunications services, especially train control systems;
 - Unauthorized monitoring of computer or telecommunications systems;
 - Unauthorized disclosure of proprietary or classified information stored within or communicated through computer or telecommunications systems;
 - Unauthorized modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities; or
 - Manipulation of computer or telecommunications services resulting from fraud, financial loss, or other criminal violations.
- Hijacking—seizing control of a transit vehicle by force.

- Sabotage—sabotage or tampering with transit facilities' assets may be a means to achieve any of the above events, such as starting a fire or spreading an airborne chemical agent, or it may be a stand-alone act, such as tampering with track to induce derailment.

CRIME TRENDS

The general U.S. crime rate according to the Bureau of Justice Statistics (BJS) has been on a downward trend since 1996. In the 1996–2005 period, a 37% decrease was seen, with much of the decline (33.7%) having occurred in the 1996–2001 period and, in particular, violent crimes and thefts decreased markedly. In 2001, the decline slowed and then began to plateau.

Researchers have noted several possible causes of the nationwide decline in crime (Blumstein and Wallman 2000; McDonald 2001; Conklin 2003):

- Better and increased police intervention
- Rise and decline of the cocaine trade
- Aging of the population
- Enhanced economic conditions
- Higher incarceration rates
- Improved quality of medical care.

Transit crime incidents generally have followed national trends, declining by 45% from 1997 to 2002 (BJS 2000, 2003). New York City Transit experienced an even more pronounced decline in crime rates:

In 1990, NYC Transit Police initiated a comprehensive crime control process considered a precursor to NYPD's CompStat. Serious crime declined significantly in the 1990–1995 period—robbery offenses diminished by 80% and all other crime by 72%. The process involved targeting serious and minor crimes, and quality of life issues, systematically tracking offenders, and sending a clear message to the public and would-be offenders that the transit system was under control. When CompStat was implemented in New York City, it is believed to have spurred a dramatic improvement in city-wide crime rates (McDonald 2001).

To identify transit crime trends and offense types for the 2002–2006 period, NTD data were analyzed. The results of detailed analysis did not reflect the experiences of some transit agencies and concerns were raised with the reliability of the data. However, the following general conclusions can be made from the data analysis:

- Serious crimes, including the most violent crimes, are infrequent compared with minor crimes:
 - Many more Part II than Part I offenses (6 to more than 11 times) occurred for each year from 2002 to 2006.

- The numbers of the most violent crimes, homicide and rape, were extremely low:
 - Homicide accounted for 0.01% of 2002–2006 Part I offenses.
 - Rape accounted for 0.2% of 2002–2006 Part I offenses.
- The most problematic Part I offense was *theft*:
 - Theft accounted for 50%–60% of Part I offenses for every year in the 2002–2006 period.
 - Aggravated assault accounted for 10%–15%; motor vehicle theft for 8%–13%; and robbery for 10%–18% of Part I offenses.
 - Bus and heavy rail modes accounted for much of the Part I offenses, followed by commuter rail and light rail.
- The most frequent Part II offense was *fare evasion*:
 - Fare evasion citations accounted for more than 90% of Part II offenses for every year in the 2002–2006 period.
- The majority of the fare evasion citations occurred on light rail systems, which typically have no turnstiles and operate on the honor system. Because the number of fare evasion citations recorded by an agency typically correspond to the transit agency’s enforcement level at a particular time, changes in the citation statistics are difficult to interpret—for example, it is not possible to determine whether an increase in the number of citations was the result of an actual increase in the number of fare evaders or the result of increased enforcement activity.

SUSPICIOUS ACTIVITY

Transit agencies reported that reports of suspicious activities, persons, and items increased in the immediate period after 9/11, and none reported a decrease. In general, reports of suspicious activity, although higher than in the period before 9/11, have diminished and plateaued over the past few years. An increase in suspicious activity incidents does not necessarily mean that the threat of terrorism against an agency is rising, because the increase may be the result of better reporting. For example, Washington State Ferries had 157 suspicious incidents in the three years after 9/11. Seven had an “extremely” high likelihood of being preoperational planning, 11 had a “high” likelihood, and 49 had “medium” likelihood. From spring 2004 to fall 2005, the FBI reported 247 suspicious incidents for the Washington State Ferries; however, they believed that the increase was because of better reporting and not because the actual likelihood of an attack had changed (Blumenthal 2006).

DATA ISSUES

Industry experts have raised concerns about the accuracy of the NTD crime and security-related incident data. In addi-

tion, crime data analysts and researchers believe that although homicide statistics are the most accurate and well-reported of all crime data, issues with the other crime statistics include crime categorization and changes in reporting rates.

National Transit Database Issues

The results of detailed analysis performed for this study revealed abnormalities and inconsistencies in the NTD data, and did not reflect the experiences of some transit agencies. Not all transit agencies required to report crime and incident data have been reporting them to the NTD, and the number of transit agencies reporting to the NTD has not been consistent. Therefore, year-to-year comparisons and trend analysis may be inaccurate. Data entry errors also occur. For instance, a data entry error caused the analysis to show a significant increase in burglaries, when this was not the case.

Although hijackings, sabotage, and other incidents had been reported each year from 2002 to 2005, none had been reported in 2006 and 2007, raising questions about the reliability of the data. Also, contrary to the fact that no terrorist attacks involved transit since 9/11, the database indicated that security incidents had occurred, such as bombings and chemical/biological releases. Details of these incidents were not available, but it may be assumed that these incidents were insignificant—a prank involving dry ice placed within a plastic bottle would still be classified as a “bombing,” but may unnecessarily be alarming to the public.

Crime Categorization

In terms of crime categorization, although definitions of homicides and robberies have remained stable over the years, more discretion may be used to categorize assaults; namely, whether an assault is considered aggravated or not. This, in turn, can affect aggregate Part I and Part II numbers.

Reporting Rates

The BJS determines reporting rates by using the National Crime Victimization Survey, which is a household survey, ongoing since 1972, that includes data from interviews of about 80,000 people age 12 and older in 43,000 households each year about their victimizations from crime. BJS then compares the National Crime Victimization Survey data with UCR and other national crime reports. A BJS study for the period 1992–2000 revealed that all homicides were reported, 90% of any type of violence involving a shooting was reported, and about 81% of motor vehicle theft was reported; however, only 57% of robberies, 55% of aggravated assaults, and 31% of rapes were reported to the police. About half of the crimes were reported by the victims themselves, whereas the rest were reported by relatives, household members, friends, bystanders, and officials. Violence against the elderly and against females was more likely to

be reported (BJS, March 9, 2003). However rape is a category that is significantly underreported because of the stigma attached to the crime. In general, underreporting of less serious crime is believed to occur on a more widespread basis (Blumstein and Wallman 2000).

Even more underreporting of transit crime may be the result of several factors:

- Local law enforcement may receive reports directly from the public and not share the data with the transit agency.
- Transit workers may receive a report from a passenger and may fail to report it to transit police or security.
- Crimes committed against juveniles and minorities may be underreported because of the antipolice culture cultivated within these subgroups. Those who have had prior involvement in the criminal justice system are more likely to be victims themselves and therefore are reluctant to report crimes (Blumstein and Wallman 2000; Conklin 2003).
- Passengers know what to do if they see suspicious activity thanks to effective public outreach campaigns conducted by many transit agencies, but they may be unaware of what steps to take if they witness a crime or if they are the victim of a crime. If security or transit personnel are not present, the victim of a minor crime may decide not to file a report, particularly if they need to travel to a different location or do not know how to make a report.

Although overreporting may not be a widespread issue, the possibility of overreporting exists and should be considered in data analysis issues. For instance, overreporting can occur if the same incident is reported by more than one party and the duplication is not flagged.

Other Data and Data Analysis Issues

The primary security data sources included system reports and police reports; one agency indicated that it obtains crime data from online news as well. In addition to Part I and Part II crime data, other security data collected by agencies included threats, suspicious activity, persons, and items; results of threat and vulnerability assessments; number of security personnel by location; the number of security checks by location and average response time of security personnel; ingress and egress at all facilities; calls for service data by location; training data; location of transit centers; number

of vehicles; contact information for personnel; public comments; accident data; and landscaping information.

Although crime mapping is not performed by many agencies, crime trend analysis by location (e.g., transit station or stop) is used more often by transit agencies for resource allocation purposes.

Data-related needs and concerns cited by survey respondents included the following:

- Changes in federal transit security funding allocation procedures,
- Notification and documentation on all relevant incidents from frontline personnel,
- Development of security metrics,
- Development of a more consistent way to compare crime and security incidents, and
- Verification of more accurate data (e.g., data can be categorized incorrectly)

CHARACTERISTICS OF CRIME VICTIMS AND OFFENDERS

Data on the characteristics of crime victims and offenders are not available from the NTD, and few responses were provided for questions related to this topic on the survey. However, the characteristics of crime victims and offenders for crime committed on a national level are collected by the FBI and Department of Justice. An analysis of 1976–2005 homicide data revealed that males and blacks, and the 18 to 24 age group, were disproportionately represented as victims and offenders. The male victimization rate was three times higher and the offending rate was eight times higher, with males accounting for 77% of homicide victims and 90% of offenders. The victimization rate for blacks was six times higher and the offending rate was more than seven times higher than for whites (BJS Homicide Trends in the U.S. and FBI 1976–2005).

While violent crime rates have declined for all age groups since their height in the mid-1990s, the rates for younger age groups remain far greater than that of older age groups. The violent crime rate for those 65 and older was 2.4 per 1,000 persons while the rate for those in the 20–24 age group was 20 times greater and those in the 12–15 and 16–19 age groups were 18 times greater (BJS Trends in Victimization Rates by Age and FBI 2005).

CHAPTER THREE

SECURITY MEASURES

Before September 11, 2001, transit agencies were focused on crime along with quality-of-life issues. Since then, transit agencies have been challenged with countering terrorism as well. The threat of terrorism brought forth an expanded set of security-related objectives that includes the following, as listed in the National Academy of Science report, *Making the Nation Safer* (National Research Council 2002):

- Predict: Intelligence and surveillance of targets and means
- Prevent: Disrupt networks, contain threats
- Protect: Harden targets, immunize populations
- Interdict: Frustrate attacks, manage crisis
- Response and Recovery: Mitigate damage, expedite cleanup
- Attribute: Identify attacker to facilitate response.

Protective measures for transit systems can be people-based, technology-based, or a mix of the two. Because every transit agency faces unique challenges and operates under differing institutional, political, economic, and legal constraints, no single set of countermeasures is appropriate for every agency. Each transit agency needs to assess these issues within their own operating environment and consider numerous factors, such as the agency's budget, threat assessments including expected future threat level and expected nature of the future threat, and vulnerability assessments by asset type and mode.

Cost and value of security investments are important and necessary considerations for agency management. Cost-effectiveness or cost-benefit analysis and the use of performance metrics can determine the overall value, specific benefits, and effectiveness of a protective measure. To maximize limited resources and address natural disasters that can exact a significant toll in terms of human life, property, and economic effects, the "all-hazards" approach to emergency planning and incident management is being promoted by federal, state, and local governments.

According to FTA's *Transit Agency Security and Emergency Management Protective Measures report* (Batelle, TotalSecurity US, and Transportation Research Associates 2006), general measures can be taken at specific Homeland Security Advisory System (HSAS) threat levels to address the additional two response conditions shown in Figure 3.



FIGURE 3 HSAS Threat Condition Connectivity (Source: Batelle et al. 2006).

As the threat level increases, the type and intensity of recommended countermeasures increase as well. Transit agencies can modify and fine tune these generic measures for use within their own system to address their specific threats and security needs; note that some agencies have developed their own threat-level identification system, which may be somewhat different from the HSAS. The following are the recommended countermeasures:

- Low or Green threat condition:
 - Focus on completing security and emergency preparedness-related plans,
 - Ensure existence of capabilities to address higher threat conditions,
 - Conduct inventory of all needed resources to execute the plans,
 - Conduct needed training, and
 - Implement Security Vulnerability/Risk Assessment process.
- Guarded or Blue threat condition, the first level of potential threat:
 - Review all plans and procedures,
 - Identify steps that need to be undertaken in managing an incident,
 - Test equipment and systems and address problems,
 - Recheck inventories,
 - Design and execute drills and exercises,
 - Develop and disseminate public awareness information, and

- Prepare security awareness messages for higher threat conditions.
- Elevated or Yellow threat condition, a significant risk for terrorist activity or attack:
 - Increase surveillance,
 - Coordinate emergency plans and procedures, and
 - Initiate contingency activities.
- High or Orange threat condition, a high risk of terrorist activity:
 - Coordinate security efforts at the transit agency, local, state, and federal levels;
 - Address security for scheduled public events;
 - Tighter access control to facilities; and
 - Place higher priority on activation of emergency and contingency plans.
- Severe or Red threat condition, the highest level of readiness: Activate and deploy the maximum security and emergency preparedness processes, procedures, and activities available, which can require resource redirection or facility closings.
- Attack or Active Incident: Certain protective measures should be implemented at the time that an attack, active incident, or another major emergency (e.g., natural disaster) has occurred or is occurring against a specific transit agency or within its service area, and during the recovery phase. Protective measures implemented may respond to casualties, assisting in evacuations, inspecting and securing transit facilities and infrastructure, or helping with other tasks as directed by an emergency management authority. An attack or active incident may occur at any time, even while the transit system is at any of the other lower threat conditions.
- Recovery: During the recovery phase, restoring service, repairing or reopening facilities, adjusting employee work schedules and assignments, responding to customer inquiries about services, and other activities are required to fully restore transit service. Recovery will be accomplished while maintaining the prevailing threat level readiness status in other parts of the transit system's operations.

In coordination with the DHS Science and Technology Directorate (DHS/S&T) and TSA's Office of Security Technologies, TSNM Mass Transit pursues the development of multiple technologies to advance capabilities to detect and deter terrorist activity and prevent attacks. Project priorities are informed by input from security partners in the mass transit and passenger rail community. Particular priority is given to the development of capabilities to mitigate the risk to underwater infrastructure. Ongoing development projects include the following:

- Anomalous Explosives Detector for Surface Transportation
- Intelligent Video Monitoring at Mass Transit Sites
- Bus Command and Control

- Chemical/Biological Program for Mass Transit
- Explosives Testing and Assessment of Rail Car Vulnerability
- Mass Transit Tunnels Entry Denial Systems
- Rapid Response to Extreme Events in Tunnels.

The measures intended to deter one type of threat address others as well. The indicators of an incident and the required response, however, may vary significantly based on the threat (Batelle, TotalSecurity US, and Transportation Research Associates 2006). For instance, to detect a biological threat, explosives detectors or radiological pagers would be futile. Furthermore, many measures address one or more of the following three key transit security concerns: terrorism, crime, and quality of life.

Survey respondents were asked the purpose(s) for which measures had been implemented—crime, terrorism, and/or quality of life. Almost three-quarters of respondents reported that crime prevention was the purpose, slightly more than half indicated counterterrorism, and about half of the respondents indicated improvement of quality of life. With regard to years of deployment, respondents stated that some of the measures had been implemented long before 2001, whereas others had been recently implemented.

The key measures used by transit agencies or available for their use are discussed further in this chapter. They are Access Control and Identity Management; Crime Prevention through Environmental Design (CPTED); Patrols, Plainclothes, and Manual Surveillance; Video Surveillance; Passenger Security Inspections; Operational Strategies; Threat Detection Technologies; Cyber Security; and Communication Security.

TECHNOLOGY ISSUES

Although security technologies are becoming increasingly sophisticated, they cannot replace the judgment and experience of transit police officers and security personnel. Whether or not they are dominated by technological solutions, all measures require human input and judgment. Technologies do provide transit police officers and security personnel with additional tools to assist them in carrying out their responsibilities safely, effectively, and efficiently.

Technologies, before implementation, should undergo appropriate testing and evaluation to ensure that they are feasible as well as effective within the environment of a specific transit system. In addition to operational issues, customer acceptance, potential health-related effects, and cost (unit/maintenance/life cycle) need to be considered in the technology implementation and selection process.

Furthermore, any applicable standards should be consulted when planning and implementing security technolo-

gies. APTA working groups develop security standards for emergency management, infrastructure security, and risk management. APTA also established a Technical Standards Working Group to create standards for developing and procuring video systems and associated software and analytics. The standards will address all aspects of the systems, including camera location, resolution, frame rates, compression, and recording elements. Currently, the following standards are being finalized by the APTA working groups:

- Closed-Circuit Television (CCTV) Camera Coverage and Field of View Criteria for Passenger Facilities
- Continuity of Operations Plan (COOP)
- First Responder Familiarization of Transit Systems
- General Guidance on Transit Incident Drills and Exercises
- Security & Emergency Management Aspects of Special Event Service
- Trash/Recycling Container Placement to Mitigate the Effects of an Explosive Event
- Development and Implementation of a Security and Emergency Preparedness Plan.

Other resources for security-related standards are provided in Appendix B.

ACCESS CONTROL

Access control measures are designed to ensure that only authorized individuals enter a transit facility or premises. Access control may be used in conjunction with identity management techniques described in the following subsection and can be as basic as manual identification (ID) checks by security personnel or the use of locks and keys. Technologies such as intrusion detection and presence sensors, video surveillance, and biometric systems can also be used. Physical barriers and locks may or may not be electronic and may or may not be linked with an alarm and video system. Most transit agencies have implemented access control measures to varying degrees.

The TCRP Report 86, Volume 4: Intrusion Detection for Public Transportation Facilities Handbook (2003) provides information about intrusion detection systems and technologies, and is a useful reference for agencies considering the selection and installation of these systems.

Identity Management

Terrorists, criminals, and cyber criminals may seek to infiltrate their target agency's assets by impersonating transit employees. It is vital that only authorized transit employees and contractors have access to sensitive locations, transit vehicles and equipment, and the system's computer network, software programs (especially control programs for safety-critical functions), and databases. This access is addressed by

centralized identity management combined with access control. Transit agencies issue some type of employee ID card; as smart cards, they may also be used for other purposes such as fare payment. Transit agencies reported that they have some type of admission control system in place: encoded cards, manual verification, memorized code, mechanical lock, and electronic locks. They also reported having access control in place for vehicles within their facilities.

Transit agencies often require employees to display their ID cards on transit agency property and have a policy of revoking the cards when an employee has been discharged; strict adherence to this policy is important because discharged employees may forget or be reluctant to return their ID cards. Some agencies practice selective access so that only employees who need to access a sensitive area of the agency or a particular database are able to access it.

New post-9/11 identity management measures include background checks—survey respondents reported that they perform background checks on new hires; some reported that they already had this practice in place before 9/11. A few agencies reported that they initiated the fingerprinting of all employees after 9/11. Although background checks on contractors and vendors are important, some states disallow agencies from conducting these checks. The guidance on background checks most recently issued by the TSA helps transit agencies conduct more robust background checks and makes the process more consistent across agencies by identifying the factors to consider and the recommended scope of the checks and procedures.

Access control to transit vehicles and facilities is another issue. For instance, most bus fleets do not have access control systems, revealing a vulnerability that still needs to be addressed: if a driver is assaulted or is simply on a break, the bus is vulnerable to theft and vandalism, and terrorists may use the vehicle as a weapon. Automated Vehicle Location (AVL) systems in use by some agencies can determine the location of individual buses and alert a central dispatcher if a bus is off-route. For these agencies, the risk is somewhat mitigated, but access control for all transit vehicles would still be recommended.

Biometrics

Biometrics uses physical features and behaviors for identification and verification purposes. Identification, a one-to-many process, determines who a person is; the person's identity need not be known at the onset. Verification, a one-to-one process, confirms (or denies) a person's claimed identity. Behavioral biometrics such as keystroke or speaker recognition is generally used for verification, whereas physical biometrics such as fingerprint analysis, hand geometry, facial recognition, and iris scan can be used for either identification or verification (Nakanishi and Western 2005a).

A biometric identification credential is being implemented in federal agencies: Homeland Security Presidential Directive-12 required all government agencies and departments to implement a standard for secure and reliable forms of identification for employees and contractors, for access to federal facilities and information systems. The Transportation Worker Identification Card (TWIC) Program, which uses biometric systems and is compliant with much of Federal Information Processing Standard 201, was mandated by the Maritime Transportation and the Aviation and Transportation Security Act to create a common credential for workers in the transportation industry and has been initiated at 28 sites across the United States. It is expected that TWIC eventually will be used in conjunction with physical access control by all 12 million transportation workers, including transit employees. Transit agencies do not report the use of biometric systems for physical access control purposes.

Perimeter Security

A security perimeter demarcates public and semi- or non-public areas. Once a perimeter is crossed, transit agency rules apply and passengers should be informed of this by the use of proper signage.

Access control systems can secure the perimeter to ensure that only authorized persons are allowed access. For heavy rail systems, for instance, automated fare collection systems that utilize electronic turnstiles are used to ensure that only fare-paying passengers enter the system. For bus depots and rail yards, fencing is used. Electronic fencing has sensors that can alarm and identify the location of a disturbance. Free-standing sensors can be used without fencing. Buried sensors are appropriate for uneven terrain. These perimeter detection systems when accompanied by a CCTV system allow visual assessment of a situation should the system alarm (Nason 2008). With advances in video technology, intrusion detection capability can be integrated into video analytics. Specific guidelines for fences and gates are provided in FTA's *Transit Security Design Considerations report* (FTA 2004). For administrative and other facilities, authorized transit workers along with contractors and vendors need to be allowed easy access, although visitors may receive additional scrutiny by security personnel. Identity management discussed in the preceding section facilitates this process.

Vehicular Security

Transit assets may be vulnerable to vehicular threats when nontransit vehicles can access areas near or underneath transit infrastructure, vehicles, stations and stops, and entrances to transit facilities. Vehicle barriers protect against bombs in a moving vehicle, bombs in a stationary vehicle, or forced entry and also can protect against theft and contribute to pedestrian safety. Traffic calming devices and traffic con-

figuration strategies can be used to slow vehicular traffic in areas surrounding a transit station or facility. CPTED strategies for security of facilities are discussed in the Station/Terminal and Transit Facility sections later in this chapter.

Access control techniques can be used to enhance security for transit facility parking lots. Manual checking would be feasible when a limited number of vehicles need to be searched. Electronic methods such as automated license plate readers may be considered for use in higher-volume facilities or unattended parking areas. Automated license plate readers read plate numbers of vehicles entering a checkpoint and automatically compare them against a list of authorized numbers. If there is a match, the vehicle will be allowed to enter the premises. License plate and vehicle images along with driver images and times and dates for highly secure facilities may be stored for future use (Nakanishi and Western 2005b). The use of biometric readers, electronic card readers, or specially issued stickers or placards are alternative access control methods.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

Transit systems supply criminals not only with targets, but also cover in dark passageways and hidden corners of the systems. Isolated areas of the system during off-peak periods allow criminals to target passengers who already may have a heightened level of fear. Situations that otherwise are not threatening may be threatening when they take place within a transit system environment (e.g., an aggressive panhandler blocking a narrow passageway) or onboard a transit vehicle.

The theoretical basis of Situational Crime Prevention (SCP) is rational choice. The offender decides to commit a crime based on risks, efforts, and rewards. SCP attempts to make the risks and efforts greater than the rewards. The five key categories of SCP techniques are increasing perceived effort, increasing perceived risks, reducing anticipated rewards, reducing provocations, and removing the excuses (Clark 1997). (CPTED) used by many transit agencies to address security issues is “a method of situational crime prevention that is based on the premise that the proper design and effective use of the built environment can lead to a reduction in crime and an improvement in the quality of life” (FTA 2004) and is believed to have a significant impact on crime rates and the customer perception of security (Reed et al. 2000).

CPTED strategies include enhancing visibility of passenger terminals and rail stations by the use of bright lighting and mirrors, eliminating hiding places such as dark corners, eliminating unnecessary columns, and strategically placing vendors such as newsstands. These strategies are effective in countering terrorism by eliminating hiding spaces that pro-

vide cover for terrorists and for explosives. Clear signage, easy-to-remember timetables, and any other measure that lessens confusion will hinder the efforts of criminals to take advantage of lost or confused passengers (Nelson 1997). Although older systems may not be able to implement some of the CPTED strategies, transit stations and facilities can be retrofit and redesigned during renovation efforts.

Metropolitan Atlanta Rapid Transit Authority (MARTA) has been upgrading lighting in its rail stations, parking lots, and other special-use facilities. The lighting program, which is expected to be complete in 2010, has a budget of approximately \$15 million. Design considerations included color rendering and vertical luminance, expected foot-candle readings in critical areas, and computer photometric analysis (Goodfellow 2005). The Washington Metropolitan Area Transit Authority's (WMATA's) heavy rail stations have been designed to enhance sightlines and minimize hiding places.

Transit vehicle design measures are a subset of CPTED measures. Typically, newer rail cars are designed with CPTED principles to enhance visibility within the train cars. Because clear and audible communications systems are important during regular transit operations and during emergencies and incidents, many transit agencies use public address systems to communicate with their passengers. Many transit vehicles also have silent alarms and emergency call buttons for their employees. These results reflect the findings of an Advanced Public Transportation Systems (APTS) deployment report that indicated that more than 80% of agencies in the 78 largest metropolitan areas and 45% of agencies in the rest of the United States had deployed or were planning to deploy silent alarms (Radin 2005). Silent alarm and emergency call buttons can be linked with covert microphones, which allow dispatchers and responders to listen in during emergency situations, or with AVL systems, which allow dispatchers and responders to identify the location of the vehicle in distress.

The following are rail car and station, bus and bus stop, and transit facility CPTED design and SCP measures based on the project findings. Some of these measures such as improving visibility enhance both actual security and passenger perception of security.

Rail Car

Following are the rail car CPTED design and SCP measures:

- Install access control to operate the train.
- Install communications, vehicle location, and alarm systems:
 - Train location system (e.g., Communications Based Train Control);
 - Radios for train personnel;

- Passenger alarm buttons with a voice link to train operators on rail cars;
- Silent alarms for train operators linked to control center, dispatch, or police; and
- Public address systems with battery backup.
- Improve visibility:
 - Use bright lighting, colors, and materials;
 - Eliminate potential hiding spaces;
 - Help train operator see inside the rail cars (video or mirrors);
 - Install emergency lighting;
- Modularize components (as noted in the FTA *Transit Security Design Considerations* report, modular components such as seating have fewer parts and will create less shrapnel in case of explosions; replacement of these components is easier so future upgrades will be affordable).
- Secure components:
 - Harden fuel, engine, and electrical compartments;
 - Harden fuel tanks, electrical wiring and fuel lines;
- Comply with appropriate safety design and materials standards.
- Install video technology.
- Other:
 - Encourage passengers to ride in the same subway car as the conductor during off-peak hours;
 - Install radiological pagers inside and outside of train cars;
 - Perform blast analysis for all applicable train components;
 - Install power kill switch; and
 - Place car number on roof.

Bus

Following are the bus CPTED design and SCP measures:

- Improve visibility
 - Use bright lighting, colors, and materials
 - Eliminate wrap-around advertisements
 - Eliminate potential hiding spaces.
- Install access control (e.g., key ignition system).
- Modularize components.
- Secure components
 - Secure bus operator compartments
 - Harden fuel, engine, and electrical compartments
 - Harden fuel tanks, electrical wiring, and fuel lines.
- Comply with appropriate safety design and materials standards.
- Deploy video technology.
- Install communications, vehicle location, and alarm systems
 - Install AVL systems on buses to track and monitor buses
 - Install silent alarms connected to bus signage, bus control center/dispatch, or police
 - Install mobile data terminals to exchange messages with the control/dispatch center

- Install Drive Cams (event-triggered cameras focused on drivers).
- Other
 - Place bus vehicle numbers on roof of the bus
 - Install chemical detection sensors.

Station/Terminal

Some of these station and terminal design strategies can be implemented in existing stations, but others may be too costly or otherwise infeasible and would be more appropriate for incorporation into the design of new stations. These strategies include the following:

- Improve perimeter security
 - Strategically locate structures (away from roads and parking areas)
 - Install physical or natural barriers for vehicles and setbacks to prevent use of vehicles as weapons
 - Minimize number of vehicle entrances and access points.
- Improve visibility
 - Clear sightlines surrounding the station
 - Locate operator booth for maximum visibility
 - Improve lighting, colors, materials, and mirrors
 - Minimize hiding places.
- Secure critical assets
 - Locate critical assets and nonpublic areas away from the public and from any vulnerable locations
 - Secure critical equipment.
- Deploy clear, appropriate signage and indicate public versus nonpublic areas.
- Install new or better communication and alarm systems
 - Install communication links and backup communications for transit police and personnel
 - Install call boxes in passenger waiting areas to provide passengers with a voice link to transit police or personnel
 - Install or upgrade public address system
 - Install intrusion detectors/alarms on vehicle entrances, entrances to sensitive areas, and to rail ROW.
- Comply with appropriate safety design and materials standards.
- Install video technology.
- Secure trash receptacles (explosive-proof or transparent).

Bus Stop

Bus stops and some light rail stops that are similar to bus stops fall under this category. The results of a 2001 research study indicated that the bus stop shelter should not be fully enclosed to provide customers a quick escape in an emergency and should have good visibility with unobstructed sightlines (Lusk 2001). Shelters should be located a certain

minimum distance from the roadway. Other design measures include the following:

- Deploy signage to deter nontransit vehicles from the stop area.
- Anchor structures and street furniture to prevent being dislodged.
- Choose materials to minimize flying glass and debris.
- Install emergency call boxes for passengers.
- Use appropriate lighting.

Transit Facility

Many of the transit facility measures are similar to transit station and terminal measures, such as those related to perimeter security and the use of special materials. Specific facility location measures may be useful for agencies considering relocation of their facilities (FTA 2004). They include the following:

- Choose inconspicuous facility location.
- Colocate with facilities having similar security needs.
- Ensure securable perimeter with unobstructed sightlines.
- Secure strategic location of structures (away from roads and parking areas).
- Minimize number of access points.
- Secure and locate critical assets and equipment within the core of multiple layers of security.
- Each activity zone should have a different purpose, with outer layers reserved for the public and visitors.
- Ensure ability to isolate critical areas and maintain operations.

In addition to FTA's *Transit Security Design Handbook*, the Federal Emergency Management Agency (FEMA) publishes references on building protection that are applicable to transit facilities including stations and administrative buildings. A compelling account of the Port Authority Bus Terminal Turnaround (Felson et al. 1996) is provided in *Preventing Mass Transit Crime* and has been summarized in the literature review. In the late 1980s, the large and busy bus transit transfer facility was plagued with both major and minor crimes that had escalated to an uncontrollable level. Once CPTED and SCP strategies were implemented, there was a significant decrease in crime and an increase in customer perceptions of security within the bus terminal.

Other CPTED resources and training sources include the following:

- ASIS International (www.asisonline.org).
- The National Institute of Crime Prevention (www.nicp.org).
- The National Crime Prevention Council (www.ncpc.org).

PATROLS, PLAINCLOTHES, AND VISUAL SURVEILLANCE

The composition of a transit agency's security personnel affects the agency's policing and security management. For instance, having many in-house sworn officers may be more effective in combating recurring violence within a multimodal transit system serving urban areas. At the same time, having part-time contracted officers versus full-time in-house security personnel may give a small agency with budget constraints more flexibility. Most transit agencies have some combination of full-time and part-time, sworn and nonsworn, and in-house and contracted security personnel. Nineteen of the FTA's top 50 transit agencies have in-house sworn officers. The agencies that had in-house sworn officers were more likely to be multimodal or rail-only agencies.

According to the survey respondents and case studies, multimodal and rail-only agencies have moderately or significantly increased either the number of their security personnel or security staff hours after 9/11. The typical bus agency, however, increased either the number of its security personnel or security staff hours after 9/11 only by a small or moderate percentage, and some bus agencies made no changes.

Patrols such as foot patrol are a conventional and effective tactic used by agencies to combat crime on transit vehicles. Bicycle patrols are conducted by BART police as noted in the BART case study (see chapter six). A survey respondent noted that at the agency's park-and-ride facilities, surveillance by plainclothes officers in unmarked vehicles succeeded in significantly reducing motor vehicle crimes.

In response to 9/11, high-visibility patrols were initiated by transit agencies, mainly multimodal agencies and rail systems, to enhance security and increase passenger perception of security. High-visibility patrols are made highly visible through the saturation of specific locations with multiple specially uniformed officers and the use of visible tactical vests. Officers may arrive as a team at stations unscheduled to perform highly visible station or train sweeps. Train Order Maintenance Sweeps (TOMs) or a similar method are used by some of the rail systems—TOM teams also arrive unannounced and alert the conductor that they will be performing a sweep of the train. They spread out on the platform and each officer steps onto a train car and performs a visual screening of the car. Regular aerial surveillance performed by a commuter rail system can also ensure the security of rail infrastructure.

TSA's VIPR teams may consist of federal air marshals, transportation security inspectors, transportation security officers, explosives-detection canine teams, behavioral detection officers, explosives security specialists, and necessary supporting equipment. VIPR teams work with local security and law enforcement officials to supplement

existing security resources, provide deterrent presence and detection capabilities, and introduce elements of randomness and unpredictability to disrupt potential terrorist planning activities. To enhance the effectiveness of VIPR teams, TSA and the representatives of the Transit Policing and Security Peer Advisory Group worked cooperatively to improve coordination, preparation, planning, execution, and after-action review of VIPR deployments in mass transit and passenger rail systems. This cooperation culminated with the completion of mutually agreed-on operating guidelines for "Effective Employment of VIPR Teams in Mass Transit and Passenger Rail." The guidelines have been distributed to Federal Security Directors (FSDs), Assistant Federal Security Directors (AFSDs) (Surface), and Federal Air Marshals Special Agent in Charge (FAMSACs) around the country by the Joint Coordinating Committee to improve the effectiveness of the VIPR program. A follow-on product, developed and distributed in February 2008, details the roles and capabilities of the multiple TSA resources available to participate in VIPR deployments and provides recommendations on effective deployment in antiterrorism activities.

Plainclothes officers are used by transit police to combat crime and terrorism. For rail systems operating on the honor system, fare-checking efforts act as a security measure as well. Several respondents reported that they practice behavioral assessment by transit staff or security staff.

VIDEO SURVEILLANCE



FIGURE 4 Video Technology (Source: *TCRP Report 86, Volume 4*).

Video surveillance, which has been widely used by transit agencies for a number of years to protect their systems and infrastructure, is believed to deter both crime and terrorism, and enhance transit customer perception of security. Newer video technology uses digital systems with digital video recorders or network video recorders, and this new technol-

ogy is easier to network and integrate with other technologies (see Figure 4).

Bus agencies use video technology to deter crime and investigate criminal incidents, traffic accidents, and passenger injury claims. In Albany, New York, the Capital District Transportation Authority (CDTA) is installing digital video cameras in its bus fleet to deter assaults, vandalism, other crimes, and terrorism. In New Orleans, when cameras were installed on buses, criminal incidents including fare evasion and false injury claims decreased (“Cameras on Buses” 2002). Subway systems use cameras to deter and detect crime and terrorism—the MBTA has cameras in every subway station.

Commuter rail systems are installing security cameras at bridges and tunnels so that stopped vehicles and other suspicious activity may be identified and addressed. Commuter rail systems also use cameras to detect unauthorized entry onto their tracks because damage to rail infrastructure can cause train derailments. The Chicago Transit Authority (CTA) is planning the installation of cameras in its new rail cars; when a passenger pushes an emergency call button, the cameras will deliver real-time video feed to the train operator, CTA command center, and police, and an audio connection between the passenger and train crew will be enabled (Conry-Murray 2007).

Unveiled in August 2005, The Integrated Electronic Security System, Command, Communication and Control Program is planned for implementation by New York City Transit (NYCT) to enhance security throughout its transportation network and to provide incident management response and recovery capabilities. The system will enhance monitoring, surveillance, access control, intrusion detection, and response capabilities, and calls for the installation of more than 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 (MTA 2005).

Recorded video is used to determine the causes of accidents and to identify the perpetrators of assaults and other crimes committed within the transit system. In addition, false liability claims can readily be identified and disputes between passengers and drivers can be more speedily and equitably resolved. In addition, video surveillance systems are scalable and can be installed in stages. For example, one bus system, CDTA in Albany, New York, installs video surveillance with new bus procurements and is considering the implementation of software that can transmit images wirelessly onto a laptop in a police vehicle that is within a certain distance from the bus (see chapter six, CDTA case study). CTA’s \$2.4 million Mobile Security Network project will use a network of cameras and digital video recorders in

CTA’s bus fleet and rail stations to transmit video wirelessly to CTA and Chicago police vehicles that are within 600 ft of a bus (Conry-Murray 2007). A majority of agencies in the 78 largest metropolitan areas and about half of the agencies in the rest of the United States had deployed or were planning to deploy surveillance cameras within transit vehicles (Radin 2005).

Intelligent video surveillance offers transit agencies the ability to automatically identify suspicious activity, abandoned items, and unexpected movements. Intelligent video may be useful to detect potential terrorist activities as well as impending or real-time assaults, larcenies, burglaries, vandalism, drug-dealing, car thefts, and ROW intrusion. Some systems are able to track the movement of a suspect in a crowded environment. Also, linking these systems with chemical or other threat-detection systems can allow real-time images to be automatically sent to a control center if the detection system alarm sounds. Automated surveillance is believed to be more accurate than conventional surveillance because of the inability of humans to constantly monitor numerous screens. After only 20 minutes, the ability of the operator to concentrate on a monitor decreases by as much as 90% (Gomersall n.d.). Intelligent video saves personnel hours and is more scalable because it is possible to expand the systems without having to hire and train additional personnel.

Video analytics, preset algorithms built into the software to identify specific behaviors or conditions, are able to work with multiple camera types as long as images are recorded onto a video recorder (Gomersall n.d.). Houston Metro uses intelligent video surveillance at their park-and-ride facilities to prevent vehicle thefts, burglaries, and vandalism and to ensure the security of their passengers. The cameras can be controlled from a central operations center at TranStar; at the center, Metro police officers are able to turn, pan, and zoom the camera images in to specific areas of the facility. They can control the lot’s electronic gates and speak to the drivers when necessary from TranStar (On-Net Surveillance Systems, Inc. n.d.). The Maryland Transit Administration and DHS developed an intelligent video surveillance system that is being installed in the Maryland Transit Administration’s Baltimore metro subway, the Maryland Area Regional Commuter (MARC) rail service, and Baltimore light rail stations with a \$12.7 million state and federal grant. The cameras will focus on rail station platforms, surrounding areas, and valuable equipment. The video analytics software will scan images and detect unusual movement and activity such as intrusions, suspicious activity, and abandoned items. The surveillance system allows viewing of a map of the transit systems and selection of desired camera views to monitor (“Maryland Transit Deploys Intelligent Video” 2006). MBTA is also planning to implement intelligent video software capable of identifying suspicious behavior and objects (for additional details about the MBTA’s video surveillance and monitoring system, see chapter six).

Audio analysis is able to detect gunshots and screaming and to estimate the location of a shooting or some other incident through triangulation techniques; it is now being used in some urban crime response and prevention applications. Transit agencies may consider the combined use of both video and audio analytics for an even more effective surveillance solution. One survey respondent reported using audio technology as a security measure.

Currently, intelligent video and audio analytics are not widely used by transit systems, but many systems are considering implementation. Other future applications of intelligent video include the use of facial recognition analytics, which would enable transit agencies to scan crowded terminals and stations for wanted terrorists or criminals, and the use of radiological detection sensors in conjunction with intelligent video (if the sensor detects a threat, intelligent video cameras may be able to track the source of the radiation).

Although, generally, video is an excellent, scalable security solution and addresses multiple security needs, issues such as desired image quality, compatibility with legacy systems, and maintenance and storage requirements should be considered in the planning process. Transit systems that have older analog video equipment from different manufacturers, and systems that use video systems without recorders may experience increased complexity in upgrading their technology.

PASSENGER SECURITY INSPECTIONS

Passenger Security Inspections (PSIs), described in detail in *TCRP Report 86, Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers* (TRB 2007b), are suspicionless inspections of transit passengers by transit security or staff. PSIs are believed to both deter and detect terrorist activity and are being used by larger multimodal agencies and by ferry systems. A benefit of PSIs is the relative ease with which screening intensity (rates), method, and location can be altered based on the threat level and other intelligence information. Because the Fourth Amendment requires warrants or individual suspicion to conduct inspections, PSIs are legally permissible only if they can be justified. Therefore, legal and other issues need to be carefully considered by transit agencies before implementation. The PSI decision-making model recommended in *TCRP Report 86, Volume 13*, is an excellent way for transit agencies to deter-

mine whether to use PSI, which PSI to use, and how to implement it.

Random Bag Inspections

Random bag inspections conducted manually or with the aid of portable trace detectors are a form of PSIs currently being performed by large multimodal agencies within their rail systems and by ferry operators.

- In Boston, the MBTA began conducting PSIs during the Democratic National Convention in 2004. The PSI program was suspended until October 6, 2006, when the program resumed on a systemwide basis for MBTA's subways, buses, ferry boats, and commuter rail systems.
- In the NY/NJ metropolitan area, MTA (subways and rail) and NJ Transit (rail) initiated the PSI program of random passenger bag inspections immediately after the second London transit bombing in July 2005.
- Ferry operators initiated PSI programs in response to the Maritime Transportation Security Act of 2002 mandate of a number of security measures, including PSIs.
- Amtrak started a PSI program involving the random screening of carry-on bags in February 2008.

Canine Teams



FIGURE 5 MBTA Transit PD Canine Team (Courtesy: MBTA).

Canines with explosives-detection capability as part of regular or high-visibility patrol teams are considered an excellent PSI option because of their ability to detect explosives and their source, unobtrusiveness, and adaptability to the transit environment (see Figure 5). Their drawbacks are their inability to work for long periods and their need for continuous training.



FIGURE 6 MTA Customer Awareness Poster for New York City subways, buses, and rail cars (Courtesy: MTA).

TSA's NEDCTP was expanded in 2005 to encourage the use of canine teams for explosives detection on transit and commuter rail. Previously, canine teams have been used primarily at airports by the TSA. The canines are screened to ensure an acceptable temperament and excellent sensory ability. By the end of 2007, 62 TSA-certified explosives-detection canine teams were deployed in a risk-based approach to 14 transit systems across the country. These teams provide a visible and effective detection and deterrence capability in the public transportation system and can be surged to other venues as threats dictate. Their mobility enables deployment randomly and unpredictably in patrols throughout passenger rail and mass transit systems and postings at key junctions or points within systems, stations, terminals, and facilities.

Agencies selected for the program included MBTA, BART, Southeastern Pennsylvania Transportation Authority (SEPTA), WMATA, PATH, CTA, LACMTA (Metro), Maryland Transit Administration, San Francisco Municipal Railway (Muni), and San Diego Trolley, Inc. (TSA 2008). Other agencies using canine teams include NYCT (see Figure 6), New Jersey Transit (NJT), MARTA, Houston METRO, Niagara Frontier Transportation Authority, and Tri-County Rail (TSA 2005).

The NEDCTP established protocols for other agencies and departments to request the temporary use of TSA-certified canine teams during National Special Security Events and level 1 and 2 stolen explosive and recovery events. Additionally, the Transit Security Grant Program guidance has been revised to allow eligible agencies to procure the canines

and training of the team through other sources that meet the TSA standard. Highly trained and certified canine teams continue to be one of the more effective and highly mobile explosives-detection methods in the mass transit and passenger rail environment.

Behavioral Assessment

Behavioral assessment consists of training security officers and transit personnel to identify suspicious behavior. The assessment is cost-effective because it does not require capital investment or the hiring of additional personnel. Israel experienced success with their program at airports and shopping malls, which was aimed at identifying potential suicide bombers. Boston's Logan Airport, the first U.S. airport to start using the behavioral assessment technique, implemented the system soon after 9/11, and MBTA Transit officers have been trained in the technique. Some ferry operators have trained their ferry employees in the technique to enhance the security at ferry terminals. In the normal course of selling tickets or providing information, ferry workers come into contact with potential ferry passengers and can continually perform behavioral assessment to spot suspicious individuals during their work day. Several survey respondents reported that they practice behavioral assessment by transit staff or security staff.

THREAT DETECTION TECHNOLOGIES

Currently, the threat detection technologies in use by transit agencies include portable trace detection equipment and radiological pagers. An Innovations Deserving Exploratory Analysis (IDEA) project has produced a working prototype to detect dangerous levels of radioactivity in rail transit stations. The fully developed product will be able to detect dirty bombs using digital cameras as the radiation detector and can be connected with appropriate software to disseminate alerts to responders (Rubenstein 2006).

Chemical and biological threat sensors have been tested and continue to be tested by MBTA, NYCT, and other large transit systems. According to industry experts, chemical sensors are three to five years from off-the-shelf availability to transit agencies. These threat detection systems can be linked to event-triggered video cameras; if the detection system alarm sounds, video cameras would automatically transmit images of the relevant location to a central command center.

Although airport-style explosives-detection passenger screening equipment has been tested at selected transit systems, transit agencies are not convinced of their operational feasibility within their transit settings. Other equipment being tested does not cause delays to passengers and may be more promising: For instance, portable heat-sensing

equipment using millimeter waves can detect explosives strapped to suicide bombers at a maximum distance of 20 yards and currently is being tested at rail and bus stations (Frank 2007).

Trace detection technology focuses on detecting vapors or particles given off by explosives. A fingertip trace detection scan for integration with transit ticket vending machines is being developed. SEPTA uses portable trace explosives-detection devices enclosed in a suitcase-style container along with its canine units to rapidly and safely screen unattended or suspicious packages, reducing service delays caused by false alarms (TRB 2007b).

TUNNEL SECURITY

Protecting high-risk underwater and underground assets is a high federal priority. The National Tunnel Security Initiative is an interagency working group formed by TSA, DHS, and U.S.DOT that brings together subject matter experts from a range of relevant fields to identify, assess, and prioritize the risk to mass transit systems with underwater tunnels. The effort assists transit agencies in planning and implementing protective measures to deter and prevent attacks, mitigate blast effects, and enhance prevention and emergency response capabilities. Through regular meetings, this initiative has produced tunnel-specific risk-mitigation strategies, engaged security partners from passenger rail systems that operate in underwater tunnels, analyzed and applied the results of risk assessments, prepared statements of work for testing and modeling programs, and integrated the overall risk-mitigation effort for a cohesive, coordinated, and effective approach. Accomplishments completed to date include the following:

- Identified and assessed risk to underwater tunnels,
- Prioritized tunnel risk mitigation based on risk to drive DHS Transportation Security Grant Program funding to most pressing areas, and
- Produced and disseminated recommended protective measures that transit agencies may implement to enhance security with available resources or through targeted grant funding.

The working group has developed strategies to fund future technology research and development aimed at producing novel approaches to this challenging problem. For example, TSA is forming a partnership with the DHS/S&T on a new program called “Resilient Tunnel.” This program aims to address post-9/11 concerns that terrorists will target vulnerable tunnels causing catastrophic damages. Resilient Tunnel is a High Impact Technology Solutions project that specifically is pursuing novel solutions to protect critical transportation tunnels. The working group has developed priorities for tunnel-related transit security grant projects,

such as enhanced surveillance and detection capabilities, antiterrorism operational teams integrating dedicated law enforcement officers with explosives-detection canine patrols for enhanced deterrence, and bolstered detection capabilities through antiterrorism training, drills, and exercises and multimedia public awareness activities.

In New York City, security checkpoints have been created at MTA and Port Authority Bridge and Tunnel crossings where vehicles are randomly inspected. Because bus and rail transit vehicles share ROW and infrastructure with other traffic, this is an important security measure. Terrorists have been known to use trucks as weapons or to transport threat materials; in a 10-year period, there have been 150 attacks worldwide using trucks (Kilcarr 2003). BART has alarms on key access points to the underwater tunnel, including vent structure and portal intrusion alarms. MBTA has designed a motion-detection system that is connected to cameras in underwater tunnels; if the system detects an unauthorized person(s), an alarm is triggered and images are sent from the camera to a control center. Installation of the system is scheduled to begin in 2008.

TCRP Report 86, Volume 12: Making Transportation Tunnels Safe and Secure provides a detailed look at the vulnerabilities of tunnels and a description of the various countermeasures that may be taken by the tunnel operator (TRB 2007a).

OTHER MEASURES

Station Managers and Agents

At BART, station agents are responsible for performing security sweeps and reporting suspicious activity or items. A station manager program implemented in 1990 by NYCT created a highly visible position of station manager for selected stations. The manager “owned” their stations and was responsible for coordinating all aspects of transit service and operations, including passenger security and safety. They were physically present in various areas of the station, constantly communicated with transit customers, and reported suspicious activity (Kelling and Coles 1997b).

Operational Strategies

The survey respondents indicated that they have implemented the following operational strategies. No particular strategy dominated the responses.

Fleet Management and Vehicle Tracking

AVL systems use Global Positioning Systems and other technologies to determine the location of transit vehicles. Half of agencies in all areas of the United States and 66% of agen-

cies in the 78 largest metropolitan areas report implementing or planning to implement this technology, according to FTA's APTS deployment report (Radin 2005).

WMATA replaced its legacy pushbutton control panel at its Falls Church yard with a Domain Operator Controller System (see Figure 7), which allows WMATA to track all of its train car movements through the yard from a central control center (Judge 2007).

Other operational measures reported by survey respondents included the following:

- Inventory Control
- Limiting Station Access
- Modifying Hours of Service
- Modification of Dispatcher Responsibilities
- Modifying Pretrip Inspections
- Parking Lot, Vehicle Flow/Placement Reconfiguration
- Strategic Location of Bus Stops.

Other security measures also include the following:

- Forming a graffiti task force to address graffiti problems.
- Offering rewards to the public and employees for crime tips.
- Placing report cards stating burglary risk on vehicles parked [this has been effective within the Utah Transit Authority park-and-ride facilities to encourage passengers to take additional precautions regarding their vehicles].

operations, storage, and emergency response procedures for different types of emergencies involving natural gas (Murphy 2005).

CYBER SECURITY

The E-Government Act of 2002 (Public Law No. 107-347, Sections 301-305) recognized the importance of information security to the U.S. economy and national security ("Evaluation of DHS' Information Security Program for Fiscal Year 2007" 2007). In addition to having a standardized information technology (IT) policy to protect employee data and sensitive information, the primary cyber-security measures recommended by the IT literature are restricting access to devices (PCs, laptops, mobile) that are linked to the network; firewalls at all public-private network transit points; virus protection software; complex passwords; and centralized authentication of user identity. Additional measures include turning off unneeded ports, centralized security updates, and monitoring for suspicious activity. Because mobile devices and remote connections are especially vulnerable, data encryption and other additional measures are recommended (Leidigh 2005).

Firewalls to prevent unauthorized network access and access control using passwords were the most frequently mentioned cyber-security measures by survey respondents. Other measures in use included physical access control to the server room, power backups and redundancy, and constant data backups. A few agencies reported using biometric technologies. Recent introductions of portable biometric systems

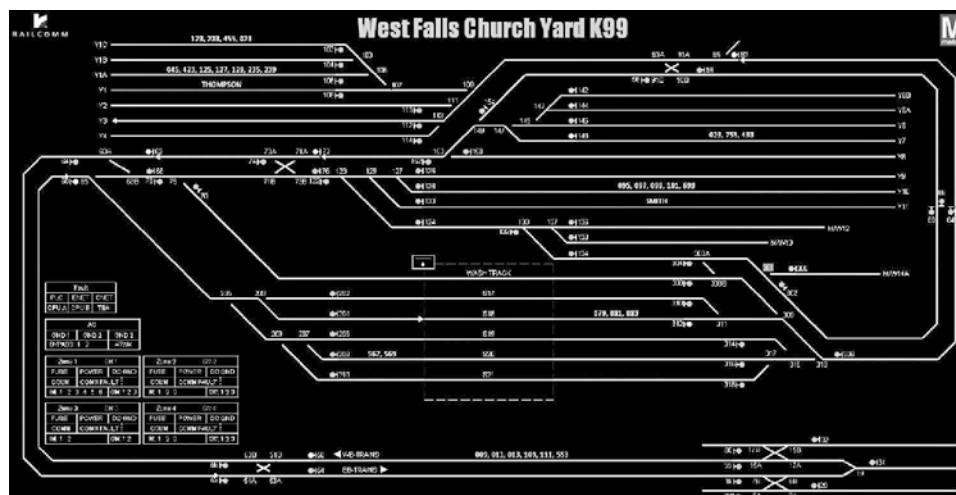


FIGURE 7 WMATA's Domain Operator Controller System Screenshot (Courtesy: RailComm).

The specialized topic of how to handle natural gas transit vehicle emergencies is studied in *TCRP Synthesis 58: Emergency Response Procedures for Natural Gas Transit Vehicles*. The Synthesis report provides information about the special considerations necessary for natural gas fuel usage,

that remain in the possession of the user alleviate some of the privacy-related issues associated with biometrics.

Additional cyber-security information can be found from the National Cyber Security Alliance at <http://www.nccsa.org>.

staysafeonline.info/, as well as in the FTA's *Transit Agency Security and Emergency Management Protective Measures* report (Batelle, TotalSecurity US, and Transportation Research Associates 2006).

COMMUNICATIONS SECURITY AND REDUNDANCY

Communications security and cyber security are interrelated. Cyber attacks can disable communications systems that are crucial in daily transit operations and in emergency situations. Most survey respondents stated that they have network security measures in place, most have power supply backups, and many have redundant communications systems. Respondents noted that these measures had been implemented during the post-9/11 period.

Maintaining the functionality of a security system including communications during an attack is critical, especially if one part of the system has been disabled (FTA 2004). Redundancy is also important for continuity of operations. The extent to which agencies practice redundancy differs: Some agencies continuously back up their data and store the backups in a separate location. One agency maintains a separate command center in the event the primary command center is destroyed or otherwise rendered unusable.

INTEROPERABLE COMMUNICATIONS

Interoperable communications facilitates the ability of personnel and equipment from different agencies and entities to share and communicate information and data, including video feeds, and is vital during emergency response and recovery efforts. Wireless communications interoperability, the ability of personnel to share information through voice and data signals on demand, in real time, when needed, and as authorized is especially significant during emergencies ("SafeCom Program" n.d.). Communications interoperability, including wireless communications, requires the resolution of many operational and technical problems and remains a difficult challenge for transit police departments. Many have serious problems with tactical communication with the local police agencies within their service area. In the NYC metropolitan area, \$34 million in DHS Public Safety Interoperable Communications Grant Program funds were released as part of the Urban Area Security Initiative. The NYC Urban Area Security Initiative region covers New York City, Yonkers, Westchester, Nassau, and Suffolk counties, and the Port Authority of New York and New Jersey. The funds will be used to enhance communication within the MTA tunnel system; create a shared communication

platform for first responder agencies; and enhance public safety communications technology within the PATH system ("\$34 Million for NYC Metro Area" 2008). NJT is implementing an emergency response system integrating dispatch, records, and mobile field reporting capabilities and enabling NJT personnel and responders to access real-time intelligence. The system will feature a transit system map showing the locations of incidents and will have the capability for cross-agency information sharing (Starcic 2008). WMATA has had a great deal of success in communications interoperability; the agency's successes are profiled in chapter six.

DHS/S&T's Command, Control and Interoperability Division actively promotes communications interoperability through the provision of grants, technical assistance, standards formation, and the creation of programs such as SafeCom. SafeCom continues to improve interoperability by producing a Statement of Requirements, which describes the steps needed to achieve full interoperability and a Statewide Communications Interoperability Planning Methodology.

SAFECOM's RapidCom initiative ensured that a minimum level of emergency response interoperability would be in place in 10 high-threat urban areas ("SafeCom Program" n.d.).

COLLABORATIVE TRANSPORTATION IMAGERY PROJECT

TSA and its partner agencies are working jointly on the Collaborative Transportation Imagery Project to produce detailed mapping and interactive imagery of key assets and systems to inform and enhance the quality of operational activities and address threats and security incidents, security plans, training programs, and exercises. The product, in digital video format, incorporates multiple types of imagery, satellite maps, schematics, and related materials to provide a comprehensive view of the transit system, detailing significant infrastructure and security apparatus.

These may include overhead imagery, architectural drawings on the physical layout of the facility, and access modes to the facility (i.e., roadways, rail links, water frontage, utilities, sidewalks, vents, and so on). The product is produced at the sensitive security information (SSI) classification level to permit controlled distribution among an agency's management, security, and operating officials; local law enforcement agencies; fire and emergency medical service personnel; and TSA Federal Security Directors (FSD) and their staffs.

CHAPTER FOUR

SECURITY PRACTICES

Security practices presented in this chapter include those relevant to both terrorism and crime. They include security and policing management; security resource allocation; risk management and security planning; regional coordination, cooperative relationships, and intelligence information; customer outreach, education/training, and awareness; employee security and policing training; evaluation procedures, drills, and covert testing; and ferry security. Youth outreach strategies are also discussed in this chapter. These and other security practices are described further for each case study agency in chapter six.

Transit agencies, according to Synthesis findings, have made numerous changes and enhancements to their security practices as a response to the attacks on September 11, 2001. The primary changes were the implementation or enhancement of the following:

- Transit Watch or similar employee and passenger awareness and outreach program;
- Security training for employees, and increased counterterrorism training for security personnel and transit police officers;
- Threat and vulnerability assessments (TVAs) as part of a stronger overall risk management effort;
- Increases in security personnel or hours, including the addition of security personnel where there were none;
- Plainclothes efforts;
- Background checks;
- Security drills and exercises;
- Cooperative relationships and regional coordination including participation in local and regional counterterrorism committees;
- Receipt of intelligence, and intelligence and information sharing; and
- Additional investment in security programs and measures and their incorporation into the budgeting and planning processes.

In line with these findings, FTA's *Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies* reports that the largest 50 agencies demonstrated "significant strengths in critical areas of importance" (Bahr et al. 2007). Synthesis results indicate that smaller agencies also have implemented core security practices. In other areas,

however, practices varied across agencies because of differing agency policies, TVA results, needs and constraints, and operating environments.

SECURITY AND POLICING MANAGEMENT

The "Broken Windows" theory links minor crimes, disorder, and quality-of-life problems with more serious crime. Addressing minor disorder is believed to mitigate and prevent serious crimes from occurring (Kelling and Coles 1997a). Those who commit minor offenses often have outstanding warrants or criminal records, and they will go on to commit more serious crimes. The public perception of security also diminishes as minor disorders increase. This poor perception will cause the ridership to decline and "sets in motion an inevitable cycle of deterioration spurred by the decline in revenues and the migration of potential middle-class and affluent riders to other modes of transportation" (Nelson 1997). At the same time, for a significant impact on crime to occur, the focus should not only be on minor crimes but also on serious crimes.

In 1989, the NYC subway system was experiencing problems with both serious and minor crimes such as "visible homeless people on the system, ubiquitous panhandling and begging, and roving banks of uncontrolled youths riding the subways" (Widawsky 1989, p. 3). At the time, even the NYC passenger advocacy group—Permanent Citizens Advisory Committee—believed that "crime happens," stating that the "incidence of crime is steady and somewhat predictable" and that efforts by the transit police to reduce crime would be "self-defeating" (Widawsky 1989, p. 4). MTA's "total commitment to order restoration" led by NYCT Police Chief William Bratton was a comprehensive policy that targeted all types of crime—both serious and minor. The policy directing transit police to enforce subway rules implemented in the NYC subway system in 1990 was a phenomenal success. In the four-year period after 1990, felonies decreased by 75% and robberies by 64% (Kelling and Coles 1997c). (In 1995, a merger between the NYPD and the NYC transit police took place, establishing the NYPD Transit Bureau.) The model was further developed by Bratton who had become NYPD's 38th Police Commissioner in 1994, and Jack Maple Deputy

Police Commissioner for Crime-control Strategies, when they joined the NYPD.

The NYPD model, CompStat, systematized information sharing among units and among different levels of the NYPD. At the core of the model was up-to-date crime statistics that were mapped and used to forecast crime and evaluate crime-reduction practices. Commanders were accountable for results within their precincts and were empowered to initiate staffing and resource deployment recommendations and plans to reduce and prevent crime. Commander profiles, which included each precinct commander's background and training, performance, demographics, crime statistics, response time, and absences, were created and provided to senior management for promotion and transfer decisions. Also, officers at all levels of the organization were expected to contribute to the development of crime-fighting tactics and problem-solving efforts (McDonald 2001). See Appendix B for additional information about CompStat.

Currently, transit agencies outside of New York City that have implemented CompStat or portions of the model include MBTA, NJT, MARTA, and MTA (P.P. McDonald personal communication, Feb. 19, 2008). Since the 1995 merger of the NYC transit police with NYPD, the transit police department is now situated within the NYPD.

Community Policing

The community in transit systems includes transit passengers and transit workers who are the eyes and ears of transit police; the community also includes vendors within the system or in the surrounding neighborhoods. The constant presence of the same officers will establish a rapport between the officers and the community, and will allow transit police to obtain useful information and garner their cooperation during emergencies. Community policing is practiced by transit police forces because the effectiveness of security and crime-prevention measures is often associated with the willingness of the public to provide information about crimes and suspicious persons or activities, and relies on citizens to set limits on disorderly behavior. Community policing also supports decentralization of police forces, allowing flexible responses to local problems (Kelling and Coles 1997d). Additional information about community policing is provided in Appendix B.

Rules and Codes of Conduct

Unlike in public places, transit systems have set clear boundaries and have established specific codes of conduct or rules by which passengers must abide. These codes can contribute to conflict mitigation and prevention of assaults. Transit agencies have a passenger code of conduct in place, including all 22 transit agencies responding to the survey question. Because many persons arrested for code-of-conduct infractions have outstanding warrants or carry illegal weapons,

disorder and minor crimes are prevented or mitigated and serious crimes are deterred by enforcing these rules (Kelling and Coles 1997a).

SECURITY RESOURCE ALLOCATION

Security resource deployment decisions are complex and are based on a variety of factors such as intelligence information; crime and incident statistics and trends; information about suspicious activity; available budget, personnel, and technologies; and results of planning and budgeting tools. The FTA's Security Manpower Planning Model is a flexible decision support tool created to run within Microsoft Excel 2003. The model enables transit security planners to assess the impacts of strategic decisions on resources and staffing. Based on the data input, the model identifies staffing levels and budgeting. The model can be used by any transit agency with existing or planned security resources, regardless of operating mode(s) or size. Furthermore, the model can help security planners assess the impacts of various scenarios on resource and deployment strategies (Security Manpower Planning Model May 2008).

Almost all responding agencies (30 of 33) stated they were currently making moderate to high investments in CPTED, which was followed closely by technology and employee training, and customer outreach and education. Fewer agencies reported additional investments in security personnel, perhaps because investments were made in the few years immediately following 9/11. All responding agencies reported that security investments have had a positive impact on crime mitigation, terrorist deterrence and detection capabilities, and public and passenger perception of security.

RISK MANAGEMENT AND SECURITY PLANNING

TSA works with mass transit and passenger rail agencies to elevate their security posture through the BASE program. The BASE program assesses the security posture in 17 Security and Emergency Management Action Items. Developed through a joint effort of TSA, DHS, DOT, and agency security officials, the Action Items encompass activities and measures that are fundamental to an effective security program.

Security assessments commenced during fiscal year 2007 (FY07) with an initial focus on the 50 largest mass transit and passenger rail agencies. In 2007, BASE assessments were conducted in 46 of the nation's 50 largest transit agencies. To date, 64 BASE assessments have been completed in total, covering 47 of the largest 50 agencies, second assessments on two of the top 50 agencies, 10 on agencies ranked in the 51–100 size range, and five smaller agencies. Three key areas for which assessment results produced timely action

to address identified weaknesses included (1) security training in which TSA produced focused training guidance and revised and streamlined processes under the Transit Security Grant Program to expand training opportunities; (2) approval of the Transit Security Grant Program funding of antiterrorism teams (Op-Packs) in high-risk locations; and (3) development of the national exercise program mandated in the 9/11 Act, which is being pilot tested in the National Capital Region.

Transit agencies are using the results of TVAs to address vulnerabilities, allocate resources, and mitigate crime as well. The majority of responding agencies indicated that they have up-to-date security related plans, including COOPs, emergency plans, or incident response plans, and have integrated an Incident Command System (ICS) into these plans.

Additionally, TSA has produced a compilation of Smart Security Practices derived from the BASE results and has identified the implementing mass transit or passenger rail agency and its point of contact. This compilation enables mass transit and passenger rail security officials to network and discuss how the particular practice has been developed and implemented, and to consider how it may be adapted to the operational circumstances of other systems. TSA has expanded its BASE program to assess security among the largest 100 mass transit and passenger rail agencies by ridership volume. TSA surface inspectors have also assessed smaller agencies, meeting a direction of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law No. 110-53). As of May 2008, TSA inspectors have conducted BASE reviews of more than 20 bus-only systems. This figure will increase through TSA's partnership with the FTA in the Bus Safety and Security Program. Collectively, this effort helps mass transit and passenger rail agencies to identify security gaps and update their COOPs and their security and emergency plans.

Additional information about how to create, update, and execute COOPs can be found in *TCRP Report 86, Volume 8: Continuity of Operations Planning Guidelines for Transportation Agencies* (TRB 2005). For agencies developing or updating an emergency response or security plan, *TCRP Report 86, Volume 10: Hazard and Security Plan Workshop: Instructor Guide* (TRB 2006b) is a useful reference. Relevant information is also found in the FTA's *Transit Agency Security and Emergency Management Protective Measures* report (Batelle, TotalSecurity US, and Transportation Research Associates 2006). NCHRP Project 20-59(17) has produced "A Guide to Risk Management of Multimodal Transportation Infrastructure" (2006), which addresses multimodal risk by focusing on the consequences of particular threats. One of the products of the project was an Excel tool that assists multimodal agencies in prioritizing security measures to address relevant threats.

REGIONAL COORDINATION, COOPERATIVE RELATIONSHIPS, AND INTELLIGENCE INFORMATION

Actionable information such as who will be carrying out an attack and intended target(s) is essential for agencies to formulate an effective counterterrorism strategy. The National Counterterrorism Center, now within the Office of the Director of National Intelligence, has the primary federal responsibility for all terrorism-related intelligence and information analysis. The Center also has a knowledge bank and provides intelligence support on terrorists and terror groups. The National Strategy for Information Sharing "provides the vision for how our Nation will best use and build upon the information sharing innovations which have emerged post-9/11 in order to develop a fully coordinated and integrated information sharing capability that supports our efforts to combat terrorism" (National Counterterrorism Center 2007). The Strategy's core principles are as follows:

- Information sharing must be woven into all aspects of counterterrorism activity.
- The procedures, processes, and systems that support information sharing must draw on and integrate existing technical capabilities and must respect established authorities and responsibilities.
- State and major urban area fusion centers represent a valuable information-sharing resource, should be incorporated into the national information-sharing framework, and operate in a manner that respects individuals' privacy and other legal rights.

Joint Terrorism Task Forces (JTTFs) have been created in major cities to improve state and local information-sharing efforts. All agencies responding to Questions 25 or 26 reported that they have cooperative relationships with external agencies and many reported that their policing and security units have cooperative relationships with other units within their own agency.

Specific intelligence can guide the agency regarding the nature of the threat against each of its modes and may provide specific information on how, when, and where to implement security measures. Transit agencies receive frequent periodic intelligence from DHS/TSA, FBI, U.S.DOT, FTA, and local law enforcement agencies. Some agencies engage in intelligence and information sharing with other transit agencies and first responders, and participate in regional counterterrorism committees or other regional security-related groups. A few survey respondents indicated that the intelligence they receive is often too general and that they would like the intelligence to be more focused to their system and region. The largest agencies, such as MTA in New York City, reach out to both domestic and international peer agencies (R. Masciana, MTA Police, personal communication, Dec. 30, 2007).

Transit employees and customers are important sources of intelligence, typically in the form of threat information, but the information can be variable in terms of timeliness and accuracy. As noted in *TCRP Report 86, Volume 1*, pre-incident indicators such as propaganda, vandalism, direct threats, thefts, and surveillance attempts should be identified, closely monitored, and shared with other agencies on a frequent basis (TRB 2002).

Regional coordination and cooperative relationships are important among transit agencies and first responders in information and resource sharing; developing drills and exercises; effective emergency response; establishing communications interoperability; and avoiding duplication of work. Additional information about how transit agencies can address cooperative relationships within their region, including their participation in regional emergency response plans and conducting regional drills and exercises, and information about intelligence-gathering, including threat and vulnerability information collection and analysis and information-sharing techniques, are found in the *Transit Agency Security and Emergency Management Protective Measures* report (Batelle, TotalSecurity US, and Transportation Research Associates 2006). Another way in which agencies address cooperative relationships is through Connecting Communities Emergency Response and Preparedness Forums, a successful FTA/TSA partnership project. These two-day workshops enhance security and safety by sharing transit policies, procedures, resources, and best practices with local first responders to transit emergencies. The program uses realistic scenarios, including terrorism, to focus discussion on emergency preparedness, management, and response. A key objective is expanded understanding and effective integration of the roles of federal, state, and local emergency management offices and response entities to facilitate efficient planning, preparedness, and response coordination. In 2007, eight Connecting Communities Forums were held across the country.

TSA, FTA, and FEMA cosponsor the biannual Security and Safety Roundtable. These roundtables bring together security coordinators and safety directors from the nation's 50 largest mass transit and passenger rail agencies with federal security partners to discuss security challenges and develop effective risk-mitigation and security-enhancement initiatives. The roundtables also provide a forum for agency safety and security officials to share effective practices and develop relationships to improve coordination and collaboration.

Intelligence-sharing between the agencies and their federal, state, and local partners is further facilitated through TSA's Mass Transit Security Information Network's inter-agency communication and information-sharing protocols. The Homeland Security Information Network Public Transit (HSIN-PT) Portal has been integrated into this network to

provide one-stop security information sources and outlets for security advisories, alerts, and notices. Additionally, TSA is actively involved in regional security forums and supports these collaborative efforts by sharing intelligence products and related security information. Another key initiative is the joint classified threat and analysis briefings provided by intelligence professionals in DHS, TSA, and the FBI to mass transit and passenger rail security officials and their federal partners. These briefings occur on a quarterly basis, with additional sessions as threat developments may warrant. They engage regional mass transit and passenger rail security professionals and their TSA and FBI colleagues in metropolitan areas simultaneously through the FBI's secure video teleconference system maintained in the JTTF network.

CUSTOMER OUTREACH, EDUCATION, TRAINING, AND AWARENESS

Customer outreach, education, training, and awareness programs inform transit customers on what to do in emergencies and how to identify suspicious activity, persons, or items. Examples of security awareness literature are presented in Figure 8 and Appendix A. Many transit agencies have instituted Transit Watch, and some agencies provide evacuation instructions to their rail and subway passengers. WMATA conducts training for selected commuters within its subway tunnels to help themselves and other riders navigate them in case of an emergency (Layton 2004). NYCT provides its customers with a web-based video on how to safely evacuate trains in case of an emergency.



FIGURE 8 Example of a Security Awareness Poster (Courtesy: BART).

Some agencies such as WMATA and TriMet collaborate with Community Emergency Response Teams (CERTs) to enlist the assistance of neighborhood CERT members to be

their eyes and ears. The CERT program educates the public within a specific community about disaster preparedness and trains them in disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. During an emergency, CERT members can assist others if professional responders are not immediately available. Some agencies provide toll-free numbers or hotlines for their passengers to report suspicious activity, and some have implemented a crime-prevention program. Some agencies encourage the general public as well as their customers to be alert and report any suspicious activity. For example, a catchy television, radio, and in-vehicle transit campaign stating that in 2006 1,944 New Yorkers “saw something and said something” reminded the public to be aware and alert.

Additional information about Transit Watch and how transit agencies can create, update, and execute public and employee information communications plans are found in the FTA’s *Transit Agency Security and Emergency Management Protective Measures* report, on TSA’s website (<http://www.tsa.gov>), and on FTA’s safety and security website (<http://transit-safety.volpe.dot.gov>).

TSA issues brochures such as the *Highway Passenger Security for Motorcoach*, which includes a visual guide of the areas on a bus in which devices and objects may be placed by a terrorist, and the *Security Awareness Tips for Passengers*, a guide on commuter and intercity rail systems. National Transit Institute (NTI), in conjunction with the FTA, also issues awareness and other relevant brochures. Individual agencies distribute these brochures and issue agency-specific publications and informational materials to their customers and employees. Samples of these brochures are shown in Appendix A.

Public education and outreach efforts are being further enhanced by programs such as the Play Your Part initiative. The initiative is a key component of public awareness campaigns. Under this program, TSA, in joint efforts with mass transit and passenger rail agencies, advances security awareness among the traveling public and public and private partners. TSA Transportation Security Inspectors—Surface, supported by the Mass Transit Division, form partnerships with the agencies in high-visibility public awareness campaigns, altering the normal activities at terminals or stations and enhancing passenger awareness of and vigilance for suspicious activities and items, which are possible indicators of terrorist preparations for or execution of an attack. TSA and the agency’s employees and surge personnel display posters and distribute security awareness literature and promotional items to passengers at random dates, times, and locations throughout the system. Local police and emergency response personnel are informed of the event and invited to join.

The agencies do not incur additional expense to participate in the program. TSA funds the cost of the public awareness materials distributed during the joint campaigns. These materials include a bookmark-size flyer, with a photograph from the transit system; the participating agency’s logo and emergency contact number(s); security awareness and vigilance tips for passengers; and a plastic key-ring light promotional item. The light is imprinted with the words “Transportation Security Administration” and “Play Your Part,” linking the promotional item to the public awareness campaign.

Transit customer education is important in crime prevention, because many transit crimes are crimes of opportunity. Many agencies distribute educational literature on crime prevention and advise passengers on steps that can be taken to deprive criminals of the opportunity to commit crimes (e.g., not displaying jewelry). This information is more valuable for infrequent transit patrons who may forget to take these precautions. Passengers should be educated about security features of transit vehicles in all modes, and the transit system should clearly identify those features for the riding public. *TCRP Synthesis 68 on Methods of Rider Communication* (Schweiger 2006) describes the state of the practice in effective transit agency communication methods. “Effectiveness” is defined as providing accurate, clear, accessible, understandable, and timely information. Regarding security communications, the Synthesis study reported that nearly all survey respondents provided some type of security-related information to their customers, with reminders about suspicious activities and packages being the most common (Schweiger 2006).

EMPLOYEE SECURITY AND POLICING TRAINING

Transit agencies strongly emphasize security training of their transit officers, security personnel, and frontline transit personnel and supervision.

To assist these agencies further in improving training, TSA, in consultation with the FTA and other public and private security partners, developed and published the Mass Transit Security Training Program. This program provides detailed guidelines for mass transit and passenger rail agencies to facilitate development and implementation of security training programs, specifying the subject areas in which particular categories of employees should receive training. The guidelines are implemented under the Transit Security Grant Program. Course options include programs funded by FTA/TSA (transit-specific terrorism prevention and response) and FEMA (general terrorism prevention and response).

The FTA, through the NTI, issues publications that are available to all domestic transit agencies for use in employee

training. These publications include the following brochures, which are distributed by transit agencies to their new hires and current employees.

- *Employee Guide to System Security.* This guide describes how to identify system vulnerabilities, how to identify and respond to suspicious people, activity, and objects, and how to report suspicious people, activity, and objects.
- *Terrorist Activity Recognition and Reaction.* This guide for employees provides information on how to recognize suspicious activities, including surveillance activity, testing security, infiltrating secure areas, deploying assets, and individual behaviors. It describes how to recognize and respond to dangerous activity and how to report suspicious or dangerous activity.
- *Emergency Preparedness Guide for Transit Employees.* This guide explains what to do before and during emergency situations and includes specific tips on how to handle a variety of emergencies, including natural disasters. The guide contains general system security awareness information. It is unique in that it has two sections—one pertaining to emergencies on the job and the other to emergencies at home.
- *Employee Guide to Workplace Violence.* This guide includes basic strategies on how to deal with difficult or dangerous individuals are described. Although this publication focuses on worker-on-worker violence, these strategies are applicable to public-on-worker violence as well.

According to survey results, transit agencies have provided or are planning to provide, at a minimum, security awareness training to their frontline employees, supervisory personnel, and security personnel. Security training is typically conducted either in house or through NTI or the Transportation Safety Institute. Other sources are available including APTA, FEMA, and universities such as Johns Hopkins University (JHU). Most training has been delivered by classroom training or workshop, and the rest has been a combination of video/digital video disc, interactive compact disc, or online training without an instructor. The length of most training is between one and four hours. It is interesting to note that few courses are directed toward transit managers. One such course is the FTA-sponsored Strategic Counterterrorism for Transit Managers provided by JHU.

The MBTA Transit Police Department is one of a few transit agencies with its own police training academy that trains both MBTA officers and local responders (MBTA 2000) (see Figure 9).

Capital Metro provides training to its local responder community using a valuable tactical operations guide. Additional information about the guide is included in the Capital

Metro case study (see chapter six). WMATA has a unique and realistic training facility and vehicles for its transit police officers and personnel. The training facility, ideal for interagency drills, may be used by other transit agencies.

Following are some of the security-related classes or courses provided by transit agencies:



FIGURE 9 MBTA Police Officers (Courtesy: MBTA).

- Transit Watch
- System Security Awareness for Transit Employees
- System Security of Operators
- Security Awareness Train-the-Trainer
- Recognizing Terrorist Activity
- Terrorist Recognition and Response
- Strategic Counterterrorism for Transit Managers
- The Mark (video/DVD)
- Other NTI Transit Security DVDs
- Behavior Recognition Train-the-Trainer
- Incident Response to Terrorists
- Terrorism Awareness
- Transit Terrorist Tools and Tactics
- Transit System Security and Design Review
- National Incident Management System (NIMS) ICS 100, 200, 300, 400, 700, and 800
- Homicide/Suicide Bomber Training
- Domestic Preparedness
- Emergency Management
- Transit Emphasis Inc. Management Service
- Transit Vehicle Emergencies
- Crime Prevention
- CPTED
- Firearms, arrest control technique, taser, baton, and pepper spray training
- Peace Officers Standards and Training (POST)
- First Aid/CPR (cardiopulmonary resuscitation)
- Customer Service and Customer Relations.

FEMA's Center for Domestic Preparedness in Anniston, Alabama, is the DHS's only federally chartered WMD training center. The Center provides hands-on training to emer-

gency responders using actual chemicals and other threat materials. DHS covers the cost of travel and other expenses for qualified participants (Center for Domestic Preparedness 2008).

Eleven of the responding agencies reported having updated their performance appraisal system since 9/11 to include security matters. Covert evaluations of transit workers in implementation of security training content, security awareness, and other related matters usually are not completed. Although drills are performed on a regular basis, large drills are costly, and agencies typically cannot accommodate all transit police and security personnel and frontline employees. Simulation is an alternative training and evaluation tool that provides a realistic but safe three-dimensional setting in which employees may be trained and assessed. Simulation is being used in military settings to train military personnel and has been considered for use by a few transit agencies as a training tool.

YOUTH OUTREACH STRATEGIES

Transit systems with high juvenile ridership often experience problems with disorderly behavior. Juveniles can be a major source of disorder and provoke fear in transit customers, including in other youths and transit employees (Nelson 1997). In some cases, bus drivers have refused to drive into certain neighborhoods or during certain times of the day because of the fear of violence.

According to the MBTA Youth Study results, 75% of weekday afternoon riders were intimidated by the crowds of juveniles on the system (MBTA 2000). Their behavior, which included loud and vulgar language, blocking subway doors, and other unruly acts, caused these riders to avoid using the system during the afternoon hours. Furthermore, juveniles have accounted for a disproportionate number of arrests, especially for assaults and battery.

The MBTA Transit Police Department addressed the problem by taking several actions: police presence was increased; kiosks were installed in several stations to provide easier access to the police; gang issues were addressed in partnership with the Boston Police Departments' Youth Violence Strike Force; MBTA Transit Police Department collaborated with the YMCA to provide youths loitering in the transit system with free YMCA passes so that they would be able to participate in athletic and other activities; and the MBTA Transit Police Department worked with a high school to reduce youth violence. In addition, Field Interviews and Observations were conducted to address truancy, and MBTA transit officers stopped possible truants and obtained information about them. This effort indirectly reduced loitering, minor violations, and gang activity.

The CDTA in Albany, New York, has engaged in a collaborative effort with one of the major school districts and police agencies in its service area to prevent juvenile crime and disorder. The CDTA worked with the schools to establish the idea that CDTA buses are extension of the classroom; and, thus, students who violate either CDTA's code of conduct or the school's code of conduct are subject to suspension from school and CDTA bus service and its facilities for a period of time. Additional details about this effort can be found in the CDTA case study (see chapter six).

EVALUATION PROCEDURES, DRILLS, AND COVERT TESTING

According to survey respondents, evaluations of policing strategies and measures are often performed by measuring the impact of the strategy or measure on the specific problem being addressed. Additionally, specific testing and evaluations of new equipment are performed.

Some agencies conduct or participate in simulations or tabletop exercises or workshops. Many transit agencies regularly conduct at least one to two inter- and intra- agency drills a year, according to the Synthesis findings. After-action reports are useful for agencies in assessing their preparedness, and identifying and addressing system-related vulnerabilities and individual weaknesses. WMATA's Metro subway system conducted Operation Trouble Waters, a Multi-Agency Emergency Preparedness Safety Exercise on the Yellow Line bridge over the Potomac River in October 2007. The drill took place on location using WMATA's training vehicle, which simulated a smoke-and-fire event with several injured passengers onboard a stranded four-car train. The multiagency event required the response, coordination, and communication of several agencies, including Metro Transit Police, Rail, Safety, FBI, Operations Control Center (OCC), DHS, and the Maryland, District of Columbia, and Virginia fire departments. The training facility, ideal for interagency drills, may be used by other transit agencies as well (WMATA 2007). Additional information for planning drills and exercises is available in *TCRP Report 86, Volume 9: Guidelines for Transportation Emergency Training Exercises* (TRB 2006a).

Transit agencies tend not to engage in covert testing of their security personnel or their frontline workers, but a few agencies reported that they do conduct covert observations of operators with respect to safety and security, including pretrip inspections along with passenger relations, Americans with Disability Act (ADA) compliance, and on-time performance. One agency reported that they conduct hostage drills on buses once a year; another reported that nighttime entry into transit facilities is tested; and another reported that access to transit vehicle panels and compartment doors is checked randomly to verify adherence to standard operating procedure.

FERRY SECURITY

Ferries outside of the United States have been targets of attacks, and U.S. ferry systems have been cased by suspected terrorists. Ferries are vulnerable to IEDs, acts of force, and chemical, biological, and radiological agents. Delivery methods can be by person, by vehicle, by vessel, by air, underwater, or as artillery. Ferries that carry cars as well as passengers are believed to be more vulnerable than passenger-only ferries because of the large amount of fuel being carried (TRB 2006c).

Vehicle screening for explosives is performed by ferry systems that carry vehicles as well as passengers to comply with regulations of the Maritime Transportation Security Act of 2002, which became effective on July 1, 2004. The screening can be made visually, by canine, or with a car-screening van. The car-screening van contains explosives-detection equipment and is used by slowly driving past a vehicle to scan it for explosives. Passenger screening is done by ferry operators. In addition to screening requirements, other security measures include new regulations for training and drills, approved security plans, onsite assessments by the U.S. Coast Guard, designated company and vessel security officers, Declarations of Security between termi-

nals and vessels, and automatic identification systems. The nature and extent of the measures that are required by federal regulations are directly linked to the Maritime Security threat level (I, II, or III).

Security officers for one of the larger ferry systems use explosive-detection canine teams to screen vehicles stopped in the vehicle holding lane. If explosives are detected by the canine unit, a secondary physical inspection of the vehicle is performed. Random visual inspections of vehicles are performed, and drivers are asked to open trunks and other compartments for visual checks. The Coast Guard Marine Safety and Security Team escorts ferries at random and increases the escorts during special events. Ferry vessel security was increased by securing the ferry captain's compartment. The following are primary security measures for ferry systems (TRB 2006c):

- Fencing/Barriers
- Access Control
- Intruder Sensors
- Monitoring
- Procedural/Low-Cost Waterside Security
- Screening
- Human Observation.

CHAPTER FIVE

CONFLICT MITIGATION STRATEGIES

Based on panel member interest in this topic, this chapter describes conflict mitigation strategies, including verbal judo, assertive limit-setting, listening tactics, and problem-solving skills. Transit employees are in constant contact with the public, and the transit environment creates stressful situations for both passengers and employees (e.g., a commuter who is already late to work may be further delayed by a late bus or train.) Potential conflict situations occur within transit systems on a daily basis and can escalate and erupt into physical confrontations or assaults. Assaults on front-line workers create a great deal of anxiety and stress for all workers and contribute to a reluctance to work in high-crime areas. Therefore, training employees in conflict mitigation techniques is important. Conflict mitigation techniques go hand in hand with customer relations training, which should be provided to all transit employees who have contact with the public. Effective customer relations management can enhance customer satisfaction and stave off conflict situations. Although outside the scope of this study, transit employee versus employee conflict situations have been increasing in frequency as well.

Transit agencies practice one or more conflict or assault mitigation techniques. The two primary methods, as reported by the 22 survey respondents, include passenger codes of conduct and presence of security or transit personnel; these measures also address other anticrime and counterterrorism objectives. About half of the respondents indicated that their personnel use verbal techniques such as verbal judo, and less than half of the responding agencies indicated that they implement community policing practices and roving security patrols. A few respondents indicated that they use nonverbal techniques and restraining techniques to resolve and mitigate conflicts. Some agencies reported they provide specific training in conflict resolution techniques, participate in school outreach efforts to discourage juvenile offenders, and install cameras to act as a deterrent to criminal behavior and conflict escalation.

Conflict management training for all transit workers is important to address both customer and workplace violence, especially for frontline workers who interact with the public on a daily basis. Increased fear and stress from potential confrontations and violence can cause increased absences, increased disability and workers compensation claims, decreased productivity, and poor employee retention; and,

ultimately, such fear and stress may damage the reputation of the transit agency. Recognizing the warning signs of a volatile or emotionally disturbed individual, understanding what to do to defuse potentially violent situations, and knowing how to respond if violence does occur will make transit employees feel safer both physically and emotionally. Typically, physical aggression does not occur out of the blue but develops along a continuum such as the one shown in Figure 10.



FIGURE 10 Physical Aggression Continuum (Source: Crisis Prevention Institute's 2007 Webinar on Workplace Violence Prevention).

An appropriate training mechanism is role-playing, in which transit workers would be taught ways in which they can respond to attackers and potentially threatening behaviors by actually playing out different confrontational interactions. As noted earlier, customer relations training is just as vital for transit employees because good customer relations can obviate the need for conflict mitigation. In addition, transit management should have a written policy on violence that includes what employees are expected to do in specific situations and how those incidents should be reported, and it should communicate this policy to all of its workers.

Transit patrons are naturally going to experience anger and frustration, especially if they experience a delay or other issue with transit service. However, they should not be abusive or manipulative toward transit personnel or other customers. If the aggressor achieves his or her objective in controlling the situation, the interaction will likely continue. As shown in the Escalation/Crisis Cycle Flowchart (see Figure 11), if the transit worker participates in

and responds to the conflict, the interaction may escalate into a physical confrontation. For example, a customer may complain about the bus being late and blame the bus operator, stating, “If you knew how to drive the bus, this wouldn’t happen. What the hell is wrong with you!” To defuse the situation before it escalates, the transit personnel initially should acknowledge the customer’s feelings, empathizing with the customer, and communicating with them as a real person with a name and feelings. Next, the transit personnel should try to control the interaction by beginning to defuse the situation early in the interaction and by being assertive and never losing control. If the transit worker loses control and becomes angry at the attacker, the possibility of escalation and violence greatly increases (Bacal 1998).

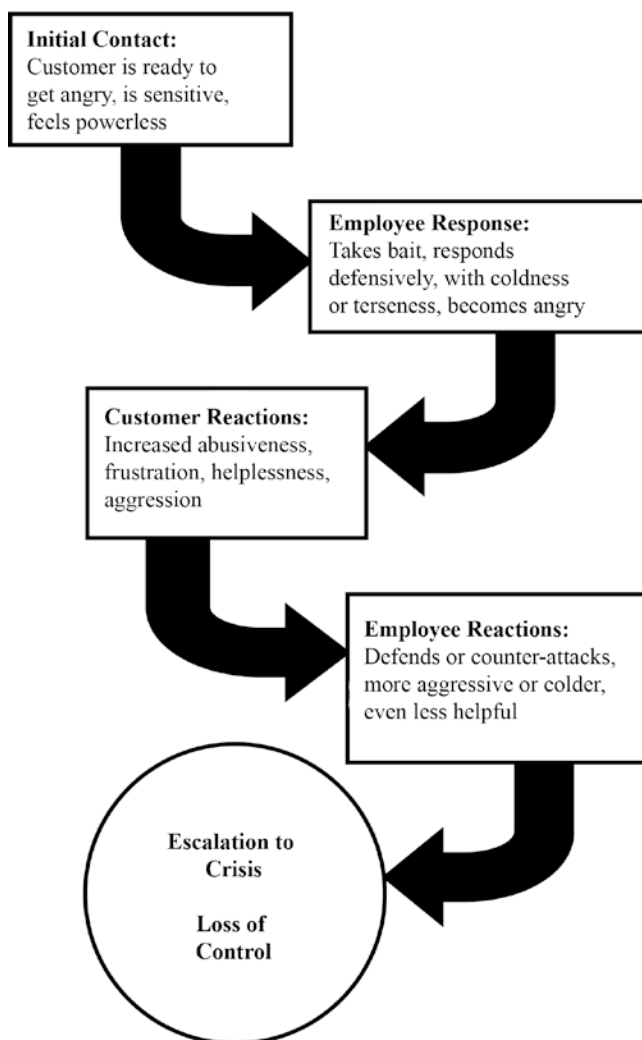


FIGURE 11 Escalation/Crisis Cycle Flowchart (Source: Defusing Hostile Customers Workbook).

Aside from contact with the public, transit workers may be affected by other risk factors such as the following (NIOSH 2006):

- Exchange of money
- Delivery of passengers, goods, or services
- Working alone or in isolated locations
- Working late at night or during early morning hours
- Working in high-crime areas
- Responsible for property of interest to terrorists or criminals.

TECHNIQUES

Conflict mitigation techniques can be broken down into the following categories.

Initiating contact: When initiating contact with a hostile customer, verbal tone and nonverbal cues are both important. It is best if the transit worker is the first one to speak and ask a question to gain control of the situation.

Use of cooperative language: The use of nonconfrontational language is important—this type of language is milder, does not challenge the customer, and does not place blame. Also, hot phrases that suggest disinterest such as “whatever” or “I don’t care” and references to ethnic background or unequal treatment should not be used. Words with threatening or challenging undertones and absolute words (such as “never”) should not be used.

Verbal judo and self-defense techniques: Verbal judo, a tactical communication technique originally developed for law enforcement, is based on some of the principles of judo (e.g., redirecting the attacker’s energy to control the situation). Surprising the attacker (e.g., saying something that is unexpected) is a good technique to confuse and stop the attacker from continuing their verbal abuse. This provides the transit worker with an opportunity to gain control of the interaction.

Acknowledgment or listening tactics: Empathy statements such as “I understand that you are upset about the delay” acknowledge the customer’s feelings. These types of listening responses rephrase what the customer has said and demonstrate to the customer that the transit worker is listening to them.

Problem solving: Trying to resolve the customer’s problem and giving them useful information shows goodwill to the customer and may reduce hostility toward the transit worker. Also, explaining why the problem occurred may be helpful.

Assertive limit-setting: Assertive limit setting is used to end a conversation that the transit worker has not been able to control by employing other tactics to change the attacker’s behavior. The following concepts are imparted to the attacker in assertive limit-setting:

- A description of unacceptable behaviors,
- A request to change that behavior,
- An explanation of the consequences that will occur if the behavior does not change, and
- A question that gives the customer a choice.

Countering nonverbal intimidation: A transit worker can change his or her physical position relative to the attacker by standing at an angle or side-by-side to counter physical intimidation and diminish confrontation. At the same time, it is important not to move into their space. In addition, distracting the attacker by directing them to something else such as a clipboard or map may help.

Other techniques: Many other techniques may be used, including redirecting the customer's anger or giving the customer an address to send a complaint letter. Removing the audience (other customers, the public) by interacting with the customer in a more private area may be helpful. Creating agreement about anything with the customer and giving away something (e.g., transit map) may lessen the intensity of their hostility. Certain behaviors such as a sudden change in expression, voice tone, or an intimidating body posture might identify customers who may need to be treated with caution (Bacal 1998, p. 22).

INFORMATION SOURCES

The following sources of information and references on workplace violence may be useful in providing guidance to transit management:

- Bureau of Labor Statistics, Survey of Workplace Violence Prevention, 2005.
- International Labour Organization. Code of Practice on Workplace Violence in Services Sectors and Measures to Combat this Phenomenon, 2003.
- National Institute for Occupational Safety and Health, Violence in the Workplace: Risk Factors and Prevention Strategies, 1996.
- National Institute for Occupational Safety and Health, Violence on the Job, 2004.
- Occupational Safety and Health Administration. Voluntary Guidelines for the Prevention of Workplace Violence.

There are also many training manuals developed by non-profit and for-profit organizations such as the Crisis Prevention Institute's *Prepare Training Program Manual* (2005).

PREVENTION STRATEGIES

Strategies to counter the risk factors include the implementation of smart cards and the elimination or reduction of cash-based transactions. Many agencies have implemented automated fare collection systems that do not accept any form of cash. When taking tokens or cash out of fare boxes, extra security should be present. Physical separation of workers from the general public using bullet-resistant barriers or enclosures may be helpful. To address a rise in assaults on its Metrobus bus operators, WMATA, in February 2008, started testing a clear plastic shield separating the bus operator from fare boxes used by passengers (NIOSH 2006). LACMTA and CTA are also testing the separation device on their bus systems.

Strong legislation can act as a deterrent to assaults on transit workers. The D.C. City Council is considering legislation to increase the penalties and fines for those who assault bus operators on the job. Similar legislation has been proposed in Maryland. In New York City, assaulting a transit worker is equivalent in severity to assaulting a police officer, which is considered a felony. This penalty has been advertised within the transit system and acts as a deterrent to assaults on its workers.

Incidents should be documented to determine the extent and types of conflicts occurring between transit employees and the customers, and the outcomes of the incidents to determine optimal conflict management techniques. Threats should be documented and evaluated by interdepartmental teams composed of representatives from security, human resources, unions, management, employee assistance, and other relevant units to determine how specific a threat is and whether the person making the threat has the means to carry it out. Law enforcement and transit security personnel should be contacted immediately for imminent threats, and employees should be aware of what to do in case a confrontation does become physical. A plan should describe the composition of the response team, who should be responsible for the victim's immediate care, and should explain how to debrief the victim(s), their coworkers, and families. Guidelines on reestablishing transit service should be developed.

CHAPTER SIX

CASE STUDIES

The objectives of the case studies were to obtain an in-depth coverage of both crime and terrorism-related security challenges faced by the selected transit agencies, examine their security practices and measures, and learn how they are holistically integrated and utilized by the agencies to address the challenges. The case study question categories included post-9/11 changes in security, policing, policy, and practices; security-related technologies and other implemented security measures; changes in crime, incident, and suspicious activity trends; training and personnel issues; security data collection and analysis practices and concerns; and other information relevant to the study.

Case studies of four transit agencies and a transit agency profile are provided in this chapter. The case study agencies are Massachusetts Bay Transportation Authority (MBTA), serving the greater Boston area; the Bay Area Rapid Transit (BART), serving San Francisco, California's Bay Area; the Capital District Transportation Authority (CDTA), serving the Albany, New York Capital District; and Capital Metro serving the two counties in the Austin, Texas, region. The transit agency profiled is the Washington Metropolitan Area Transit Authority (WMATA)—this agency's successes in interoperable communications are described.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY (BOSTON, MASSACHUSETTS)

The MBTA, established in 1964, serves greater Boston and eastern Massachusetts. With a daily ridership of 1.1 million passengers, MBTA operates the oldest subway system in the country (the original subway opened in 1894) and is now composed of five subway lines, the Silver Line bus rapid transit, 13 commuter rail lines, four passenger ferry routes, and 181 bus routes, along with paratransit (see Figures 12 and 13). Serving a community with a daytime population of more than 2.5 million people, the MBTA employs approximately 8,000 workers, covers nearly 3,244 square miles, and operates more than 2,200 vehicles on a daily basis.

MBTA Transit Police Department

The MBTA Transit Police Department was created in 1968 and has continuously evolved to meet MBTA's security and public safety needs. Currently, under the leadership of Act-

ing Chief Paul MacMillan, the MBTA Transit Police Department consists of 282 officers, 267 sworn and 15 nonsworn, who are specially trained to meet the unique challenges of securing the urban transit environment. In addition to 800 hours of training mandated by state law under the Municipal Police Training Committee, MBTA Transit police officers receive specialized training in counterterrorism, youth relations, juvenile law, cultural diversity, and ROW railroad safety training. The MBTA Transit Police Department is one of the few transit agencies with its own police training academy, which trains both MBTA officers and city and town officers and responders.



FIGURE 12 MBTA Subway Map, Partial View
(Courtesy: MBTA).

On March 19, 2005, the Commission on Accreditation for Law Enforcement Agencies unanimously granted full accreditation status to the MBTA Transit Police Department. This agency grants this status to law enforcement agencies that are in compliance with more than 400 standards that represent the highest level of law enforcement professionalism.

MBTA Transit police officers have jurisdiction and full police authority in all 175 cities and towns within its service area. Outside this area, the officers exercise street railway police powers on the vehicles, properties, and ROWs that make up the Commuter Rail System. The MBTA policing area is divided into four geographic districts, each of which is headed by a commander. The commanders and their

personnel interact with residents, passengers, and vendors within their district to build good relationships with the community.

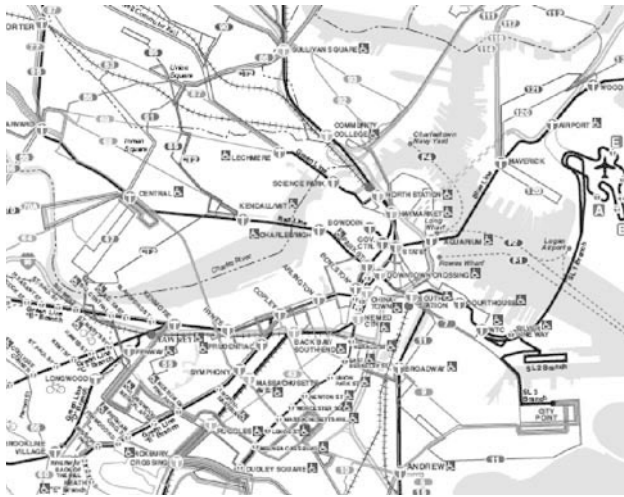


FIGURE 13 MBTA System Map, Partial View (Courtesy: MBTA).

MBTA Transit police officers are assigned to one of three divisions in the Department: Patrol Operations Division, Investigative Services Division, and Administrative Services Division. Transit police officers are responsible for the following:

- Protecting life and property;
- Upholding the constitutional rights of all people;
- Ensuring a safe environment within the transit system;
- Reducing fear;
- Preventing and detecting crime;
- Arresting, detaining, and prosecuting violators of the law;
- Recovering stolen property;
- Preserving public peace;
- Promoting *Transit Watch* and other transit security initiatives, including coordinating special national security events (e.g., the 2004 Democratic National Convention); and
- Promoting the confidence of the riding public through community policing.

Policing Management

One of the management strategies used by the MBTA Transit Police Department is CompStat (computer-driven crime statistics). Monthly CompStat meetings are held by the chief with the commanders to identify and address changing crime trends. Timely information sharing and awareness of problems within the MBTA system are the key benefits of CompStat for the MBTA Transit Police Department.

MBTA Interactive Crime Statistics Map

The MBTA Transit Police Department issues crime data in a timely and innovative manner. Annual statistics are provided for each station on MBTA's heavy rail and light rail systems as well as its Silver Line. A similar interactive crime statistics map is provided for MBTA's commuter rail system (see Figure 14). The public benefits from these maps include assessing the frequencies of specific crimes and altering trip-making decisions accordingly, which promotes a greater sense of security and control over their trip.



FIGURE 14 MBTA Transit Police Department's interactive crime statistics map (Courtesy: MBTA).

Counterterrorism Efforts

Twenty-five officers are formally dedicated to antiterrorism efforts. All officers have been trained to address both ordinary crime and antiterrorism matters and to take appropriate action when the situation warrants. Professionals in the field agree that antiterrorism efforts can have an impact on day-to-day crime. Therefore, focusing officer attention on homeland security issues will affect minor offenses such as disorderly conduct and vandalism. This is an important issue for police management because serious offenses may often follow such minor offenses.

Post-9/11 Security Measures

The results of risk assessments have indicated that IEDs pose the highest threats to MBTA's system for all of its transportation modes. Underwater tunnels, because of the potential result following an explosion, are the most significant threat locations.

Shortly after the 9/11 attacks, the MBTA Transit Police Department focused on increasing its counterterrorism security measures—and either implemented new programs or measures or expanded existing ones. Passenger reaction to

these measures generally has been positive, with many passengers expressing a desire to see even more security within their transit system. Many of these measures such as High Visibility Patrols and Train Order Maintenance Sweeps not only deter terrorism but also prevent and detect ordinary crime, as well as increase customer perceptions of security, and therefore are viewed as highly efficient as well as effective.

High-Visibility Patrols

High-visibility patrols are patrols that are made highly visible through the saturation of specific locations with multiple specially uniformed officers (battle dress uniformed and IMPACT teams) and the use of visible tactical vests (ATLAS teams). These patrols are viewed as one of the most effective security measures instituted by the MBTA Transit Police Department. These patrols monitor all MBTA modes and all areas of the MBTA system, and act as a strong deterrent against both terrorism and ordinary crime.

Train Sweeps

Train sweeps involve officers who appear unannounced at a station and spread out along the platform. They step onto every car of the train while the train is stopped to observe passengers and identify suspicious activity or objects; they then step off the train. Because the procedure takes only several seconds, there is little disruption to train service. Similar to high-visibility patrols, the visible presence of officers on station platforms monitoring the interior of each train car acts as a strong deterrent against both terrorists and criminals.

Explosives Detection Unit

The MBTA Transit Police Department significantly expanded its explosives-detection unit by acquiring additional canine units and participating in the TSA canine program. Currently, the MBTA Transit Police Department has 10 explosives-detection canine and 10 officers assigned to this unit. The canine teams patrol all MBTA modes aside from paratransit. Currently, 10 patrol dogs are part of the normal patrol unit within the MBTA system and provide security for the agency's facilities, including bus depots and train yards.

Passenger Security Inspections

MBTA was the first transit agency in the United States to implement PSIs. In 2004, when Boston hosted the Democratic National Convention, the MBTA transit police initiated random passenger bag and luggage inspections. This is now implemented on a systemwide basis for *all* MBTA modes except paratransit to deter acts of terrorism and enhance passenger perception of security. Explosives trace detection (ETD) equipment is typically used during the inspections. The ETD analyzes a swab taken by an officer from the zipper, seams, or handle of a bag; alarms sound if it detects any

traces of explosives material; and does not require that bags be opened, which protects the privacy of passengers. The inspections are random and can occur at any time, on any day, and at any location within the MBTA system, enhancing the deterrence effect of this security measure.

Behavioral Assessment

Behavioral assessment is the observation of passenger behavior and the identification of suspicious behavior. Officers question passengers deemed to be acting suspicious and take further action if warranted based on the observed behavior during the interaction. This procedure is not based on the physical appearance of the individual, and ethnicity is never taken into account. Behavioral assessment has been used successfully by Israeli airport security to identify terrorists and would-be suicide bombers.

Cameras

Every subway station has been outfitted with security cameras that were installed in conjunction with the installation of automatic fare collection equipment. More than 500 cameras have already been installed in MBTA stations and trains. All cameras are now digital, allowing the storage of images for up to 30 days. Real-time images are sent to one of several command centers where personnel monitor them. Cameras are or will be installed on 300 buses and on ferries. A motion detection system that alarms when it detects unauthorized individuals and triggers a camera is being installed in the underwater tunnels, which are deemed to be high-risk locations. Intelligent video software capable of identifying suspicious behavior and objects will be implemented in conjunction with this camera system and other cameras throughout the system.

Intelligence Unit

The MBTA Transit Police Department's Intelligence Unit engages in information sharing with local law enforcement and federal agencies as well as other domestic and international transit agencies. The unit established the Counterterrorism Hotline (1-866-PREVENT or 617-222-TIPS), which has been disseminated to the public. All reports are investigated by the Intelligence Unit and are forwarded to the FBI's Joint Terrorism Task Force, when warranted. The Intelligence Unit issues a weekly bulletin that summarizes all transit-related incidents throughout the world.

Special Operations Team

The MBTA Transit Police Department deploys its Special Operations Team (SOT) to assist in critical incidents or situations. The SOT is trained in hostage and barricade situations, as well as high-risk entry situations. SOT members participate on the high-visibility ATLAS teams.

HazMat Officer

The MBTA Transit police department has an officer specially trained to handle hazardous materials (HazMat) and who will respond to HazMat emergencies.

Chemical Detection

A chemical detection unit was tested as part of the Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) and is being used in one of MBTA's multimodal stations. If the unit detects a chemical threat, it will alarm and then trigger a camera within the station to transmit images to the MBTA's Operations Control Center (OCC).

Public Awareness Campaign

The "See Something, Say Something" Transit Watch program implemented by the MBTA Transit Police Department encouraged the MBTA employees and passengers to report suspicious activities and objects. Public address announcements remind passengers to report suspicious behavior, and the frequency with which the announcements are made is correlated to the threat level. The perceptions of threat have decreased compared with the period immediately after 9/11 and the London and Madrid bombings. Public awareness campaigns keep the public, passengers, agency employees, and officers motivated and alert. The number of reports of suspicious activity and objects, which peaked immediately after 9/11 and then again after the London and Madrid bombings, has now stabilized.

Blast Mitigating Trash Receptacles

After 9/11, blast-mitigating trash receptacles replaced regular trash receptacles in the core subway system to prevent serious consequences from the detonation of an IED placed inside a regular transit receptacle.

Training

In addition to normal police training that all officers undergo in MBTA's police academy, the following training is provided either to all officers or to a select group of officers:

- Behavioral Assessment Training
- Counterterrorism Training
- General Electric Itemizer Training (the Itemizer is a portable trace explosives detector used by MBTA Transit Police Department officers to conduct PSIs)
- HazMat Technician Training

- NIMS ICS 100, 200, 300, 400, 700, and 800
- Strategic Counterterrorism for Transit Managers (provided by JHU).

All MBTA employees receive NTI security awareness training.

Exercises and Drills

The MBTA Transit Police Department initiated counterterrorism training after 9/11, as well as more basic security awareness training for its officers and MBTA employees. The MBTA Transit police participate in three to four inter-agency exercises and drills per year.

Stop Watch Program

This program was initiated in September of 2003 as a result of increased complaints from students and other passengers that large groups of youths were congregating in stations or riding trains in a disorderly manner that created the perception of fear. Stations at which large groups of juveniles tend to gather are identified and are the focus of the program. The program is a collaboration among many public service and law enforcement agencies to address this issue. Program participants include the Boston Police, the Boston School Police, juvenile probation officers, faith-based organizations, and city of Boston street workers. Participants do not necessarily make arrests but attempt to interact with the juveniles and disperse the groups that tend to engage in disorderly conduct or disturb passengers just by their presence.

Challenges and Issues

Unions representing MBTA workers are influential and often fight for compensation for any extra security-related tasks requested of MBTA workers. These labor relations items can impede the efforts of the MBTA Transit Police Department to implement desired security measures. At the same time, many MBTA workers are aware of security issues and some have called in with useful information about suspicious activity and items.

MBTA has experienced issues with the manner in which the TSA has implemented VIPR programs. The MBTA Transit Police Department is working with the TSA to ensure that TSA personnel on VIPR teams deployed to the MBTA system are properly trained and that VIPR missions support ongoing MBTA Transit Police Department operations. To allay these concerns and potential liability issues, a Memorandum of Understanding between the MBTA and the TSA on the use of the VIPR team is currently under consideration.

Crime Trends

Little has changed in terms of crime categories over the past several years; the most problematic crime throughout the MBTA system is larceny. In general, there has been a downward trend in crime compared with the mid-1990s during the height of the crack cocaine trade. Some of this decline may be the result of the increased presence and visibility of police officers because of the post-9/11 security enhancement at MBTA, along with a decline in the use and distri-

bution of cocaine. MBTA's 2007 Crime Statistics indicate that Part I offenses have decreased by 10%, whereas Part II offenses have increased by 12%. Part I offenses are composed primarily of larceny and robbery, with aggravated assaults a distant third. Part II offenses are distributed more evenly among the categories. Crime statistics are reported based on the rate per 100,000 passengers and on average weekday occurrence. Examples of the statistics produced by the MBTA Transit Police Department are presented in Figures 15–20.

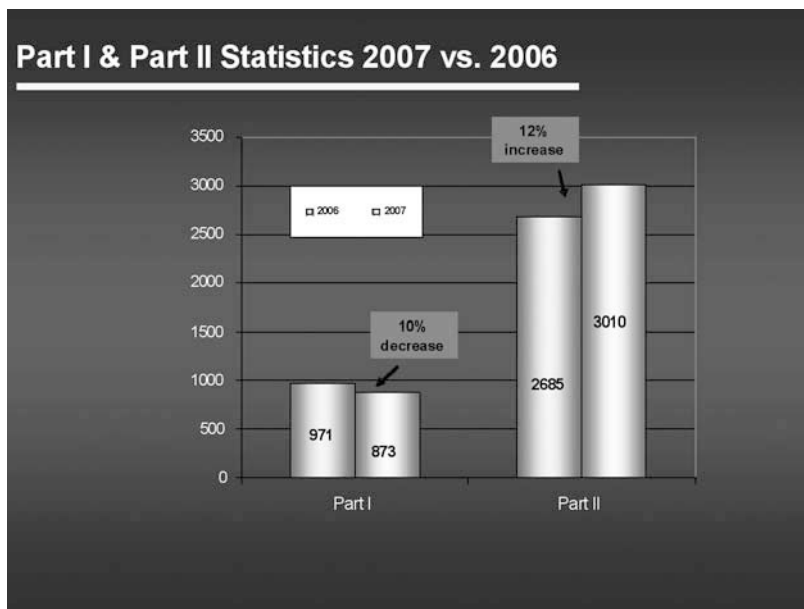


FIGURE 15 MBTA Transit Police Department's Part I and Part II crime statistics (Courtesy: MBTA).

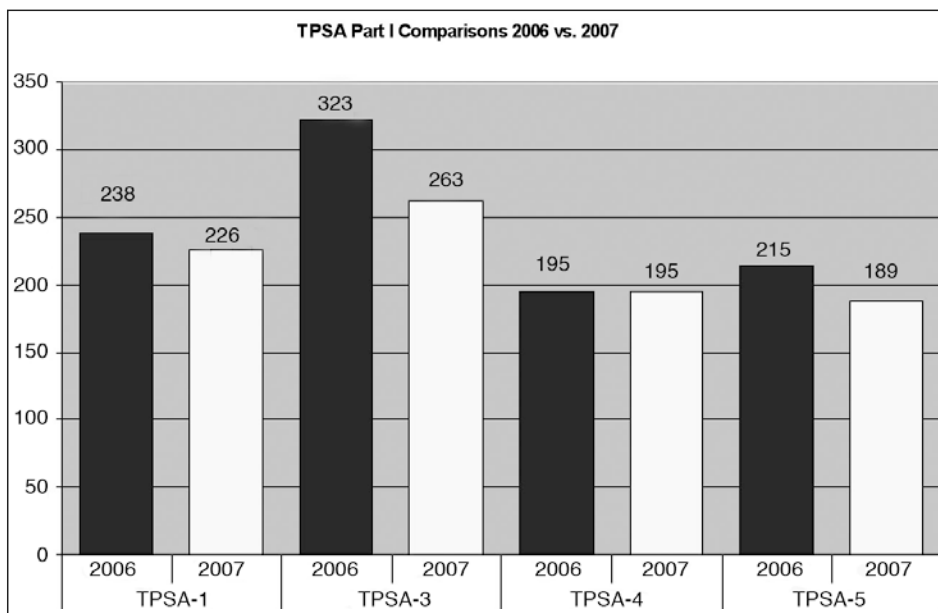


FIGURE 16 MBTA Transit Police Departments comparisons 2006 vs. 2007.

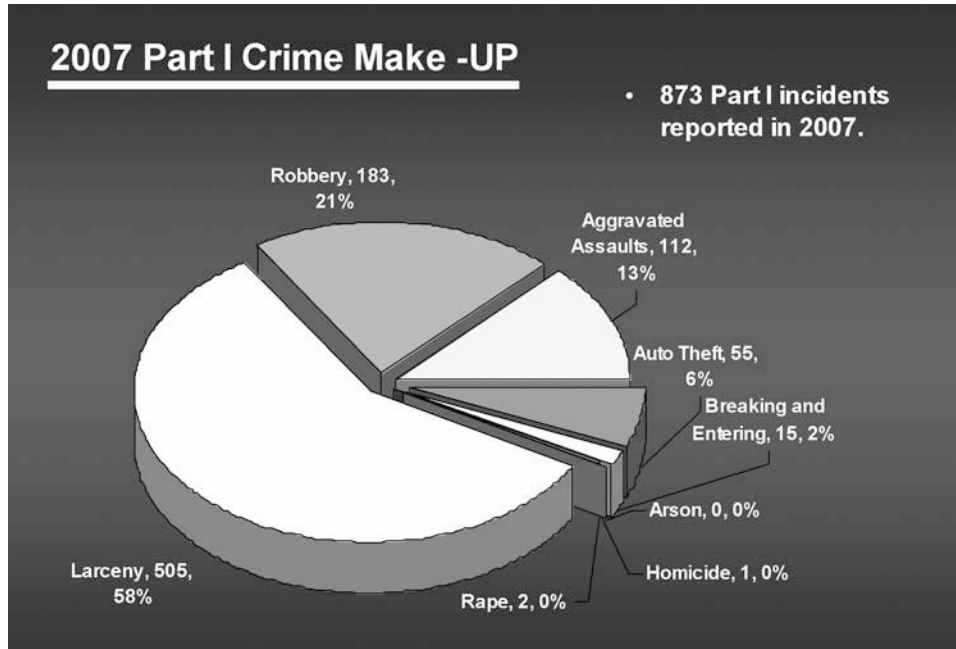


FIGURE 17 MBTA Transit Police Department’s 2007 Part I crime categories (Courtesy: MBTA).

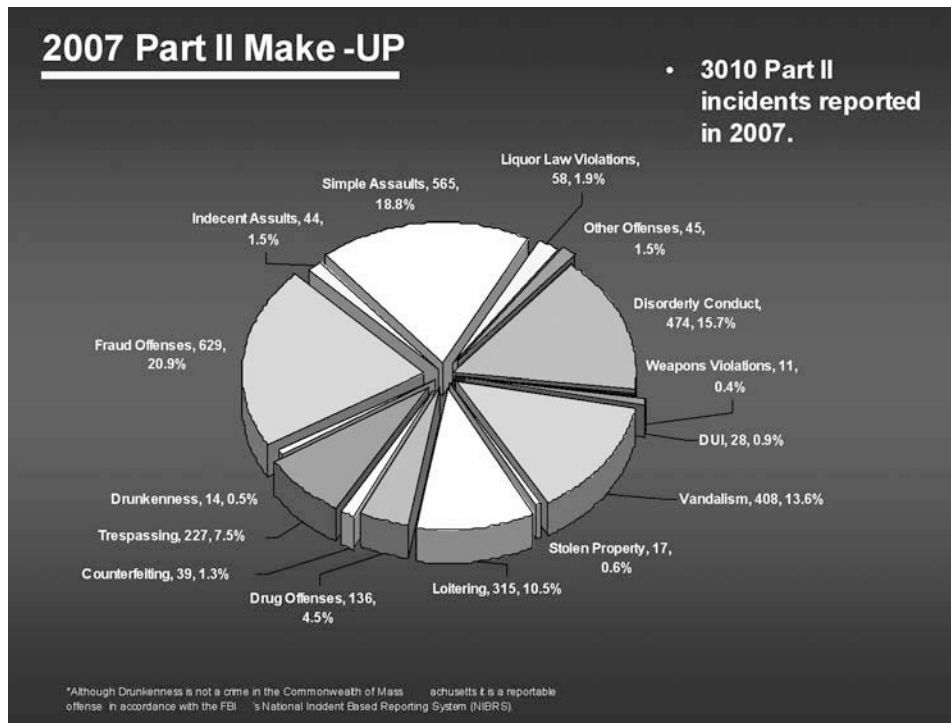


FIGURE 18 MBTA Transit Police Department’s 2007 Part II crime categories (Courtesy: MBTA).

BAY AREA RAPID TRANSIT (SAN FRANCISCO, CALIFORNIA)

BART is a regional heavy rail mass transit system that carries about 92 million passengers annually, with a weekday rider-

ship of approximately 350,000. BART’s service area spans four counties (Alameda, Contra Costa, San Francisco, and San Mateo) and 60 different police jurisdictions in the urban San Francisco Bay Area. Plans are under way to expand to a fifth county, Santa Clara, which includes San Jose (see Figure 21).

Victimization Rates

Rates of Part I Crime Victimization on the MBTA system			
Line	Typical Week day Ridership -Unlinked (FY 2006)	Average Weekday Part I Crime (FY200*)	Rate of a I Crime occurring per 100,000 Passengers
Red Line			
Totals	213,700	0.80	0.37
Blue Line			
Totals	60,950	0.06	0.07
Orange Line			
Totals	161,350	0.74	0.45
Green Line			
Totals	202,400	0.15	0.07
Buses/MBTA Yards			
Totals	373,250	0.39	0.1
Commuter Rail			
Totals	136,805	0.57	0.41
Silver Line			
Totals	25,715	0.02	0.07
System Wide			
Totals	1,188,071	0.02	0.04

*2007 Part I Crime data was used with the 2006 Ridership numbers due to 2007 Ridership number not being established as of yet.

FIGURE 19 MBTA Transit Police Department Part I crime rates by line (Courtesy: MBTA).

System Wide Statistics

UCR Group	UCR Sub-Group	1997	1998	1999	2000	2001	2002	2003	2004	2005	0006	2007
Part Total		1182	1114	1321	1095	1233	1144	1215	1009	1000	971	873
Arson		3	3	2	3	1	4	2	2	1	0	0
		3	3	2	3	1	4	2	2	1	0	0
Assault		132	146	143	137	144	125	152	127	162	135	112
	Firearms	6	11	8	9	5	6	7	3	9	4	10
	Hands/Fists/Feet	0	0	0	0	0	0	12	14	16	12	9
	Knife/Cut	35	38	45	46	61	40	38	31	47	37	26
	Other Weapon	91	97	00	82	78	79	95	79	90	82	67
Burglary		48	59	36	26	35	37	36	15	26	18	15
	Attempted	6	12	10	6	12	7	3	0	0	0	0
	Forcible	41	41	24	19	22	28	32	15	26	18	15
	Unlawful	1	6	2	1	1	2	1	0	0	0	0
Criminal Homicide		0	2	0	1	1	1	3	2	2	0	1
	Manslaughter/NEGL	0	0	0	0	0	1	0	0	1	0	0
	Murder/ Nonneg MNSL	0	2	0	1	1	0	3	2	1	0	1
Forcible Rape		4	4	3	4	4	3	4	1	3	3	2
	Assault to Rape	1	3	1	0	2	1	4	0	3	3	2
	Rape by Force	3	1	2	4	2	2	0	1	0	0	0
Larceny-Theft		653	661	852	642	800	674	705	636	550	541	505
	Bikes	48	44	72	61	105	74	58	81	98	88	101
	From MV	276	271	394	246	255	267	299	218	159	143	155
	Other	150	156	143	128	168	123	125	131	151	188	148
	Pick-Pocket	150	156	143	128	261	202	210	188	123	112	83
	Shop lifting	18	16	16	14	11	8	13	18	19	10	18
Motor vehicle Theft		112	72	101	64	60	73	83	46	41	46	55
	Autos	112	70	100	64	60	72	82	46	41	46	55
	Stolen Other Vehicle	0	0	0	0	0	0	1	0	0	0	0
	Trucks/ Buses	0	0	1	0	0	1	0	0	0	0	0
Robbery		230	167	184	218	188	227	230	180	215	228	183
	Firearms	34	21	20	24	21	21	31	10	17	21	9
	Knife/ Cut	55	32	50	52	47	54	54	26	29	17	9
	Other weapon	6	3	6	3	3	4	8	25	25	29	26
	Strong Arm	135	111	108	139	117	148	137	119	144	161	126
Part II Totals		503	509	437	471	518	487	585	555	618	623	565
Simple Assaults		503	509	437	471	518	487	585	555	618	623	565
Grand Total		1685	1623	1758	1566	1751	1631	1800	1564	1618	1594	1438

FIGURE 20 MBTA Transit Police Department's Part I and Part II systemwide crime statistics (Courtesy: MBTA).

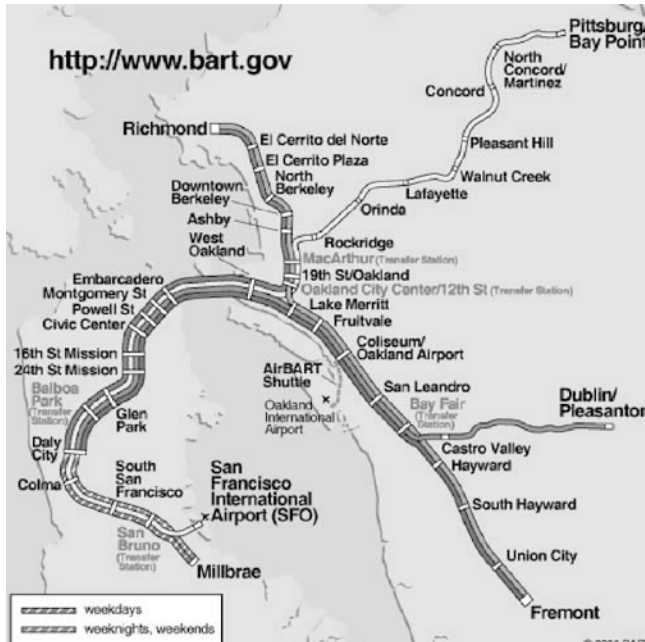


FIGURE 21 BART system map (Courtesy: BART).

September 11, 1972, was BART's opening day of passenger service. BART is governed by a nine-member board of directors who are elected officials from the nine BART districts. The 43 BART stations include 15 surface, 13 elevated, and 15 underground stations. In 2003, BART completed an extension to the San Francisco International Airport. BART's track mileage totals 104 miles of which 3.6 miles are in an underwater Transbay tunnel. BART currently has 669 revenue vehicles with another 80 cars being planned for acquisition; 46,000 parking spaces are provided to BART customers.

BART trains operate from 4:00 a.m. to midnight on weekdays, 6:00 a.m. to midnight on Saturdays, and 8:00 a.m. to midnight on Sundays. On weekdays, trains operate approximately every 15 minutes. Transbay train intervals between downtown Oakland stations and San Francisco stations are every 2.5 minutes during the peak hour and every 5 minutes in the midday.

The system has both entry and exit gates; at the exit, the Automated Fare Collection system determines the distance-based fares, takes tickets, and informs passengers if additional payment is needed or deducts the proper amount from multi-ride tickets.

Chief Gary Gee heads the BART Police Department, an autonomous law enforcement agency with more than 300 personnel, of which 215 are sworn peace officers who provide the full range of law enforcement services. To prepare for major emergencies, critical incidents, and tactical responses, the department has teams of highly trained officers for tactical response and crisis negotiations and is a signatory to the Bay Area's mutual-aid pacts (see Figure 22).



FIGURE 22 BART police vehicle (Courtesy: BART).

Qualifications and training for BART police officers exceed the guidelines of the state's Commission on POST. In addition to meeting POST requirements, every BART police officer applicant must have at least 30 college semester units. Although most officers are assigned to the Patrol Bureau, specialized assignments include field training officer, canine handler, investigations, bicycle patrol, field evidence technician, personnel and training, background investigations, crime analysis, traffic, FBI Joint Terrorism Task Force, and the antivandalism and special-enforcement teams.

In addition to regular police and counterterrorism training, the provision of behavioral assessment training to BART officers is being considered. Counterterrorism training is provided by BART to frontline transit employees, and drills are conducted on a regular basis with other agencies and law enforcement. Also, training (primarily DVD-based and targeted train-the-trainer workshops) is provided to local law enforcement and members of the police academy as they are about to graduate.

During BART's first 13 years of revenue service, police officers reported to the transit district's headquarters in Oakland. In 1985, the success of a field office in Concord spawned the establishment of additional field offices. They enabled officers to patrol their beats longer and become more familiar with their communities. In 1993, BART was further decentralized when the department was divided into four police zones, each with its own headquarters and field offices. Zone commanders were provided with personnel, equipment, and resources to manage their operations. This decentralized structure enables BART police officers to work more closely with the local residents, community organizations, businesses, schools, allied public-safety agencies, and other transit district employees.

Today, BART police facilities and field offices are located in Oakland, Concord, Walnut Creek, Pittsburg/Bay Point, El Cerrito, Dublin/Pleasanton, Castro Valley, Hayward, San Francisco, Colma, and San Bruno. Police commanders provide input to planners for BART's future extensions.

SWAT Team

The Special Weapons and Tactics (SWAT) Team receives special training on equipment techniques and training.

Personnel are selected from applicants based on a range of criteria, including physical fitness, firearms proficiency, and supervisory recommendations. Team members receive specialized training from several sources, including local FBI courses and joint training with other local teams. Team members train on scenarios that include situations aboard trains within tunnels, on elevated trackways, or in stations. In addition to situations unique to the BART system, the department's SWAT Team is utilized to make "high-risk entries" pursuant to warrants obtained by the department. The use of the specially trained team members decreases the likelihood for resistance and enhances the safety of police personnel and the general public.

Bicycle Patrol

In 1991, the BART Police Department became the first domestic transit agency to implement a dedicated, full-time bicycle patrol unit. The unit supplements the regular patrol beats and focuses on problem areas in and around the BART stations. The unit was especially effective in and around the stations with parking facilities, bus transfer areas with heavy pedestrian traffic, and urban areas with heavy traffic. Where an untimely train schedule would make a regular patrol officer's response slow, the bike officers were able to respond more quickly. The unit's interaction with the community was high, with 98% of the bike unit's cases self-initiated.

Graffiti Task Force

In 1997, BART created an antigraffiti task force to fight the ongoing problem of graffiti, which costs the agency more than \$1.5 million each year in cleanup and repair expenses. The task force includes members of several different operating departments at BART, including the BART Police Department, which has a dedicated unit of officers known as the TAG (Together Against Graffiti) Team. TAG officers and other BART officers arrest suspects and encourage the public to report graffiti vandalism by calling 9-1-1 or BART's graffiti hotline; a cash reward of up to \$500 is offered for tips that lead to an arrest.

Post-9/11 Security Measures

The most significant impact that 9/11 has had on BART's security and policing management is the inclusion of homeland security to its mission. Since 9/11, the emphasis has been to further harden BART's critical infrastructure against the threat of terrorism. Risk assessments confirm that the most vulnerable elements of BART's system are the Transbay Tube, other tunnels, and underground stations; likely threats include IEDs on trains and platforms.

The department hosts drills for the region's first responders and participates in local, state, and federal counterterrorism working groups. An officer is assigned full time to

the FBI Joint Terrorism Task Force, and a command officer is designated as the department's mutual-aid, counterterrorism, and homeland security liaison. All of the BART Police Department's canines are highly trained and certified to detect explosives. After the London and Madrid attacks in 2004, BART started acquiring explosives-detection canines, and currently nine canine teams patrol BART stations. Every canine undergoes two hours of training on a daily basis to maintain their explosives-detection capability.

Although general crime is a daily concern for BART officers, the BART Police Department recognizes the importance of preparedness against terrorist attacks, because it is likely that the United States will be attacked again. Historically speaking, transit is a likely target of a terrorist attack, and all major U.S. systems have vulnerabilities associated with being open to the public. After 9/11, the BART Police Department took steps to mitigate vulnerabilities and implemented counterterrorism measures even though no additional resources were provided for these efforts. Following are the key post-9/11 security measures implemented by BART. A more detailed chronological listing is shown at the end of this case study.

- Conducted outside threat and security assessments (FTA and Total Security Services International, Inc.)
- Closed public restrooms (first at all stations, then at subway stations only)
- Controlled elevators by station agent (previous on automatic control)
- Removed garbage cans from subway platforms
- Trained employees on nuclear, biological, and chemical agents, WMDs, and terrorism
- Trained police officers on first response to critical incidents, including joint training with allied law-enforcement agencies
- Enhanced alarm and CCTV systems in stations and facilities
- Enhanced perimeter and internal controls at facilities
- Implemented employee, contractor, and vendor background checks
- Increased high-visibility patrols and train sweeps
- Issued an unknown-powder protocol
- Purchased escape masks and safety vests
- Participated in counterterrorism task forces
- Conducted regular searches and sweeps of stations and trains
- Installed alarms at both ends of the Transbay Tube
- Installed seals on fire hose cabinets and areas where items could be concealed
- Implemented a marketing plan to enhance awareness of personal safety and security
- Held ongoing training and distributed reminders to employees that BART is a potential target for terrorists
- Purchased handheld chemical-agent detectors

- Cross-trained police canines in explosives detection
- Included WMD scenarios as part of regularly scheduled emergency drills
- Enhanced access control through smart-card technology
- Formed partnerships with national labs on vulnerability to explosives blasts and air distribution in underground areas
- Held security meetings with other in-house departments and general management;
- Created a threat-assessment matrix for police and transit operations.

To further ensure the personal safety of BART riders, pay phones and emergency call boxes in parking lots connect directly to the BART police 9-1-1 communications center. The District also uses video surveillance systems in trains, stations, and parking lots. Police reports are transmitted electronically on a new computer-aided dispatch and records-management system.

BART is part of the Bay Area’s Regional Transit Security Working Group. It is a joint-powers consortium, which includes members from the Bay Area’s Tier 1 and Tier 2 agencies. The Regional Transit Security Working Group meets regularly to discuss how the Bay Area’s Super Urban Area Security Initiative resources will be distributed among the transit agencies.

BART is currently facing challenges related to interoperable detection equipment and communications. BART has received \$5.4 million to outfit four stations with an interoperable CCTV network—images from the CCTVs will be provided to BART police headquarters as well as to the OCC. Images are stored for one week. Intelligent video capability to identify suspicious objects and activities is being planned. This network is a significant step forward for BART because the many cameras it now has in its stations are not interoperable and do not store images.

In terms of threat detection technologies, radiological pagers are available to BART officers and are used when warranted. Other threat detectors have been tested, but they were not considered to be feasible for BART. Biological, chemical, and explosives detectors that would be viable for use on train cars for continuous environmental screening are desired.

Local law enforcement and emergency responders may need to access BART stations, trains, and infrastructure to apprehend criminals or to respond to emergencies and incidents in the system. Although some communications interoperability with fire departments has been established, interoperable communications with local law enforcement agencies has not been achieved because each agency has its own communications system.

To augment BART police officers, administrative employees have been trained to operate two-way radios and are deployed to station platforms. The nonpolice employees wear iridescent green safety vests, are an added visible presence, and provide extra eyes and ears for the police.

Crime Statistics

The BART Police Department provides data on crimes against persons, vehicle-related crimes, and police emergency-response times that are published in a quarterly report to the transit agency’s board of directors. Examples of these quarterly graphs are provided in Figures 23–25.

In terms of crime trends and categories, other than a spate of bomb threats and reports of suspicious powder immediately after 9/11, the only significant and sustained change has been to the number of reports for unattended and suspicious packages. This is the result of customer security awareness ad campaigns and announcements encouraging riders with the message, “If you see something, say something,” and reminding them to report anything out of the ordinary (see Figure 26).

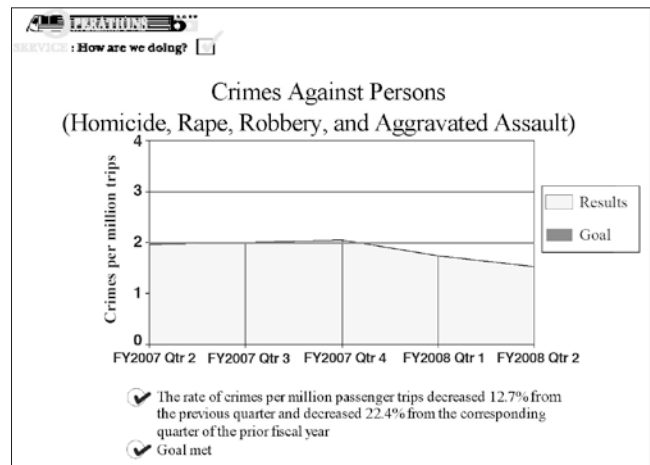


FIGURE 23 BART Crimes against Persons quarterly statistics (Courtesy: BART).

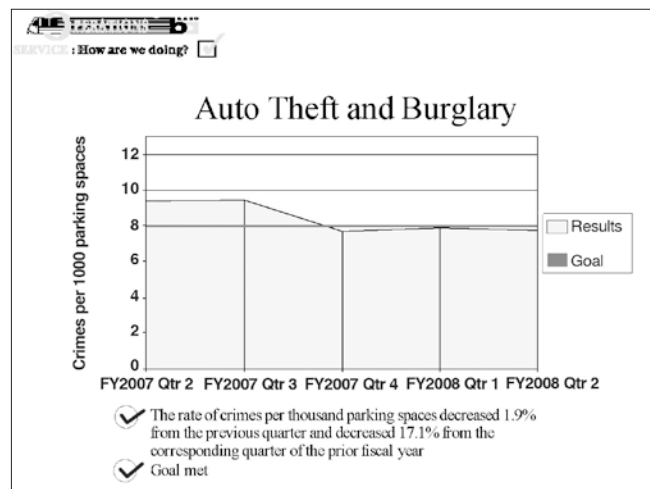


FIGURE 24 BART Auto Theft and Burglary quarterly statistics (Courtesy: BART).

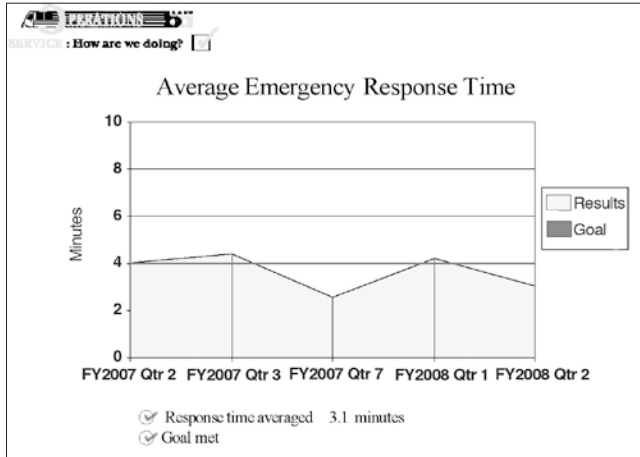


FIGURE 25 BART Average Emergency Response Time quarterly statistics (Courtesy: BART).

Controversy has continued regarding TSA’s VIPR teams. An example of this controversy occurred around the July 4 holiday. Without adequate notification, TSA’s VIPR team composed of security personnel from various states other than California arrived at BART police headquarters and notified BART that they would be patrolling the system during the holiday. The details of the VIPR team’s qualifications and training were not released to BART police; it was clear that they had not been trained on the BART system and were unfamiliar with BART infrastructure, equipment, procedures, and personnel. This raised a serious liability, security, and safety concern for everyone involved—BART’s customers, BART police officers, and employees as well as the VIPR team members. A Memorandum of Understanding is needed to establish an operating protocol, verify standard procedures, and address the many liability issues that arise as a result of the VIPR team’s presence.



If you see an unattended package, please see one of us.

You're here every day—notice anything out of the ordinary? If you see a strange package or suspicious behavior, please notify us now. Contact an employee directly, use the intercom on trains, use the white courtesy phone in the stations, or call BART police at 1-877-679-7000. Thank you for helping keep BART safe and secure.

Let's all use our common senses. We're in this together.



We've increased our alertness. Please join us.

We've added new security methods and equipment at BART, but we can still use your help. Notice unattended packages or suspicious behavior on the train or in the station? Please tell us. Contact an employee directly, use the intercom on trains, use the white courtesy phone in the stations, or call BART police at 1-877-679-7000. Thank you for helping keep BART safe and secure.

Let's all use our common senses. We're in this together. 

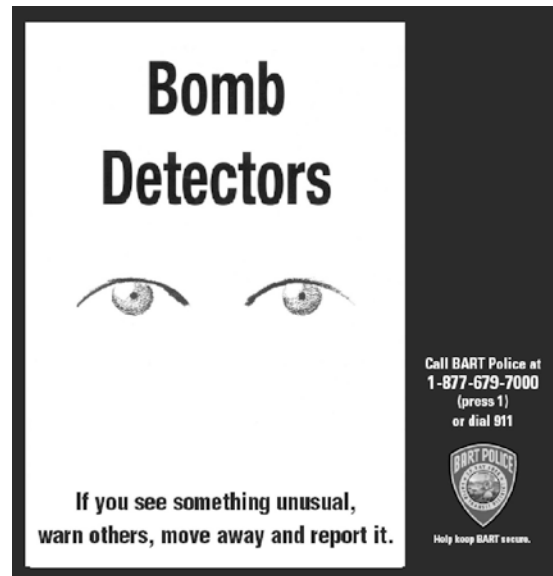


FIGURE 26 Examples of BART customer security awareness campaign literature (Courtesy: BART).

In general, BART police presence and extra security measures are welcomed by passengers. A few customers have complained that the presence of military personnel is excessive and unnecessary. Because BART is on the west coast, which was not a target of the 9/11 terrorist attacks, it is a challenge for BART police to maintain urgency in the minds of senior management and elected officials as well as BART employees and customers.

- BART Police Department is planning to hold a meeting with the BART board of directors to emphasize the seriousness of the terrorist threat and the necessity to invest in appropriate countermeasures to counter the terrorist threat.
- The level of nonofficer employee motivation concerning security-related matters is disconcerting. When NTI's security awareness training was offered on a voluntary basis, only 70 of 2,000 BART employees volunteered to take the training class, even though they would have been paid for their time.
- Customer concerns about terrorism are not significant. Customer focus groups conducted before a security awareness ad campaign determined that customers dislike the use of the word "terrorism" in the campaign because many customers feel that the terrorism threat is not real.

Following is a chronological list of BART's post-9/11 security initiatives:

2001

- Closed Restroom and Removed Bins: Restrooms have been closed and all recycling and garbage bins removed from the platform level in the underground stations.
- Transbay Tunnel (TBT) Cross-Passage Door Alarms: Hard-wired entry alarms installed on TBT cross-passage doors.
- TBT Vent Structure Intrusion Alarms: Motion and entry alarms installed on both the Oakland and San Francisco vent structures.
- TBT Portal Intrusion Alarms: An intrusion alarm system installed in the TBT that distinguish between trains and persons.
- Fire Hose Cabinets: All fire hose cabinets secured with plastic ties.
- TBT Upper Gallery Doors Locked: The doors leading to the upper gallery of the TBT have been secured to prevent unauthorized entry.
- ACT Program: The ACT Program promotes employee awareness of their work environment and encourages them to be aware, question individuals displaying behavior outside of normal patterns, and call the BART Police Department if they are unsatisfied with what they find.

- Anthrax Procedure: Outlines the district's response to suspicious powdery substances found on district facilities.
- Matrix: Outlines the district's response to terrorist events not only in the Bay Area, but also throughout the country and terrorist warnings issued by DHS.
- Police Presence: The BART Police Department stepped up its presence and visibility on the system and regularly sweeps trains during rush hour and uses bomb-sniffing canines to assist. BART police are active participants in the FBI's Bay Area Terrorism Task Force (ongoing).

2002

- Lake Merritt Administration (LMA) Perimeter Security Enhancement: Concrete planters, bicycle lockers, and CCTVs have been installed in the open areas of the LMA Plaza to restrain vehicular entry.
- Escape Hoods: The district issued escape hoods to employees in certain job classifications because they would be expected to act in such a way that their risk of exposure would be greater than if they were to immediately vacate the area.
- Awareness Campaign: The district introduced an awareness campaign for customers. It encourages customers to keep BART safe and to report any suspicious items or activities to BART Police. The latest eyes and ears campaign "Whose Bag?" was rolled out on May 26, 2004 (ongoing).
- Informing the Public of BART's Emergency Plan: Letters have been sent to large local institutions, such as business and schools, as well as city and county governments informing them of BART's emergency response plan. Letters to large local institutions were resent in June 2004.
- Updated NBC (Nuclear/Biological/Chemical) Training: Updated NBC Training material has been rolled out to all district employees.
- Joint Drills/Training Exercises: The district continues to conduct joint drills with first responders in counties served by BART to better coordinate emergency response.
- Ongoing Administrative Employee Emergency Awareness: A basic system safety and emergency awareness guide for administration employees has been distributed.
- Counterterrorism Update: In November 2002, a Counterterrorism Update was presented to approximately 500 employees from TSD, Operations, and BART Police Department. Additionally, the presentation was made at the December Monthly Managers Meeting to about 65 people. The update gives employees a history of terrorism, goals of a terrorist, new projects initiated by the district since 9/11 and a review of the ACT Program.
- Security Related Assessments:

- BART-commissioned threat assessment completed in January 2002,
- FTA security readiness assessment completed in July 2002,
- Participated in the FTA transit security and emergency management planning technical assistance project that began in January 2003, and
- Participating in an Office of Domestic Preparedness risk assessment project that began in August 2004 (ongoing).

2003

- Identification Requirements and Background Checks: Require photo ID cards for all employees, dependents, vendors, and contractors. New employees, contractors, consultants, and vendors are required to go through security and criminal background checks.
- San Francisco Vent Structure: Continuing to work on security at the San Francisco Vent Structure, including the installation of removable bollards to restrict vehicular access and installation of fence-like barrier around pier perimeter at the water line.
- Security Cards: A set of six cards on topics such as suspicious behavior, suspicious packages, suicide bombers, and chemical, biological, and radioactive agents has been distributed to employees. The cards provide employees with information on what to look for and how to respond.
- Training Video: Developed and distributed to employees security training videos, including “Secret Weapon and Bomb ... What If?”
- Station Agent Inspections: Station agents are required to inspect the stations for suspicious packages and unusual activity.
- Publishing Information on the Internet/Intranet: A group consisting of information technology (IT), Rolling Stock and Shops, Transportation, Document Control, and M&E is reviewing and updating current policy guidelines regarding external and internal publication and distribution of information on the Internet, intranet, and other media.
- Lawrence Livermore Laboratory: Lawrence Livermore is currently conducting an elaborate structural analysis study of the Transbay Tube and the vent structure. Once the study is complete, the district will look into mitigation measures that can be implemented. The study will take up to 12 months to complete.

2004

- National Guard Civil Support Team: The district provided the Civil Support Team with basic train operation training in the event of an emergency. The team was trained on how to move trains, perform check-out, and troubleshoot. They conducted a joint exercise with

the OCC in the Transbay Tube and the Berkeley Hills Tunnel. The Civil Support Team went to West Virginia on April 12 for three days to conduct their tunnel drill and exercise. The exercise consisted of a chemical release, simulated explosion at Lake Merritt Station, and structural damage to a BART tunnel.

- Update Unattended Packages Procedure: Under the revised procedures, the TBT as well as the core system from R30 and K30, A10, and M50 inclusive, where total train loading reaches maximum load point, will be treated differently from the outlying areas of the system. For example, OCC will hold trains for the BART Police Department or supervisors to inspect trains between M16 and M10 during rush hour. If the train has to be inspected by the train operator, the train is taken out of service.

CAPITAL DISTRICT TRANSPORTATION AUTHORITY (ALBANY, NEW YORK)

The CDTA, a public benefit corporation, was established in 1970 by the New York State Legislature. The Authority’s legislative purpose is “to provide for the continuance, further development and improvement of transportation and other services related thereto within the Capital Region Transportation District by railroad, omnibus, marine and air” (CDTA 2007).

The CDTA operates 55 bus routes in four counties in the Albany capital district and provides service to several campuses, including Rensselaer Polytechnic Institute, State University of New York–Albany, The College of St. Rose, and Union College. The CDTA serves an area of 2,300 square miles with a population of 769,000 (see Figure 27). The agency has 291 buses in its fleet, 650 employees, three bus depots, and surface parking facilities. The CDTA owns and operates the CDTA Rensselaer Train Station in Rensselaer, New York, and leases and operates the Saratoga Train Station in Saratoga, New York (see Figure 28).

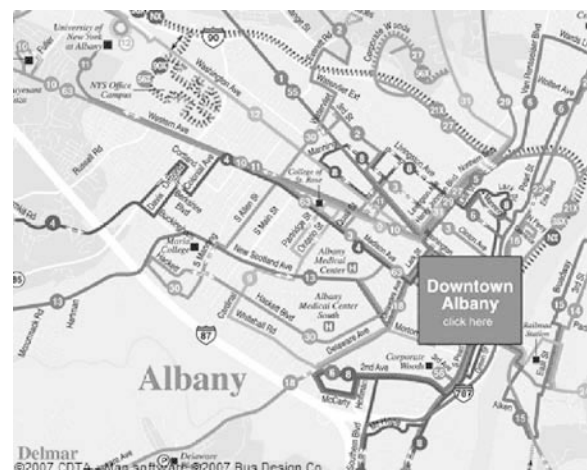


FIGURE 27 CDTA system map, partial view (Courtesy: CDTA).



FIGURE 28 CDTA bus and train station (Courtesy: CDTA).

Best Practices

The CDTA is unique in that it has an extremely small security staff and does not use local law enforcement to patrol its bus system. Conversely, drivers are asked to assist law enforcement in the course of their work when it is safe for them to do so, partnering with many local law enforcement agencies to address security issues. To address its security needs, the CDTA invests in an extensive amount of driver training, including security awareness, gang violence and preparedness training, and comprehensive training for front-line supervisors, including incident management training. In addition, the CDTA uses video surveillance and access control technology to enhance security and has developed interagency emergency response teams.

Driver Training

Because the CDTA operates in communities that experience gang-related violence and has limited security presence within the bus system, the CDTA offers a training course for bus drivers on gang-related violence. The course teaches drivers how to identify gang members and what to do should gang violence occur. Drivers are asked to assist local law enforcement by informing them of gang-related activity or criminal matters such as weapons violations. Recently, when a driver spotted a weapon that had been dropped by a rider on the bus floor, the driver immediately made a report after

it was safe to do so (after the individual exited the bus along with his companions). Subsequently, it was determined by local law enforcement that two individuals had been involved in a kidnapping and were apprehended.

Safewatch

Safewatch is a cooperative program between the CDTA and local law enforcement in which CDTA employees assist the general public. Because all CDTA buses have two-way radios, CDTA employees are trained to be alert and to inform authorities about criminal activity, potential problems, roadside incidents, or accidents. Anyone needing police assistance can flag down a bus for emergency help and the driver will radio a request for police or other assistance that may be necessary. Children in any danger can board a CDTA bus and stay on the vehicle until authorities arrive.

School Outreach Efforts

The CDTA has engaged in a collaborative effort with one of the major school districts and police agencies in the service area to help prevent juvenile crime and disorder. The agencies meet regularly to discuss incidents and ways to effectively address them. The CDTA and school codes of conduct also facilitate these efforts.

Code of Conduct

The CDTA has established a code of conduct for all patrons, including students, of buses and facilities. The CDTA has worked with the schools to establish that CDTA buses are considered an extension of the classroom and students who violate either CDTA's code of conduct or the school's code of conduct will be subject to a suspension from school, CDTA bus service, and CDTA facilities for a period of time. These suspensions become progressively longer with additional violations of the codes of conduct. If anyone who had been disallowed from entering the CDTA system or facilities is identified during the suspension period trying to use the bus system or facility, that person would be subject to arrest for trespassing.

Challenges

From time to time assaults do occur on CDTA operators. A primary security objective of the agency is to deter such attacks and, when an event does occur, to be in a position to identify those responsible and hold them accountable. CDTA bus passengers experience mostly minor harassment and disorderly conduct involving CDTA patrons. In addition, vandalism to bus windows and shelters takes place. Because of the nature of these events, they sometimes go unreported and many times unresolved.

Post-9/11 Security Measures

The height of passenger and employee awareness as indicated by the number of reports of suspicious objects or activity (about one per month for the first year) came immediately after the 9/11 attacks. This number has declined during the past several years and has since leveled off. However, CDTA passengers have welcomed security measures such as video surveillance and encourage the agency to continue to implement additional security for their transit system. The results of risk assessments have indicated that the greatest terrorist threats to the CDTA are explosives and shootings. With a 75% increase in its security budget since 9/11, the CDTA has made and is currently making significant investments in technology, employee training, and the design of buses and facilities, as well as in situational crime-prevention and security protocols and procedures to counter these threats. The CDTA has hardened facilities through security-related projects. These steps have increased the preparedness of CDTA employees and the agency as a whole in case of a major incident or attack.

Funds are still stretched thin and the greatest obstacle in policing management is the lack of resources. With additional funds, the CDTA could increase its security force and make additional investments in technology and training. Following are some of the security measures that have been implemented since 9/11 by the CDTA:

- Completed Preparedness and Security Training:
 - Emergency response training—developed and provided in house by means of the classroom; 100% of frontline employees and 100% of supervisors have taken this training.
 - NTI’s security awareness training—provided in house by means of the classroom; 100% of frontline employees and 100% of supervisors have taken this training.
 - Gang violence training—developed and provided in house by means of the classroom; 100% of frontline new employees are taking this training.
 - NTI’s violence in the workplace—provided in house by means of the classroom; 100% of frontline employees have taken this training.
- Conducted drills and exercises three to four times a year and tabletop exercises are conducted one to two times a year.
- Installed access control using proximity cards at CDTA facilities and depots.
- Performed background checks for all new hires.
- Established cooperative relationships with external agencies and initiated intelligence sharing.
- Developed evacuation instructions.

- Fingerprinted employees.
- Developed an incident response plan.
- Initiated the Safewatch Program.

Following are some of the security measures that have been implemented since 9/11 for CDTA buses:

- Digital video surveillance technology was deployed by the CDTA for enhanced incident management on new buses. The technology better protects drivers from assaults by confirming the identity of the assailant and deterring other crime and terrorism. Also, the technology will be used to review incident information for litigation and training efforts.

By June 2008, about 10% of the bus fleet (28 vehicles) will be outfitted with the video technology, and by the end of 2009, the percentage of the bus fleet with video technology may be as high as 33%. There are eight cameras per bus, one on the dashboard facing the road, five additional internal cameras, and two external cameras. Audio is also recorded along with images. With the installation of additional software, the wireless video technology will allow the transmission of images on a real-time basis to a laptop within a certain distance of the bus. This potentially would allow a police vehicle or responding supervisor to “see” inside the bus in case of an incident or emergency. No vandalism has occurred on the buses on which these cameras have been deployed.

- Silent alarms linked to the dispatch command center are installed in all buses.

Following are some of the security measures that have been implemented since 9/11 for the rail stations:

- Canine teams patrol the rail stations.
- TSA has started to conduct random passenger baggage inspections at the stations.
- Video surveillance technology has been implemented both inside and outside the station and within the stations’ underground parking facilities.
- An emergency response team was formed for the two train stations. The CDTA along with Amtrak, local law enforcement, and tenants within the station formed this team to share information on incidents and other security-related issues, develop projects to address those issues, discuss any policy matters, and engage in live drills and tabletop training. An interagency drill with about 250 participants from the CDTA, local agencies (Rensselaer Sheriff’s Department, Amtrak Police, Rensselaer Police and Fire, and the Regional Hospital), and federal agencies (FBI and ATF) was performed at the Albany/Rensselaer rail station a few years ago (see Figure 29).



FIGURE 29 CDTA emergency preparedness meeting at the Rensselaer Train Station (Courtesy: CDTA).

CAPITAL METRO (AUSTIN, TEXAS)

Currently, Capital Metro’s core system is composed of 250 buses providing both express and local bus service to two counties in the Austin, Texas, region (see Figure 30). A commuter rail system is expected to open in November 2008 (see Figure 31) and plans are in place for the development of a regional MetroRapid bus service (see Figure 32).

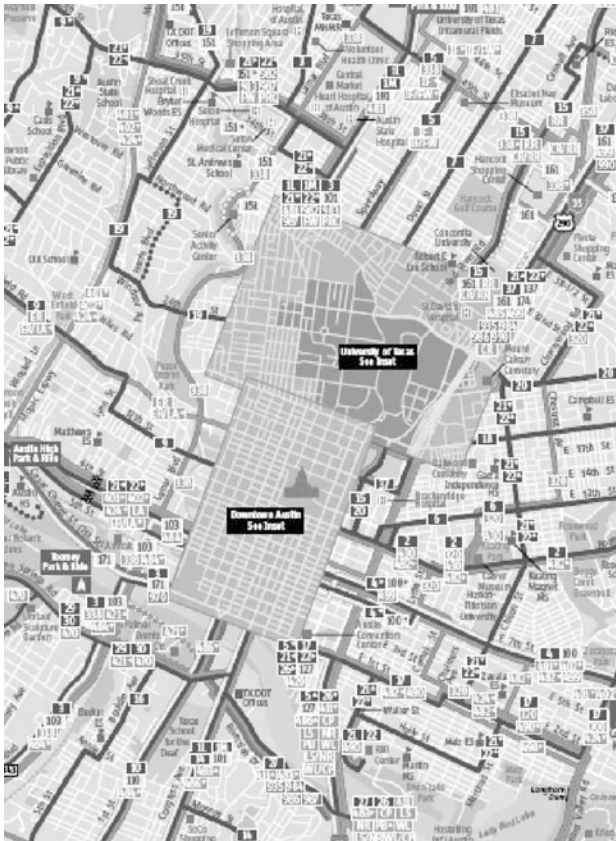


FIGURE 30 Capital Metro system map, partial view (Courtesy: Capital Metro).

**Tactical Operations Guide for
CMTA New Flyer Buses**



Bus Numbers:
7401 thru 7470
&
2001 thru 2034



**Tactical Operations Guide for
CMTA MCI 9300 Series Buses**



Bus Numbers:
9301 thru 9306




FIGURE 31 CMTA Operations Guide (Source: Capital Metro).



FIGURE 32 Capital Metro Bus (Courtesy: Capital Metro).

The commuter rail system is designed to be easily accessible. Some stations will include park-and-ride facilities, whereas other stations will be designed for accessibility by bus, bike, or foot and passenger drop-offs. Once customers reach their destinations, buses will be waiting to whisk them away to places of employment, retail centers, and other locations.

The MetroRapid will be a fleet of bus-rapid transit-articulated buses that will run on certain routes and have transit signal priority technology (transmitters that communicate with signals to keep them green as they approach intersections, if they are already green).

Capital Metro is a small system with a small security staff (three full-time equivalents), which contracts out much of the security work. Because of the small size of its security force, Capital Metro strives to identify cost-effective ways to enhance its security capability and find innovative and efficient solutions to security challenges.

Security considerations are now part of Capital Metro's procurement process. For example, all future buses of any type bought by the agency automatically will have security cameras and recording systems installed as part of the procurement package.

Capital Metro Bus System

Currently, 47% of the bus fleet has security cameras that have event-based recording capability. The total cost of the video technology system was \$1.4 million. Wireless capability that would allow images to be sent to a central command center or to law enforcement was not incorporated into the system for the following reasons: (1) the cost included a monthly fee of a few thousand dollars to maintain system availability, and (2) it used older cell phone rather than broadband technology and was extremely slow. Therefore, it was determined that a wireless system would not be a cost-effective investment for the agency.

These cameras, even without image transfer capability, have been beneficial in deterring crime, terrorism, and false liability claims against the agency. Buses were selected for the installation of video technology based on the length of time they would remain in the fleet, to get the maximum length of time usage for each camera.

Passenger perception of security has improved with the installation of the cameras. Some passengers have provided positive comments about them, whereas others were impressed when the agency was able to use the cameras to identify a subject (perpetrator of a crime). Also, bus operators have used the presence of the cameras to diffuse potential situations, by reminding problem passengers that their actions were being recorded.

Intelligent Bus System—Covert Alarm

A covert alarm is available for bus operators in case of an emergency. When the covert alarm is activated, appropriate response is taken. These alarms enhance the actual security of bus operators as well as their perception of security.

Bus Shelters

CPTED principles are incorporated into all new bus shelters. Designers that submit plans for these shelters must be CPTED certified or they are not eligible to submit their ideas. These principles include eliminating blind spots and

keeping landscaping low and trimmed back so that criminals cannot hide.

Drive-Cams

Drive-Cams were purchased in October 2007 and were installed in all buses by mid-November 2007. Drive-Cams are known throughout the taxi industry as a behavior modification tool that reduces accidents and records near-misses. The recording of the near-misses allows for the incidents to be studied and analyzed. A few transit agencies have been implementing these cameras and have experienced safety-related benefits. Many bus drivers have been caught by Drive-Cam using their cell phones.

A major security benefit associated with Drive-Cam is the ability to identify a perpetrator of a crime (e.g., assault on a bus operator); the technology has been used successfully for this purpose. Because Drive-Cams have been installed on all buses, they specifically benefit the buses that do not have other video cameras installed in them. The operator presses a button and the camera will record what happened in the previous 10 seconds. In addition to the deterrence of assaults on the operator, the Drive-Cam may deter criminals and terrorists from stealing the bus.

Automated Vehicle Location Technology

AVL is currently being installed in Capital Metro's bus fleet. The many security benefits of AVL include tracking and monitoring buses, identifying buses that are off-route (indicating that the bus may have been hijacked), enabling security personnel and law enforcement to quickly pinpoint the exact location of a bus in distress, and ensuring that help can reach the bus in case of an accident or other emergency. AVL has other benefits that make it a cost-effective system for Capital Metro. These benefits include bus performance tracking—for example, detailed reliability metrics can be calculated by stop, time of day, and scheduling support—schedules that differ from actual performance may need to be adjusted. AVL is essential for fleet management during major emergencies and evacuations.

Park-and-Ride Facilities

Park-and-ride areas are being secured by video technology and security patrols. The areas are monitored at the agency's central station by CCTV cameras and are patrolled by street security officers, who are off-duty Austin police officers.

Commuter Rail

Initially, Capital Metro's commuter rail system will serve two counties and comprise nine stations and 32 miles, with an expected first-year ridership of about 52,000; six trains have already been delivered. The system is designed to be

an open system with no turnstiles. There are plans for future expansion of the system (see Figure 33).



FIGURE 33 Capital MetroRail train design (Courtesy: Capital Metro).

CPTED design principles are incorporated in the train and station designs, including the platform areas. Other security measures include the use of CCTVs—cameras have been installed in all of the train cars and record continuously for 72 hours. Multiple benefits are expected from the cameras, including crime reduction, counterterrorism, and liability and insurance cost reduction. Security personnel will patrol the system, staff critical stations during service hours, and participate in random VIPR operations. Fare enforcement will be used as a measure to enhance the security of the rail system. Intrusion detection alarms will be installed to protect the rail system’s critical infrastructure. Capital Metro has a Transit Watch program in place, and it also will be used on the rail system.

Tactical Operations Guide

Capital Metro created a Tactical Operations Guide or First Responders Emergency Guide for the local emergency responder community, which has proven to be highly successful. The distribution of this Guide has led to more than 30 drills and exercises over this past year. The agency is involved to a greater or lesser extent in all of these drills and exercises. The important point of these efforts is that they were based on the content of the Guide and that the responders who are responsible for protecting the lives of the agency’s workers and passengers and its infrastructure during emergencies now have a full understanding of the agency’s transit operations and equipment and are familiar with its personnel. For example, operating a bus is not as simple as it appears to be. If an emergency responder needs to move the bus, they need to know how to start the bus and what to do when a bus has been intentionally disabled—a “healthy” bus can be disabled in several ways. A similar Guide will be created for Capital Metro’s new rail system.

The Guide includes an explanation of the key parts of the bus; procedures on how to start the bus, operate a standard

door, use the braking system, use the fire alarm and fire suppression systems, and use the covert alarm; and instructions on how a bus or the bus engine may be disabled. Instructions on how to force open the front door and how to open an emergency window and roof hatch are provided.

Other Security Practices

Street Patrols

Street patrols are assigned to sectors of the city. They patrol park-and-rides, transfer centers, and bus stops that have experienced criminal behavior in the past. These patrols respond when officers are not responding to calls for assistance, criminal, or accident investigations.

Random, Onboard Security Checks

Random security checks are meant to reassure the public, make them aware that security is working on their behalf, and potentially apprehend problem passengers.

Plainclothes Security Personnel on Vehicles

Plainclothes security personnel are used on routes that have experienced criminal behavior to prevent repeat criminal behavior or to apprehend the perpetrators if the crime occurs again.

Local Intelligence Sharing

Capital Metro is involved in the Austin Area Counterterrorism Planning Task Force, which meets monthly to exchange current intelligence. This task force promotes local intelligence sharing, which is more valuable and pertinent to the agency than information it receives from federal sources.

Performance Metrics and Data Issues

Capital Metro’s principle security metrics are (1) crimes against persons per 100,000 passengers; (2) crimes against property per 100,000 passengers; and (3) average security response time to calls for assistance.

Capital Metro performed a survey of its peers to determine what metrics were being used to measure crime and terrorism-related incidents in the transit industry and found that most agencies do not use metrics and only report actual numbers of incidents. When they do use metrics, they are diverse in terms of the metrics used, their definitions, data collection, and analysis methods. Therefore, Capital Metro determined that there was no way to perform peer comparisons with other agencies. A national format for security metrics along with a standardized, consistent, and comprehensive crime and security incident data collection system for safety data would be helpful.

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY (WASHINGTON, D.C.)

Washington Metropolitan Area Transit Authority (WMATA or Metro) has had a great deal of success in communications interoperability. WMATA's success may be attributed to the robust planning and coordination provided by the Metropolitan Washington Council of Governments (COG). The governments and independent agencies of the National Capital Region use COG as a vehicle to coordinate transit and public safety efforts.

Among the suborganizations of COG are committees for Fire and Police Communications Managers, including both WMATA safety personnel and Transit Police Communications. Both groups meet independently on a monthly basis and jointly each quarter. These meetings familiarize public safety managers in the region with each other and with the communication needs and capabilities of each agency. These efforts paid dividends on September 11, 2001, when the large numbers of first responders flooding into the Pentagon crash site presented unique communications challenges. The Montgomery County Police (Maryland) was in the process of upgrading its radios to a new 800 MHz system and had nearly a thousand portable radios in a warehouse. The radios were immediately reprogrammed to operate on the police and fire 800 MHz networks for the agencies surrounding the Pentagon grounds and were deployed to support the Arlington County Fire Department and responding local, state, and federal personnel. The effective communication between the many agencies on scene at the Pentagon allowed Metro to quickly move bus operations at the Pentagon (the busiest bus bay in the system) to the street in front of the nearby Pentagon City Station and to resume rail service under tight security to the Pentagon Metro Station on the morning of September 12.

Before the attacks of 9/11, the first major effort in establishing regional interoperability was to establish five Metropolitan Interoperability Radio System sites in five host agency communications centers across the region. Each of these host centers has dedicated interoperability devices that house radios from the participating agencies in and around their service area, including radios for transit providers, such as WMATA. When requested, these host agencies can link the requested radio systems so that personnel working together can communicate with each other and agencies can stay in contact with personnel operating outside the normal footprint of their home radio system. This capability would be particularly useful in maintaining communications between multiple agencies during a major incident, such as a natural disaster or terrorist attack.

The most common method of interoperability in the National Capital region is the cross-programming of radios. Most agencies in the region cross-program their radios with

those of partner agencies that have radio systems in the same band. For example, most fire and police agencies in the region use similar 800 MHz radio systems and, with cross-programming, can communicate with adjacent jurisdictions by pressing a few buttons on their radios. One exception to the primacy of 800 MHz radios in the region is the use of the ultrahigh frequency (UHF) band by WMATA Operations, the Metro Transit Police Department (MTPD), and the D.C. Metropolitan Police. However, all MTPD and D.C. Metropolitan Police UHF radios are cross-programmed, and personnel from both agencies frequently coordinate by radio. When interoperability with 800 MHz radios is needed, the Metropolitan Interoperability Radio System sites can create a link between radio systems. Tactical interoperability devices are also carried by MTPD supervisors and can be used, in the field, to link radio systems using portable radios.

Weaknesses in regional interoperability are identified for correction by frequent interagency drills, often with a transit focus. Area fire departments use either actual trains and stations, or the dedicated WMATA facility that contains full-size rail cars, and a simulated transit environment to conduct training under realistic conditions. The training conditions can include smoke, simulated fire, and even a "roll-over" train that can simulate a derailed train at any angle, including upside down. These drills are not limited to basic firefighter skills, but also include radio interoperability elements. Communications-only drills are conducted, where communications occur under conditions in which WMATA's internal radio infrastructure is not available.

The success of the deployment of a large group of radios to the Pentagon area after 9/11 demonstrated the effectiveness of having a cache of radios to deploy during special events or emergencies. As a result, COG created a regional system of radio caches, including a core group of more than 1,200 800 MHz radios programmed to interoperate with police and fire departments throughout the National Capital Area and even neighboring regions. These radios are stored in three geographically diverse sites and can be transported by dedicated vehicles on short notice. Each cache contains an evolving mix of equipment that includes tactical repeaters, cross-band switches and spare batteries, chargers, and a generator for extended operations. The basic deployment package includes specialized equipment for extending radio coverage into subway tunnels. The planning that went into creating these radio caches focused heavily on what was needed for emergencies within a transit environment. Because regional fire service personnel trained frequently in simulated transit emergencies, they recognized the subway tunnel environment as a uniquely difficult challenge to interoperable communications.

Two other areas of interoperability that the national capital region is exploring are data sharing and interoperability between Public Safety Computer-Aided Dispatch Systems.

Regional public safety officials recognize that it would be beneficial for specialized agencies like Transit Police to be notified immediately and seamlessly when an incident occurs within their jurisdiction or when it affect their operations. A

rapid flow of information between and among police, fire, and traffic management control centers would allow for limited disruptions for commuters and ease congestion around incidents.

CHAPTER SEVEN

CONCLUSIONS

Research results indicate that integration of security continues to occur holistically on many levels within transit agencies, including daily transit operations, training and education, customer outreach, capital budgeting and resource allocation decisions, and planning and procurement processes. This finding supports the FTA's Security and Emergency Management Technical Assistance Program (SEMTAP) finding that such programs are maturing and supports a proactive instead of a reactive approach. At the same time, this process needs to continue toward all-hazards, full-risk integration and management, and become more consistent across transit agencies and divisions within an agency.

Within the security industry, a similar integration process is occurring: systems are being integrated across vendors and devices, and security technologies and systems are converging. Detection systems are being integrated with access control systems, physical access devices with identity management, and physical with logical elements. The result will be a *global solution* that will effectively prevent, deter, detect, mitigate, and enable a multiunit, multiagency response to large and small incidents. Security systems eventually will be able to synthesize and analyze different streams of real-time and historical data from various sources, identify suspicious activity based on this integrated analysis, and transmit the information to appropriate internal and external personnel and responders according to the level and nature of the threat or incident.

PROJECT FINDINGS

The primary post-9/11 changes in security practices include the implementation of Transit Watch or a similar employee and passenger awareness and outreach program, and the provision of security training to frontline employees and counterterrorism training to police and security personnel. Transit agencies have increased the number and hours of security personnel; conducted threat and vulnerability assessments; received intelligence information from federal agencies; and increased local and regional coordination and outreach efforts through counterterrorism committees and intelligence and information sharing with local responders and neighboring transit agencies. Human resources practices have changed as well, particularly regarding background checks.

According to survey respondents, post-9/11 security investments have had a positive impact on terrorism deterrence and detection capabilities, general crime mitigation, and the public, passenger, and employee perception of security. Agencies report that their public outreach efforts have contributed to increased passenger and employee awareness, improved employee preparedness and increased security in terms of deterrence and detection.

The following measures were considered by survey respondents to be the five most effective for counterterrorism:

1. Transit Police Officers/Security Personnel Patrols/Sweeps
2. Security Training for Transit Employees and Police/Security Personnel
3. Video Technology
4. Public Education/Transit Watch and Outreach
5. Intelligence Information.

The following measures were considered to be the five most effective for crime prevention:

1. Transit Police Officers or Security Personnel Patrols/Sweeps
2. Plainclothes Officers/Unmarked Vehicles
3. Video Technology
4. Presence of Transit Employees
5. Lighting and Visibility.

These measures along with innovative measures are summarized in the following section.

TRANSIT SECURITY PRACTICES

There are differences in the characteristics of criminals and terrorists. An important difference is that terrorists typically

engage in careful planning and an extensive target selection process and are deterred by changes in expected conditions of the system, such as the unexpected presence of officers. Therefore, random checks and other unscheduled security measures may be strong deterrents. Criminals, on the other hand, often take advantage of any opportunity that may present itself and may be more deterred by methods that would lead to their arrest, such as video surveillance. These differences should be considered during the selection process for practices and measures.

The following are effective counterterrorism practices, anticrime practices, and practices applicable to both counterterrorism and anticrime identified by the Synthesis survey, case studies, literature review, and input from industry experts:

Counterterrorism Practices

Identity Management

The ability to verify the identity of a transit police officer or security personnel, a transit employee or contractor, or a visitor is important in preventing unauthorized physical access into sensitive transit facility areas or virtual access into the agency's network or its databases.

Intelligence Information

Gathering, sharing, and analyzing information is an important security practice. Gathering and identifying agency-specific, actionable information; analyzing intelligence information to determine its reliability and relevance to a particular agency; and sharing information can lead to redeployment of resources and changes in tactics that result in improved security and deterrence capability. Agencies that have reached out to peer agencies to share and exchange relevant information have succeeded in receiving focused intelligence as a result. A few larger agencies have created in-house intelligence units. Intelligence-sharing between the agencies and their federal, state, and local partners is further facilitated through TSA's Mass Transit Security Information Network's interagency communication and information-sharing protocols. The Homeland Security Information Network—Public Transit (HSIN-PT) Portal has been integrated into this network to provide a one-stop security information source and outlet for security advisories, alerts, and notices.

Passenger Security Inspections

Passenger security inspections (PSIs) include random baggage inspections, canine patrols, and behavioral assessment. Although the practice of PSI baggage inspections is currently limited to several transit agencies, canine PSI is conducted by rail systems, including Amtrak. Behavioral assessment is a relatively cost-effective PSI method that is readily deployable;

in addition to training transit police and security staff, training transit employees in behavioral assessment would effectively expand the reach of the police force as many transit employees are in constant contact with the general public.

Public Education and Outreach Campaigns

These campaigns inform passengers about the importance of reporting suspicious activities, persons, or items. Because it is impossible for security personnel to be in all locations at all times, enlisting thousands of the agency's transit passengers to become the eyes and ears of the agency makes sense in terms of economics and effectiveness. As time passes without a major terrorist event, passengers as well as transit workers become less alert, and public outreach and awareness programs increase in importance. Public education and outreach efforts are further enhanced by programs such as "Play Your Part" through which the Transportation Security Administration (TSA), in joint efforts with mass transit and passenger rail agencies, advances security awareness among the traveling public and public and private partners. TSA Transportation Security Inspectors—Surface, supported by the Mass Transit Division, form partnerships with the agencies in high-visibility public awareness campaigns. These campaigns alter the normal activities at terminals or stations and enhance passenger awareness of and vigilance for suspicious activities and items as possible indicators of terrorist preparations for or execution of an attack.

Regional Coordination

Coordination among transit agencies, emergency responders, local departments of transportation (DOTs), and other relevant agencies can improve the effectiveness of drills and exercises, intelligence-sharing initiatives, resource-sharing and funding-allocation initiatives, and emergency preparedness and response, and can help address regional security-related problems such as interoperable communications.

Training Transit Police and Security Personnel

Security awareness training and more specialized counterterrorism training are practices universally believed to be effective in enhancing the preparedness of transit systems. Training transit employees in basic security matters such as identification of suspicious activity, persons, and items is important because frontline employees come into constant contact with the general public and passengers. These trained employees can effectively expand the reach of transit police by acting as their eyes and ears. Additional training in countermeasures and specific threats, and in the PSI technique of behavioral assessment, is also important because transit workers are likely to be the first ones to detect a threat and respond in an emergency. Initially, a range of security training materials for transit workers were developed through FTA-sponsored programs to assist transit agencies. To further assist these agencies, TSA, in consulta-

tion with FTA and other public and private security partners, developed and published the Mass Transit Security Training Program. This program, presented on TSA's website, provides detailed guidelines for mass transit and passenger rail agencies to facilitate development and implementation of security training programs, and specifies the subject areas in which particular categories of employees should receive training. These guidelines are implemented under the Transit Security Grant Program. Course options include programs funded by FTA/TSA (transit-specific terrorism prevention and response) and Federal Emergency Management Agency (FEMA) (general terrorism prevention and response).

Trace Detection Technology

Technology to detect residues from explosives is available to transit agencies in different forms. Portable devices are especially useful in screening suspicious objects that may be found anywhere within a transit system. *Radiological pagers* are used by transit agencies to detect nuclear threats. *Chemical detectors* are being tested at major transit systems. The continued development and testing of both *chemical and biological threat detectors* are equally important. These technologies may be linked with video systems to provide real-time video feeds of identified threats.

Anticrime Practices

Codes of Conduct

These codes include rules that passengers must follow once they enter the transit system. By enforcing the code, a transit agency presents an image of being in control of its transit environment and enhances the security of its transit system.

Crime Statistics Map

An interactive, user-friendly crime statistics map is a valuable visual tool for transit police and is useful for the strategic deployment of officers. Visually presenting up-to-date crime data using a crime map provides passengers with a security tool and the sense that they have greater control over their transit trip.

Plainclothes Officers

Plainclothes officers within the transit system can catch perpetrators such as vandals or fare evaders in the act of committing a crime. The use of *unmarked vehicles* is also an effective practice in catching perpetrators of crimes in transit park-and-ride or other parking facilities.

School Outreach

These programs involve the participation of schools in the transit agency's service area to enforce passenger codes

of conduct and discourage disorderly behavior in juvenile populations.

Bus Driver Training

Training drivers in customer relations, conflict mitigation, and gang-related violence is an effective security practice and provides bus drivers with greater confidence and knowledge to deal with the public.

Counterterrorism and Anticrime Practices

Crime Prevention Through Environmental Design

Although not new to anticrime efforts, Crime Prevention Through Environmental Design (CPTED) is applicable to counterterrorism efforts as well. In the design of new transit facilities and vehicles and in their retrofitting, CPTED principles can enhance security by hardening the potential transit target and making the environment less conducive to covert activity. For crime prevention, survey respondents identified lighting and visibility as being especially effective. Some of these principles can be readily implemented by transit personnel; however, contractors and manufacturers should be consulted for major design work and retrofitting changes to stations and transit vehicles.

Collaborative Transportation Imagery Project

TSA and its partner agencies are working jointly on the Collaborative Transportation Imagery Project to produce detailed mapping and interactive imagery of key assets and systems to inform and enhance the quality of operational activities and address threats and security incidents, security plans, training programs, and exercises. The product, provided on a digital video disc, incorporates multiple types of imagery, satellite maps, schematics, and related materials to provide a comprehensive view of the transit system, detailing significant infrastructure and security apparatus.

Transit Police and Security Personnel

High-visibility patrols and specialized counterterrorism teams can perform sweeps of transit terminals, stations, and trains and buses. This high visibility is believed to deter both terrorism and crime, and present a public image of a secure and safe transit system. Making the presence of transit employees more visible (e.g., use of brightly colored vests) is also believed to be an effective anticrime and counterterrorism practice, and lessens the passenger perception of fear.

Visible Intermodal Prevention and Response

Visible Intermodal Prevention and Response (VIPR) teams have been deployed at hundreds of transit systems throughout the country. These teams augment security in the sys-

tems, expanding the agencies' capabilities to implement random, unpredictable security activities to deter both terrorism and crime.

Video Technology

Video is considered to be effective in deterring and detecting crime and terrorism. Closed-circuit televisions with recorders can identify perpetrators and verify crime occurrences such as assaults. Recordings of incidents and accidents can be used in postincident analysis. Although video technology has been in existence for many years, its continuing effectiveness as a security measure lies in the increasing power of its analytics, multiple uses, and scalability. Intelligent video technology can identify many types of behaviors, including potential burglaries, abandoned items, vandalism, and stopped vehicles. Video cameras can be linked with detection systems such as intrusion detectors and chemical detectors. Real-time image transmission is also possible.

Other Findings

Crime Trends

According to the Bureau of Justice Statistics, a nationwide decline in crime and a concomitant decrease in transit crime were seen in the United States starting in the mid-1990s. Transit crime dropped significantly from 1997 to 2002 and then began to plateau. Industry experts raised concerns about the reliability and accuracy of National Transit Database (NTD) data; however, based on the NTD analysis conducted for this study, the following conclusions can be made: There were many more minor than serious crimes, and the numbers of the most violent crimes—homicide and rape—were extremely low. For serious Part I offenses, the most problematic was theft, and for less serious Part II offenses, the most predominant was fare evasion, with a majority of the citations occurring on light rail systems.

Major Incidents, Suspicious Activity and Threats

Following 9/11, there was an increase in suspicious activities, persons, and items. These reports have diminished and have plateaued over the past few years.

Passenger Perception of Crime and Terrorism

Public perception of transit security is influenced by media coverage and the entertainment industry, which tend to aggravate public fears. Minor crimes and disorder also affect passenger perceptions even if the actual consequences are insignificant. There are also regional differences in the perception of terrorism. For example, east coast transit passengers are more aware and tolerant of terrorism-related security measures compared with their west coast counterparts.

Performance Metrics

Performance metrics help assess and track the performance of security systems, practices, and measures as well as the overall security of a transit system. Metrics can highlight the benefits of security to agency management and other stakeholders.

PROBLEMS AND OBSTACLES

The greatest obstacle in security and policing management reported by survey respondents was by far the lack of resources to implement desired security measures. Stakeholder support and related issues included the following:

- Lack of customer support and lack of qualified workers or technical expertise were reported by some agencies.
- Support from decision makers with budget authority (e.g., elected officials, board members, and senior agency management) and acknowledgment of the terrorist threat was reported by a few agencies.
- Motivating officers to focus on ordinary crime has become more challenging because officers perceive counterterrorism assignments to be more prestigious and therefore desirable. Several transit agencies expressed concern about the motivation of transit employees in implementing security practices.
- For unionized transit workers, the increased time needed to perform added security-related tasks was cited as a potential issue, because this may impinge upon prenegotiated labor agreements and cause labor relations issues. Agencies may wish to seek union participation and buy-in before implementing new security practices and measures.

Other reported problems and obstacles included the following:

- Lack of specificity of intelligence and the desire for more focused intelligence was reported by a few agencies.
- Interoperable communications barriers hamper the efforts of transit police, personnel, and first responders. Barriers to interoperability include technical, financial, and human factors issues. Rail infrastructure faces special communications challenges, including the provision of wireless communications.
- Relatively few frontline transit workers participate in drills. Because frontline workers are usually the first ones at the scene of an emergency, crime, or terrorist attack, involving them in training and evaluation exercises would be advisable.
- Two transit agencies expressed the need for the development of a Memorandum of Understanding with TSA regarding the federal VIPR program. TSA responded to these concerns with a collaborative effort to enhance

coordination of deployment and effectiveness of the security augmentation operations. Products resulting from this effort provide guidance on planning, preparation, coordination, execution, and after-action review of VIPR deployments and describe the capabilities of each component of a VIPR team with recommendations on their most effective use. The coordination and review of operational plans by mass transit and passenger rail agency security officials before VIPR deployment ensures mutual understanding of security activities and procedures to address identified threats, suspicious activities, and incidents of apparent criminal conduct.

- Questions about the reliability and accuracy of NTD security and incident data and year-to-year consistency were raised. Data terminology issues were identified—for example, insignificant incidents are classified and reported under the category of “bombings.” These issues need to be researched and addressed.

RESEARCH NEEDS

The following research needs were identified in the Synthesis report.

Data and Performance Metrics

NTD Data

Enhancing the reliability of NTD security and incident data, improving temporal consistency, and addressing terminology issues were identified in this study.

Crime Trends

Research on the underlying causes of the changes in specific crime and incident categories identified in the NTD may be of interest to transit agencies once the fundamental accuracy issues of NTD data have been addressed.

Security Metrics

Security metrics can demonstrate the value of security to the agency, the customer, the general public, and other stakeholders by conveying and quantifying the specific benefits of security investments. Clear and consistent security measures are important when comparing the security levels of peer agencies. These measures would benefit from consistent data definition, collection, analysis, and reporting methodologies.

Victim and Offender Characteristics

Research on the characteristics of transit crime victims and offenders is recommended as these data are not readily available.

Crime-Reporting Issues

More research is recommended to determine the extent of and reasons for underreporting, as well as possible overreporting of transit crime. New crime-reporting procedures, the level of customer understanding of how to report transit crimes, and how best to promote the notification and documentation of relevant incidents by frontline personnel are suggested for further research.

Intelligence Information and Information Sharing

What do transit agencies consider actionable intelligence? Is there a common definition, or does it differ from agency to agency? These questions, along with the security gaps in information sharing identified by SEMTAP, remain and need to be researched.

Interoperable Communications

Transit-specific interoperability issues need to be addressed. Some of the issues are common to many transit agencies, but each agency faces specific issues as well. Therefore, transit agencies need to identify interoperable communications issues and problems within their agency, find out how to address them, and determine how they may participate in regional, state, and federal interoperability programs and efforts.

Training, Evaluation, and Motivation

Training

Although an enormous amount of progress has been made since 9/11 in providing security training to transit employees, the lack of ample security training sources and materials for and delivery to transit managers above the supervisory level is a concern that needs to be addressed. Additionally, the need for adequate refresher training and training reinforcement for awareness and security orientation training were noted by SEMTAP.

Evaluations

Transit workers usually are not evaluated in terms of security awareness, implementation of security training content, and other related matters. These evaluations would be useful in determining the preparedness level of individual workers as well as the agency as a whole. Also, testing certain security measures may require covert testing using fake threat material. Developing methods to conduct this type of testing will enable agencies to determine the robustness of their security systems and preparedness of their workforce. Individual weaknesses can be addressed by providing remedial training to those who require it. Universal weaknesses can be addressed by changing or adding to the training content or the security system and practice.

Cross-Functional Training

As the transportation security community takes on an all-hazards approach, and to ensure the success of convergence efforts, cooperation among multiple functions and divisions within the transit agency is needed, including the police force or security unit, IT, human resources, operations planning, customer service, marketing, and others. There is, therefore, a foreseeable need for communications and cross-functional experience and training for transit employees in these areas.

Simulation

This alternative training and evaluation tool provides a realistic but safe three-dimensional virtual reality setting in which employees may be trained and assessed. Simulation is used in military settings to train military personnel and has been considered for use by a few transit agencies as a training tool.

Motivation

To address the issue of both officer and transit employee motivation with regards to both crime and terrorism, further research on transit police and employee motivation techniques is recommended.

Resource Allocation and Deployment

Resource allocation and deployment decisions for security investments and their justification are challenging for some agencies. Transit agency management, planners, and police and security departments look to determine the optimal number of security personnel, deployment locations, and schedules, as well as the best mix of labor and technology for their particular agency. Even though models may exist, the appropriate use of the resource allocation models and application to an agency's long-term and near-term investment strategy may not be known.

Transit Vehicle Design

Further research and collaboration with transit vehicle manufacturers are both required to design security into transit vehicles. Standard buses, for example, do not have compartments with access control for bus drivers; nor do they have access control (e.g., a key) for the vehicles themselves.

Weapons of Mass Destruction Detection Technologies

Whereas the testing of various weapons of mass destruction detection technologies has taken place, continued testing and improvements to these technologies are required before they can be made available to transit agencies "off-the-shelf."

Cyber Security

Cyber attacks can affect communications systems, Intelligent Transportation Systems technologies such as train control systems, or Automatic Vehicle Location systems and signal systems, and these attacks may compromise sensitive data. Although relatively few incidents of cyber crime have been reported by transit agencies, cyber crime in general has been on the rise. Large amounts of personal data of government employees and the general public have already been stolen and used by identity thieves or otherwise compromised. The more alarming aspect of this trend is that many government agencies have been targeted by cyber criminals; in June 2007, the Pentagon was a victim of hacking and sensitive information was compromised. Some speculate that hackers may be financed by foreign governments, entities, and/or terrorist organizations. Therefore, more research may be needed in cyber security issues.

Other Research Needs

Biometric Systems

As the transportation worker identification card (TWIC) program progresses, transit agencies will need to incorporate biometric technologies into their identity management efforts. Additional research into how transit agencies will be able to accommodate biometric technology and integrate their identity management with the TWIC program may be needed.

Graffiti

This fundamental quality-of-life issue from the passenger's perspective raises the question, that, if transit agencies cannot secure transit systems from vandals, how can they secure these systems from terrorists? The cost to remove graffiti for transit agencies is in the millions. Graffiti has been addressed successfully in some transit systems, but the problem remains or has reappeared in others.

Revenue Security

Because employee theft is a continuing problem for transit agencies, research into antitheft measures for transit workers may be of interest to transit agencies.

Significant progress has been made by transit agencies in transit security and counterterrorism since September 11, 2001. However, this progress needs to continue to ensure that transit systems are at a maximal level of preparedness and to counter the continued persistence and desire of terrorists to inflict harm on innocent persons and their proclivity to choose transit systems as targets. Transit agencies should renew their focus on ordinary crime and minor offenses to prevent a backslide in the remarkable improvement in crime reduction that has occurred.

ABBREVIATIONS AND ACRONYMS

ADA	Americans with Disabilities Act	HVAC	Heating, ventilation, and air conditioning
AFSD	Assistant Federal Security Director	IAs	Immediate actions
AVL	Automatic Vehicle Location	ICS	Incident command system
BART	Bay Area Rapid Transit District (San Francisco)	IDEA	Innovations Deserving Exploratory Analysis
BASE	Baseline Assessment for Security Enhancement	IED	Improvised explosives device
BJS	Bureau of Justice Statistics	IP	Internet Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear, or Explosive	IT	Information technology
CCTV	Closed-circuit television	JHU	Johns Hopkins University
CDTA	Capital District Transportation Authority	JTTF	Joint Terrorism Task Force
CERT	Community Emergency Response Team	MARTA	Metropolitan Atlanta Rapid Transit Authority
COG	Council of Governments	MBTA	Massachusetts Bay Transportation Authority
COOP	Continuity of Operations	MOU	Memorandum of Understanding
CPR	cardiopulmonary resuscitation	MTA	Metropolitan Transportation Authority
CPTED	Crime Prevention Through Environmental Design	MTPD	Metro Transit Police Department
CTA	Chicago Transit Authority	Muni	San Francisco Municipal Railway
DHS	Department of Homeland Security	NBC	Nuclear/Biological/Chemical
DHS/S&T	DHS Science and Technology Directorate	NCTC	National Counterterrorism Center
DMZ	Demilitarized zone	NEDCTP	National Explosives Detection Canine Team Program
DOT	Department of transportation	NFTA	Niagara Frontier Transportation Authority
EOC	Emergency operations center	NIMS	National incident management system
EOP	Emergency operating procedure	NIPP	National Infrastructure Protection Plan
ETD	Explosives trace detection	NJT	New Jersey Transit
FAMSAC	Federal Air Marshals Special Agent in Charge	NRP	National Response Plan
FBI	Federal Bureau of Investigation	NTD	National Transit Database
FEMA	Federal Emergency Management Agency	NTI	National Transit Institute
FOIA	Freedom of Information Act	NYCT	New York City Transit
FRAWG	Federal Risk Assessment Working Group	OCC	Operations control center
GIS	Geographic information system	OGT	Office of Grants and Training
HAZMAT	Hazardous materials	PATH	Port Authority Trans–Hudson Corporation
HSIN	Homeland Security Information Network	PC	Personal computer
HSIN-PT	Homeland Security Information Network—Public Transit		
HSAS	Homeland Security Advisory System		

PCAC	Permanent Citizens Advisory Committee	TAG	Together Against Graffiti
PIV	Personal Identity Verification	TCO	Total cost of ownership
POST	Peace Officers Standards and Training	TOMs	Train Order Maintenance Sweeps
PSI	Passenger security inspection	TSNM	Transportation Sector Network Management
ROW	Right-of-way	TS-SSP	Transportation Systems–Sector Security Plan
SCP	Situational Crime Prevention	TVA	Threat and Vulnerability Analysis
SEMTAP	Security and Emergency Management Technical Assistance Program	TWIC	Transportation worker identification card
SEPTA	Southeastern Pennsylvania Transportation Authority	UCR	Uniform Crime Reporting
SOP	Standard operating procedure	UHF	Ultrahigh frequency
SOT	Special operations team	VIPR	Visible Intermodal Prevention and Response
STISAC	Surface Transportation–Information Sharing and Analysis Center	WMD	Weapons of mass destruction
SWAT	Special Weapons and Tactics	WTC	World Trade Center

REFERENCES

- Bacal, R., *Defusing Hostile Customers Workbook*, Institute for Cooperative Communication, Winnipeg, Canada, 1998.
- Bahr, N., E. Gorrie, and M. Zannoni, *Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies*, FTA Report No. DOT-VNTSC-FTA-07-01, Federal Transit Administration, Washington, D.C., 2007.
- Batelle, TotalSecurity US, and Transportation Research Associates, *Transit Agency Security and Emergency Management Protective Measures*, Federal Transit Administration, Washington, D.C., 2006.
- Blumenthal, L., "Intelligence Suggests Terrorists Conduct Surveillance on Ferries," *HeraldToday.com*, Sep. 9, 2006.
- Blumstein, A. and J. Wallman, eds., *The Crime Drop in America*, Cambridge University Press, Cambridge, U.K., 2000.
- "Cameras on Buses and Shuttles Can Reap Rewards," *Parking Today*, Vol. 7, No. 9, 2002, p. 16.
- Campbell, G., "Demonstrate Security's Alignment with Business Objectives," *Security Technology & Design*, Feb. 2008.
- Campbell, G.K., *Measures and Metrics in Corporate Security*, Senior Executive Council, 2006.
- Center for Domestic Preparedness, Fact Sheet, Department of Homeland Security, Anniston, Ala., 2008 [Online]. Available: <https://cdp.dhs.gov/>.
- Clarke, R.V., ed., *Situational Crime Prevention: Successful Case Studies*, 2nd ed., Harrow and Heston, New York, 1997.
- CNN (Cable News Network), "FBI: Three Held in New York Tunnel Plot," July 7, 2006 [Online]. Available: <http://www.CNN.com>.
- Conklin, J., *Why Crime Rates Fell*, Pearson Education, Inc., New York, 2003.
- Conry-Murray, A., "On Location: Chicago Transit Authority," Mar. 19, 2007 [Online]. Available: <http://www.networkcomputing.com> [accessed Jan. 23, 2007].
- Criminal Victimization in the United States, 1996–2005 Statistical Tables*, U.S. Department of Justice, Washington D.C.
- CDTA Budget FY2008*, Capital District Transportation Authority, Albany, New York, 2007.
- "Evaluation of DHS' Information Security Program for Fiscal Year 2007," Office of the Inspector General, Department of Homeland Security, Washington, D.C., 2007.
- "Existing and Potential Standoff Explosives Detection Techniques." Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, Board on Chemical Sciences and Technology, National Research Council, Washington, D.C., 2004.
- Felson, M., et al., "Redesigning Hell: Preventing Crime and Disorder at the Port Authority," In *Preventing Mass Transit Crime*, R. Clarke, ed., Crime Prevention Series, Vol. 6., Criminal Justice Press, Monsey, N.Y., 1996, pp. 5–92.
- Frank, T., "TSA to Test New Thermal Cameras in Rail Stations," *USA Today*, Oct. 4, 2007.
- Gomersall, C., "Challenges and Developments in Intelligent Video Surveillance," Commentary, SourceSecurity.com [Online]. Available: <http://sourcesecurity.com>, n.d..
- Goodfellow, R., "Lighting as a Situational Approach to Preventing Transit Crime," *Proceedings of the APTA Rail Transit Conference*, Dallas, Tex., Sep. 26–28, 2005.
- Half of All Violent Crimes and a Third of Property Crimes Were Reported to Law Enforcement Agencies in 2000*, Press Release, Bureau of Justice Statistics, U.S. Department of Justice, Washington, D.C., March 9, 2003.
- Homicide Trends in the U.S., 1976–2005*, Bureau of Justice Statistics, U.S. Department of Justice, Washington, D.C., Multiple Years.
- Hull, G., "Testimony before the House Committee on Appropriations," Subcommittee on Homeland Security, Washington, D.C., Feb. 13, 2007.
- Johnson, K., "Battling Subway Crime, Both Real and Perceived," *The New York Times*, Oct. 2, 1998.
- Judge, T., "Yard Management Gets Smarter," *Railway Age*, Nov. 2007, pp. 33–34.
- Kelling, G. and C. Coles, *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*, Simon and Schuster, New York, 1997a.
- Kelling, G. and C. Coles, "Taking Back the Subway," In *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*, Chapter 4, Simon and Schuster, New York, 1997b.
- Kelling, G. and C. Coles, "Community-Based Crime Prevention," In *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*, Chapter 5, Simon and Schuster, New York, 1997c.

- Kelling, G. and C. Coles, "Fixing Broken Windows," In *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*, Chapter 7, Simon and Schuster, New York, 1997d.
- Kilcarr, S., "NPTC's Petty: Truck Terrorism Threat High," *DriversMag.com*, Aug. 27, 2003 [Online]. Available: <http://driversmag.com/>.
- Layton, L., "Metro to Prepare Riders for Terror," *The Washington Post*, Sep. 2, 2004.
- Leidigh, C., *Fundamental Principles of Network Security*, American Power Conversion Corp., West Kinston, R.I., 2005.
- Lusk, A., *Bus and Bus Stop Designs Related to Perceptions of Crime*, Federal Transit Agency, Washington, D.C., 2001.
- Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Research Council, The National Academies Press, Washington, D.C., 2002.
- "Maryland Transit Deploys Intelligent Video," Arcinc, Nov. 2, 2006 [Online]. Available: <http://www.arcinc.com>.
- MBTA Youth Study Final Report*, MBTA (Massachusetts Bay Transportation Authority), MBTA Police and Northeastern University's Center for Criminal Justice Policy, Boston, Mass., 2000.
- McDonald, P.P., *Managing Police Operations: Implementing the NYPD Crime Control Model Using COMPSTAT*, Wadsworth Publishing, New York, 2001.
- "MTA Announces a State of the Art Integrated Electronic Security System for NY Transportation Network," MTA (Metropolitan Transportation Authority), MTA Press Release, mta.info, Aug. 23, 2005 [Online]. Available at <http://www.mta.info/mta/news/releases/?agency=hq&en=050823> (accessed Jan. 23, 2005).
- Murphy, M.J., *TCRP Synthesis 58: Emergency Response Procedures for Natural Gas Transit Vehicles*, Transportation Research Board, National Research Council, Washington, D.C., 53 pp.
- Nakanishi, Y.J. and J.L. Western, "Ensuring the Security of Transportation Facilities: Evaluation of Advanced Vehicle Identification Technologies," *Transportation Research Record: Journal of the Transportation Research Board*, No. 1938, Transportation Research Board of the National Academies, Washington, D.C., 2005b, pp. 9–16.
- Nakanishi, Y.J. and J.L. Western, "Evaluation of Biometric Technologies for Access Control at Transportation Facilities and Border Crossings," *Transportation Research Record: Journal of the Transportation Research Board*, No. 1938, 1–8. Transportation Research Board of the National Academies, Washington, D.C., 2005a, pp. 1–8.
- Nason, R., "Crash Course in Perimeter Security Technology," *Security Technology & Design*, Feb. 2008, pp. 28–33.
- National Strategy for Combating Terrorism*, The White House, Washington, D.C., 2006 [Online]. Available: www.whitehouse.gov/nsc/nsct/2006.
- National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, National Counterterrorism Center, Office of the Director of National Intelligence, Washington, D.C., 2007.
- Nelson, K.R., "Policing Mass Transit: Serving a Unique Community," Federal Bureau of Investigation, Washington, D.C., Jan. 1997 [Online]. Available at <http://www.mta.com> [accessed Jan. 23, 2005].
- On-Net Surveillance Systems, Inc., Suffern, N.Y., Online presentation [Online]. Available: www.OnSSI.com, n.d.
- Prepare Training Program Manual*, Crisis Prevention Institute, Brookfield, Wis., 2005.
- "Promo and Drill CD-ROM," n.d., WMATA (Washington Metropolitan Area Transit Authority), Obtained from Capt. Brian Heanue, Washington, D.C.
- Radin, S., *Advanced Public Transportation Systems Deployment in the United States—Year 2004 Update*, Federal Transit Administration, Washington, D.C., 2005.
- Reed, T.B., et al., "Transit-Passenger Perceptions of Transit-Related Crime Reduction Measures," *Transportation Research Record: Journal of the Transportation Research Board*, No. 1731, 2000, pp. 130–141.
- "Reporting Crime to the Police," U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C., 1992–2000.
- Royal Canadian Police Departmental Performance Report [Online]. Available: <http://www.tbs-sct.gc.ca/dpr-rmr/2006-2007/inst/rcm/rcm-eng.pdf>.
- Rubenstein, E., *Detection of Radioactivity in Transit Stations*, Transit IDEA Project 42, Transportation Research Board, National Research Council, Washington, D.C., 2006.
- "SafeCom Program," n.d. [Online]. Available: <http://www.safecomprogram.gov>.
- Schweiger, C.L., *TCRP Synthesis 68: Methods of Rider Communication*, Transportation Research Board, National Research Council, Washington, D.C., 2006, 91 pp.
- Science Applications International Corp., "Guide to Risk Management of Multimodal Transportation Infrastructure," NCHRP Project SP20-59(17), Transportation Research Board of the National Academies, Washington, D.C., 2006.

- “Security Manpower Planning Model,” Federal Transit Administration, Washington, D.C., May 2008 [Online]. Available at <http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/SMPM/Default.asp>.
- Staric, J., “Technology is Key Layer to Securing Transit,” *Metro Magazine*, April 2008 [Online]. Available: <http://www.metro-magazine.com>.
- “Supplementary Homicide Reports,” 1976–2005, DOJ and FBI (Department of Justice Report and Federal Bureau of Investigation), Washington, D.C.
- TCRP Report 86, Volume 1: Communication of Threats: A Guide*, Transportation Research Board, National Research Council, Washington, D.C., 2002.
- TCRP Report 86, Volume 4: Intrusion Detection for Public Transportation Facilities Handbook*, Transportation Research Board, National Research Council, Washington, D.C., 2003.
- TCRP Report 86, Volume 8: Continuity of Operations Planning Guidelines for Transportation Agencies*, Transportation Research Board, National Research Council, Washington, D.C., 2005.
- TCRP Report 86, Volume 9: Guidelines for Transportation Emergency Training Exercises*, Transportation Research Board, National Research Council, Washington, D.C., 2006a.
- TCRP Report 86, Volume 10: Hazard and Security Plan Workshop: Instructor Guide*, Transportation Research Board, National Research Council, Washington, D.C., 2006b.
- TCRP Report 86, Volume 11, Security Measures for Ferry Systems*, Transportation Research Board, National Research Council, Washington, D.C., 2006c.
- TCRP Report 86, Volume 12: Making Transportation Tunnels Safe and Secure*, Transportation Research Board, National Research Council, Washington, D.C., 2007a.
- TCRP Report 86, Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers*, Transportation Research Board, National Research Council, Washington, D.C., 2007b.
- TCRP Report 88: A Guidebook for Developing A Transit Performance-Measurement System*, Transportation Research Board, National Research Council, Washington, D.C., 2003.
- “\$34 Million for NYC Metro Area Emergency Communications,” *Government Technology News Report*, April 17, 2008 [Online]. Available: <http://www.gov-tech.com>.
- Transit Security Design Considerations*, FTA (Federal Transit Administration), Washington D.C., 2004.
- “Transportation Sector Network Management Mass Transit Division,” TSA (Transportation Security Administration), Summary of Security Enhancement Efforts, Washington, D.C., May 14, 2008.
- Trends in Victimization Rates by Age, 1973–2005*, Bureau of Justice Statistics, U.S. Department of Justice, Washington, D.C.
- “TSA Expanding National Explosives Detection Canine Teams,” TSA (Transportation Security Administration), 2005. TSA Press Release, Washington, D.C., Sep. 28, 2005.
- “Uniform Crime Reporting,” FBI (Federal Bureau of Investigation), 1976–2005, [Online]. Available: <http://www.fbi.gov/ucr/ucr.htm>.
- Widawsky, I.D., *Passenger Security in the Subways: An Analysis of Crime, Fear, and Perceptions of Insecurity in the New York City Subway System*, A Report by the Permanent Citizens Advisory Committee to the MTA, 1989.
- Workplace Violence Prevention Strategies and Research Needs*, NIOSH (National Institute for Occupational Safety and Health), Publication No. 2006-144, National Institute for Occupational Safety and Health, Washington, D.C., 2006.

BIBLIOGRAPHY

- Acohido, B., "Theft of Personal Data More Than Triples This Year," *USA TODAY*, Dec. 9, 2007 [Online]. Available: http://www.usatoday.com/money/industries/technology/2007-12-09-data-theft_N.htm.
- Airline Passenger Security Screening: New Technologies and Implementation Issues, Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains*, GAO Report 05-457, Washington, D.C., May 2005.
- "Airline Passenger Security Screening: New Technologies and Implementation Issues," Committee on Commercial Aviation Security, National Materials Advisory Board and Commission on Engineering and Technical Systems, National Research Council, Washington, D.C., 1996.
- Assessing and Managing the Terrorism Threat*, U.S. Department of Justice, Bureau of Justice Assistance, Washington, D.C., Sep. 2005.
- "Assessment of Technologies Deployed to Improve Aviation Security: First Report," Commission on Engineering and Technical Systems, Panel on Assessment of Technologies Deployed to Improve Aviation Security, National Research Council, Washington, D.C., 1999.
- Banerjee, B., "The ABCs of TCO (Total Cost of Ownership): The True Costs of IP Video Surveillance," *Video Technology and Applications*, Feb. 2008.
- Beaver, K., "Locking Down Today's Data Centers," *Security Technology & Design*, Dec. 2007, pp. 30–34.
- Bodell, P., "Commentary: Are we Letting the Bad Guys Get Away?" *Video Technology and Applications*, Feb. 2008.
- Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, Board on Chemical Sciences and Technology, National Research Council, Washington, D.C., 2002.
- "Configuration Management and Performance Verification of Explosives-Detection Systems," Commission on Engineering and Technical Systems, National Materials Advisory Board, Panel on Technical Regulation of Explosives-Detection Systems, Publication NMAB-482-3, National Research Council, Washington, D.C., 1998.
- "Containing the Threat from Illegal Bombings: An Integrated National Strategy for Marking, Tagging, Rendering Inert, and Licensing Explosives and Their Precursors," Committee on Marking, Rendering Inert, and Licensing of Explosives, Board on Chemical Sciences and Technology, and Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Washington, D.C., 1998.
- "Cybercriminals Becoming Increasingly Professional," *Government Technology*, Sep. 17, 2007 [Online]. Available: <https://www.govtech.com/>.
- Daniel, M., "MBTA Set to Begin Passenger ID Stops," *Globe*, May 22, 2004.
- "Detection of Explosives for Commercial Aviation Security," Committee on Commercial Aviation Security, National Materials Advisory Board and Commission on Engineering and Technical Systems, National Research Council, Washington, D.C., 1993.
- Effective Employment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail*, Transportation Security Administration, Washington, D.C., 2007.
- "Evaluation of DHS' Information Security Program for Fiscal Year 2007," Department of Homeland Security/Office of the Inspector General, DHS Office of the Inspector General, Washington, D.C.
- "Existing and Potential Standoff Explosives Detection Techniques," Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, Board on Chemical Sciences and Technology, National Research Council, Washington, D.C., 2002.
- "Existing and Potential Standoff Explosives Detection Techniques," Committee on the Review of Existing and Potential Standoff Explosives Detection Techniques, National Research Council, Washington, D.C., 2004.
- "Facts and Statistics," Identity Theft Research Center, April 30, 2007 [Online]. Available: http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics.shtml [accessed Dec. 20, 2007].
- Fatah, A., et al., *An Introduction to Biological Agent Detection Equipment for Emergency First Responders*, NIJ Guide 101-00, National Institute of Justice, Washington, D.C., Dec. 2001.
- Fatah, A., et al., *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders*, NIJ Guide 100-00, National Institute of Justice, Washington, D.C., June 2000.
- FEMA 426—Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Federal Emergency Management Agency, Washington, D.C. updated Oct. 2007.

- FEMA 427—Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*, Federal Emergency Management Agency, 2003.
- “Government Smart Card Interoperability Specification, Version 2.1T,” National Institute of Standards and Technology [Online]. Available: <http://csrc.nist.gov/publications/nistir/nistir-6887.pdf>.
- Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, National Institute for Occupational Safety and Health, Washington, D.C., 2002.
- “Guidance on Background Checks, Redress and Immigration Status,” Transportation Security Administration, Washington, D.C., 2007 [Online]. Available: <http://www.tsa.gov/>.
- Haas, K., *Transportation & Homeland Security: A Critical Issues Guide for Local Officials*, Public Technology, Inc., 2005.
- Jenkins M.B., “Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks,” Dec. 1997.
- Kelling, G. and J. Wilson, “Broken Windows,” *Atlantic Monthly*, Mar. 1982.
- King, L., “SEPTA Unveils Antiterror Weapons,” *Inquirer, Employee Security Connection*, Vol. 19, No. 3, Feb. 9, 2006.
- Lawrence Livermore National Laboratory, *Evaluation of an Expedient Terrorist Vehicle Barrier*.
- Lewis, A.J., *Security and Surveillance*, Center for Strategic and International Studies, Washington, D.C., 2002.
- Marisco, R., “PATH Station to Test Bomb-Detection Plan,” *Star-Ledger*, Jan. 25, 2006.
- “Mass Transit Annex to Transportation Systems Sector Security Plan,” Transportation Security Administration, Washington, D.C. [Online]. Available: <http://www.tsa.gov/>.
- “Mass Transit Security Training Program,” Transportation Security Administration, Washington, D.C., 2007 [Online]. Available: <http://www.tsa.gov/>.
- Nakanishi, Y.J. and J.L. Western, “Advancing the State-of-the-Art in Identification and Verification: Biometric and Multibiometric Systems,” In *86th Annual Meeting of the Transportation Research Board* [CD-ROM], Washington, D.C., Jan. 21–25, 2007.
- Nakanishi, Y., K. Kim, Y. Ulusoy, and A. Bata, “Assessing Emergency Preparedness of Transit Agencies: A Focus on Performance Indicators,” In *Transportation Research Record 1822*, Transportation Research Board, National Research Council, Washington, D.C., 2003.
- Needle, J.A. and R.M. Cobb, *Synthesis of Transit Practice 21: Improving Transit Security*, Transportation Research Board, National Research Council, Washington, D.C., 1997, 36 pp.
- NewsEdge Corp., “Profile of Computer Hackers Changing,” *CommwebNews.com*, Dec. 26, 2007.
- O’Neil, D. and Y. Nakanishi, “Survey and Analysis of Transportation Security Training Needs and Programs,” *TR News*, Spring 2005.
- “Opportunities to Improve Airport Passenger Screening with Mass Spectrometry,” Committee on Assessment of Security Technologies for Transportation, National Materials Advisory Board, National Research Council, Washington, D.C., 2004.
- “Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT),” National Nuclear Security Administration, National Institute of Standards and Technology.
- Pryor, R., “TSA Trip I, II, III Tests Presentation Slides,” CTO Operational Integration Division/TSA.
- Public Transportation System Security and Emergency Preparedness Planning Guide*, Federal Transit Administration, Washington, D.C., 2003.
- Railway Age*, Nov. 2007.
- Rhykerd C., D. Hannum, D. Murray, and J. Parmeter, *Guide for the Selection of Commercial Explosives Detection Systems for Law Enforcement Applications*, NIJ Guide 100-99, National Institute of Justice, Washington, D.C., Sep. 1999.
- “Security and Emergency Management Action Items,” Federal Transit Administration/Transportation Security Administration, Washington, D.C., 2006 [Online]. Available: <http://www.tsa.gov/>.
- Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies Final Report*, Federal Transit Administration, Washington, D.C., 2007.
- Silverman, E., *NYPD Battles Crime: Innovative Strategies in Policing*, Northeastern University Press, Boston, Mass., 2001.
- Smiths Detection and TeraView Developing Hand-Held Screening Device, *Flt Tech Online Weekly News Summary*, June 17, 2004.
- Special Report 270: Deterrence, Protection, and Preparation: The New Transportation Security Imperative*, Transportation Research Board, Washington, D.C., 2002.
- Survey of United States Transit System Security Needs and Funding Priorities, “Summary of Findings,” American Public Transportation Association, Washington, D.C., 2004.

- Taylor, B., et al., "Responding to Security Threats in the Post-9/11 Era: A Portrait of U.S. Urban Public Transit," *Public Works Management & Policy*, Vol. 11, No. 1, pp. 3–17.
- TCRP Project J-3: International Transit Studies Program*, Transportation Research Board, National Research Council, Washington, D.C., June 2003.
- TCRP Report 86, Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers*, Transportation Research Board, National Research Council, Washington, D.C., 2002.
- TCRP Report 86, Volume 3: Robotic Devices for the Transit Environment*, Transportation Research Board, National Research Council, Washington, D.C., 2003.
- TCRP Report 86, Volume 5: Security-Related Customer Communications and Training for Public Transportation Providers*, Transportation Research Board, National Research Council, Washington, D.C., 2004.
- TCRP Report 86, Volume 6: Applicability of Portable Explosive Detection Devices in Transit Environments*, Transportation Research Board, National Research Council, Washington, D.C., 2004.
- TCRP Report 86, Volume 7: Public Transportation Emergency Mobilization and Emergency Operations Guide*, Transportation Research Board, National Research Council, Washington, D.C., 2005.
- TCRP Web Document 15: Guidelines for the Effective Use of Uniformed Transit Police and Security Personnel*, Transportation Research Board, National Research Council, Washington, D.C., May 1997.
- TCRP Web Document 18: Developing Useful Transit-Related Crime and Incident Data*, Transportation Research Board, National Research Council, Washington, D.C., April, 2000.
- "Title 33: Navigation and Navigable Waters, Part 104-Vessel Security. Electronic Code of Federal Regulations" [Online]. Available: <http://www.mxak.org/regulations/homeland/33cfr104.htm>.
- "Transit Security Grant Program Guidelines," Department of Homeland Security/Transportation Security Administration, Washington, D.C. [Online]. Available: <http://www.tsa.gov/>.
- Transit Security Handbook*, Federal Transit Administration, Report No. FTA-MA-90-9007-98-1, U.S. Department of Transportation, Washington, D.C., 1998.
- "Transit Threat Level Response Recommendation," Federal Transit Administration, Washington, D.C.
- Transit Tunnel Recommended Protective Measures*, Transportation Security Administration, Washington, D.C., 2007.
- "Transportation Security: Post-September 11th Initiatives and Long-Term Challenges," Report No. GAO-03-616, [Online]. Available: <http://www.gao.gov/new.items/d03616t.pdf>.
- "TSA Expanding National Explosives Detection Canine Teams to Mass Transit and Commuter Rail Systems," Department of Homeland Security, DHS press release, Washington, D.C., Oct. 6, 2005.
- "TSA Unveils Mobile Security Checkpoint Pilot Program with Maryland Transit Authority," Department of Homeland Security, DHS press release, Washington, D.C. April 3, 2006.
- "Vandalism, Terrorism, and Security in Urban Public Passenger Transport," *Report of the Hundred and Twenty Third Round Table on Transport Economics*, European Conference of Ministers of Transport, 2003.
- Verrinder, M., "N.J. Starts Bomb-Screening of Train Riders," *Associated Press*, Feb. 8, 2006.
- Washington State Ferry, [Online]. Available: <http://www.wsdot.wa.gov/ferries/security>.
- Weber, S., "Cyber Security: Ignore At Your Peril," *Forbes.com*, Feb. 28, 2008.
- Williams, T. and S. Chan, "In New Security Move, New York Police to Search Commuters' Bags," *NY Times*, July 21, 2005.
- Workplace Violence Prevention Strategies and Research Needs*, National Institute for Occupational Safety and Health, NIOSH Publication No. 2006-144, Washington, D.C., Sep. 2006.

GLOSSARY

TRANSIT SECURITY TERMS

Source: Transit security glossary definitions are primarily derived from *Transit Safety & Security Statistics & Analysis 2003 Annual Report*; *National Infrastructure Protection Plan* (July 2006) or the *National Response Plan* (December 2004).

All Hazards

An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

Arson

To unlawfully and intentionally damage, or attempt to damage, any real or personal property by fire or incendiary device.

Assault, Aggravated

An unlawful attack by one person upon another wherein the offender—

- Uses a weapon in a threatening manner, or
- Victim suffers obvious severe or aggravated bodily injury.

Assault, Other

An unlawful attack or attempt by one person upon another in which no weapon was used or that did not result in serious or aggravated injury to the victim. This includes—

- Simple assault
- Minor assault
- Assault and battery
- Injury by culpable negligence
- Intimidation, coercion, hazing
- All attempts to commit these offenses

Attack or Active Incident

An actual emergency that might include a terrorist attack, accident, or natural disaster.

Bomb Threat

Credible written or oral (e.g., telephone) communication to a transit agency threatening the use of an explosive or

incendiary device for the purpose of disrupting public transit services or to create a public emergency.

Bombing

The unlawful and intentional delivery, placement, discharge, or detonation of an explosive or other lethal device.

Burglary

The unlawful entry into a building or other structure with the intent to commit a felony or a theft. This includes offenses known locally as burglary (any degree), unlawful entry with intent to commit a larceny or felony, breaking and entering with intent to commit a larceny, housebreaking, safe cracking, and all attempts at these offenses.

Chemical, Biological, or Nuclear Release

The unlawful and intentional delivery, placement, discharge, or detonation of a biological, chemical, or nuclear lethal device.

Crime Prevention Through Environmental Design (CPTED)

CPTED is a method of situational crime prevention by which the transit environment discourages offenders from making the choice to commit a crime by increasing the risks and required efforts. The many CPTED measures include bright lighting, unobstructed sightlines, and natural and formal surveillance.

Criminal Activity

An activity that violates the law.

Cyber Incident

Involves the targeting of transit facilities, personnel, information, computer, or telecommunications systems associated with transit agencies.

Proscribed activities include the following:

- Denial or disruption of computer or telecommunications services, especially train control systems;
- Unauthorized monitoring of computer or telecommunications systems;
- Unauthorized disclosure of proprietary or classified information store within or communicated through computer or telecommunications systems;

- Unauthorized modification or destruction of computer programming codes, computer network databases, stored information or computer capabilities; and
- Manipulation of computer or telecommunications services resulting from fraud, financial loss, or other criminal violations.

Derailment/Bus Going Off Road

A noncollision incident in which either one or more wheels of a transit vehicle unintentionally leaves the rails, a bus leaves the roadway, or there is a rollover.

Detection

The identification and validation of potential threat or attack that is communicated to an appropriate authority that can act. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, alarms, surveillance, and employee security awareness programs.

Deterrence

An activity, procedure, or physical barrier that reduces the likelihood of an incident, attack, or criminal activity.

Directly Operated

Transportation service provided directly by a transit agency, using their employees to supply the necessary labor to operate the revenue vehicles. This includes instances in which an agency's employees provide purchased transportation services to the agency through a contractual agreement.

Emergency Incident

An incident in which emergency response is required; specifically, an imminent threat to human life.

Employee

An individual who is compensated by the transit agency as follows:

- For directly operated services, the labor expense for the individual is reported in object class 501 labor.
- For purchased transportation service, the labor expense for the individual meets the same criteria as object class 501 labor.

Evacuation

A condition requiring all passengers and employees to depart a transit vehicle and enter onto the transit right-of-way or roadway under emergency circumstances.

Fare Evasion

The unlawful use of transit facilities by riding without paying the applicable fare.

Fatality

A transit-caused death confirmed within 30 days of a transit incident, which occurs under the collision, derailment, fire, evacuation, security incident, vehicle leaving the roadway, or not otherwise classified categories.

Fire

Uncontrolled combustion made evident by flame and/or smoke that requires suppression by equipment or personnel.

Forcible Rape

The carnal knowledge of a person forcibly and/or against that person's will. This includes assault to rape or attempt to rape.

FTA Urbanized Area Formula Program Funds

Financial assistance from Section 5307 of the Federal Transit Act. This program makes federal resources available to finance capital projects and the planning and improvement costs of equipment, facilities, and associated capital maintenance items for use in mass transportation. The program also allows funds for operating assistance in urbanized areas of less than 200,000 population.

Grade Crossings

An intersection of highway roads, railroad tracks, or dedicated transit rail tracks that run either parallel or across mixed traffic situations with motor vehicles, light rail, commuter rail, heavy rail, trolley bus, or pedestrian traffic. Collisions at grade crossings involving transit vehicles apply to light rail, commuter rail, heavy rail, or trolley bus.

Graduated Security Response

A security response that increases in a modular or continuous fashion as the defined threat level increases in severity; protective measures implemented at lower threat levels build to the higher threat level protective measures in a cumulative fashion.

High-Visibility Patrols

High-visibility patrols are made highly visible through the saturation of specific locations with multiple specially uniformed officers and the use of visible tactical vests.

Hijacking

Seizing control of a transit vehicle by force.

Homicide

The killing of one or more human beings by another, including the following:

- Murder and nonnegligent manslaughter: The willful (nonnegligent) killing of one or more human beings by another.
- Negligent manslaughter: The killing of another person or persons through gross negligence.

Incident

Major (episodic): Existence of one or more of the following:

- A fatality other than a suicide.
- Injuries requiring immediate medical attention away from the scene for two or more persons.
- Property damage equal to or exceeding \$25,000.
- An evacuation as a result of life safety reasons.
- A collision at a grade crossing resulting in at least one injury requiring immediate medical attention away from the scene or property damage equal to or exceeding \$7,500.
- A mainline derailment.
- A collision with person(s) on a rail right-of-way resulting in injuries that require immediate medical attention away from the scene for one or more persons.
- A collision between a rail transit vehicle and another rail transit vehicle or a transit nonrevenue vehicle resulting in injuries that require immediate medical attention away from the scene for one or more persons.

Nonmajor (summary): Incidents not already reported on the Major Incident Reporting form (S&S-40) with one or more of the following conditions:

- Injuries requiring immediate medical attention away from the scene for one person.
- Property damage equal to or exceeding \$7,500 (less than \$25,000).
- All nonarson fires not qualifying as major incidents.

Injury

Any physical damage or harm to persons as a result of an incident that requires immediate medical attention away from the scene.

Larceny/Theft

The unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another person. This includes pocket picking, purse

snatching, shoplifting, thefts from motor vehicles, thefts of motor vehicle parts and accessories, theft of bicycles, theft from buildings, theft from coin-operated devices or machines, and all other theft not specifically classified.

Mitigation

Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

Mode

A system for carrying transit passengers described by specific right-of-way, technology, and operational features.

Motor Vehicle Theft

Theft or attempted theft of a motor vehicle. A motor vehicle is a self-propelled vehicle that runs on the surface of land and not on rails.

National Transit Database (NTD)

The system through which the FTA collects uniform data needed by the secretary of transportation to administer department programs.

Not Otherwise Classified (personal casualty)

A major or nonmajor incident in which persons are injured or die in transit-related operations, but not as a result of a collision, derailment/vehicle leaving roadway, evacuation, or fire. These incidents can include the following:

- Injuries or fatalities that occur in slips, trips or falls on stairs, escalators, elevators, passageways, platforms, or transit rights-of-way.
- Injuries or fatalities that occur in sudden braking or unexpected swerving on transit vehicles.
- Injuries or fatalities that occur in slips, falls, door closings, or lifts while getting on or off a transit vehicle.

Nonarson Fires

An incident involving uncontrolled combustion manifested by flame or smoke resulting in evidence of charring, melting, or other evidence of ignition of transit property. These are reported as in station, on right-of-way or other, or in a vehicle.

Nonviolent Civil Disturbance

Nonviolent public demonstrations that may or may not be disruptive.

Other

An individual who is neither a transit passenger, transit facility occupant, employee/other worker at a transit agency, or a trespasser.

Other Assault

An unlawful attack or attempt by one person upon another in which no weapon was used or that did not result in serious or aggravated injury to the victim.

Passenger

A person who is onboard, boarding, or alighting from a transit vehicle for the purpose of traveling without participating in the operation of the vehicle.

Passenger Miles

The cumulative sum of distances ridden by each passenger.

Population Density

Population divided by the area for which the population was measured. In the NTD, the number of people is the most recent census urbanized area population divided by the square miles of that urbanized area.

Property Damage

The dollar amount required to repair or replace all vehicles (transit and nontransit) and all property/facilities (track, signals, and buildings) damaged during an incident to a state equivalent to that which existed before the incident.

Protective Measures

Planned activities that reduce vulnerability, deny an adversary opportunity, or increase response capability during a period of heightened alert.

Purchased Transportation

Transportation service provided to a public transit agency or government unit from a public or private transportation provider based on a written contract. The provider is obligated in advance to operate public transportation services for a public transit agency or governmental unit for a specific monetary consideration, using its own employees to operate revenue vehicles. Purchased transportation does not include franchising, licensing operations, management services, cooperative agreements, or private conventional bus service.

Recovery

The development, coordination, and execution of service- and site-restoration plans for affected areas and operations.

Response

Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.

Risk

A measure of potential harm that encompasses threat, vulnerability, and consequence.

Robbery

The taking or attempting to take anything of value under confrontational circumstances from the care, custody, or control of another person by force or threat of force or violence and/or by putting the victim in fear of immediate harm. The use or threat of force includes firearms, knives or cutting instruments, other dangerous weapons (clubs, acid, explosives), and strong-arm techniques (hands, fists, feet).

Sabotage

Sabotage or tampering with transit facilities' assets may be a means to achieve any of the above events, such as starting a fire or spreading an airborne chemical agent, or it may be a stand-alone act, such as tampering with track to induce derailment.

Security Vulnerability/Risk Assessment (SVA)

A systematic assessment approach for security vulnerability/risk and includes threat and vulnerability analysis.

Sensitive Security Information (SSI)

Any information or records that the disclosure of the information may compromise safety or security of the traveling public and transit workers. The use of sensitive security information is intended to restrict the material from automatic Freedom of Information Act disclosure.

Situational Crime Prevention (SCP)

The theoretical basis of SCP is rational choice. The offender decides to commit a crime based on risks, efforts, and rewards. SCP attempts to make the risks and efforts

greater than the rewards. The four key categories of SCP techniques as cited by Clarke and Homel are increasing perceived effort, increasing perceived risks, reducing anticipated rewards, and inducing guilt or shame.

Suicide

A person attempting to end his or her own life intentionally. Both successful and unsuccessful attempts are counted as suicides. Suicides were previously classified as a subset of Collisions with People. They have been reclassified as nonmajor security incidents in the redesigned NTD.

Terrorist Attack

An intentional act of violence with intent to inflict significant damage to property, inflict casualties, and produce panic and fear.

Threat

A potential action or situation that may cause harm to people or property.

Transit Facility Occupant

A person who is inside the public passenger area of a transit revenue facility. Employees, other workers, or trespassers are not transit facility occupants.

Trespass

To unlawfully enter land, a dwelling, or other real property.

Unlinked Passenger Trips

The number of passengers who board public transportation vehicles. Passengers are counted each time they board

vehicles no matter how many vehicles they use to travel from their origin to their destination.

Vandalism

The willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without consent of the owner or person having custody or control by cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law.

Vehicles Operated in Annual Maximum Service

The number of revenue vehicles operated to meet the annual maximum service requirement.

Vehicle Miles

The total number of miles traveled by transit vehicles. Commuter rail, heavy rail, and light rail report individual car miles rather than train miles for vehicle miles.

Vulnerability

A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.

Weapons of Mass Destruction (WMD)

Weapons that can cause significant destruction of property and inflict significant numbers of casualties and deaths; typically considered to be a part of the group of weapons called chemical, biological, radiological, nuclear, or explosive weapons.

CYBER SECURITY TERMS

Source: These cyber security terms are from National Cyber Security Alliance Glossary (<http://staysafeonline.org/basics/glossary.html>).

Adware	Any software application that displays advertising banners while the program is running. The authors include additional code, which can be viewed through pop-up windows or through a bar that appears on the computer screen. Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge.
Alert	Notification that a specific attack has been directed at the information system of an organization.
Attack	Intentional act of attempting to bypass one or more computer security controls.
Audit Trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.
Authenticate	To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. Also see Two Factor Authentication.
Back Door	Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.
Backup	A copy of data and/or applications contained in the information technology (IT) stored on magnetic media outside of the IT to be used in the event IT data are lost.
Blended Threat	A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods, for example, using characteristics of both viruses and worms, while also taking advantage of vulnerabilities in computers, networks, or other physical systems. An attack using a blended approach might send a virus via an e-mail attachment, along with a Trojan horse embedded in an HTML file that will cause damage to the recipient computer. The Nimda, CodeRed, and Bugbear exploits were all examples of blended threats.
Bluetooth Technology	Wireless Internet technology.
Bots	Bots are remote-controlled agents installed on your system. Bots are often controlled remotely via Internet Relay Chat. Once a system is infected with a bot, it becomes part of a bot network (botnet) and is used in conjunction with other botnet members to carry out the wishes of the bot owner or bot herder. Bots can scan networks for vulnerabilities, install various Distributed Denial of Service tools, capture network packets, or download and execute arbitrary programs. Often bots will contain additional spyware or install it. Computers or systems infected with bots can be used to distribute spam to make it harder to track and prosecute the spammers.
Broadband	"Broadband" is the general term used to refer to high-speed network connections. In this context, Internet connections via cable modem and Digital Subscriber Line are frequently referred to as broadband Internet connections. "Bandwidth" is the term used to describe the relative speed of a network connection—for example, most current dial-up modems can support a bandwidth of 56 kbps (thousand bits per second). There is no set bandwidth threshold required for a connection to be referred to as "broadband," but it is typical for connections in excess of 1 Megabit per second (Mbps) to be so named.
Browser/Browser Settings	One browser configuration strategy to manage the risk associated with active content while still enabling trusted sites is the use of Internet Explorer security zones. Using security zones, you can choose preset levels of security.
Certification	The comprehensive evaluation of the technical and nontechnical security features of IT and other safeguards, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
Ciphertext	Form of cryptography in which the <i>plaintext</i> is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.

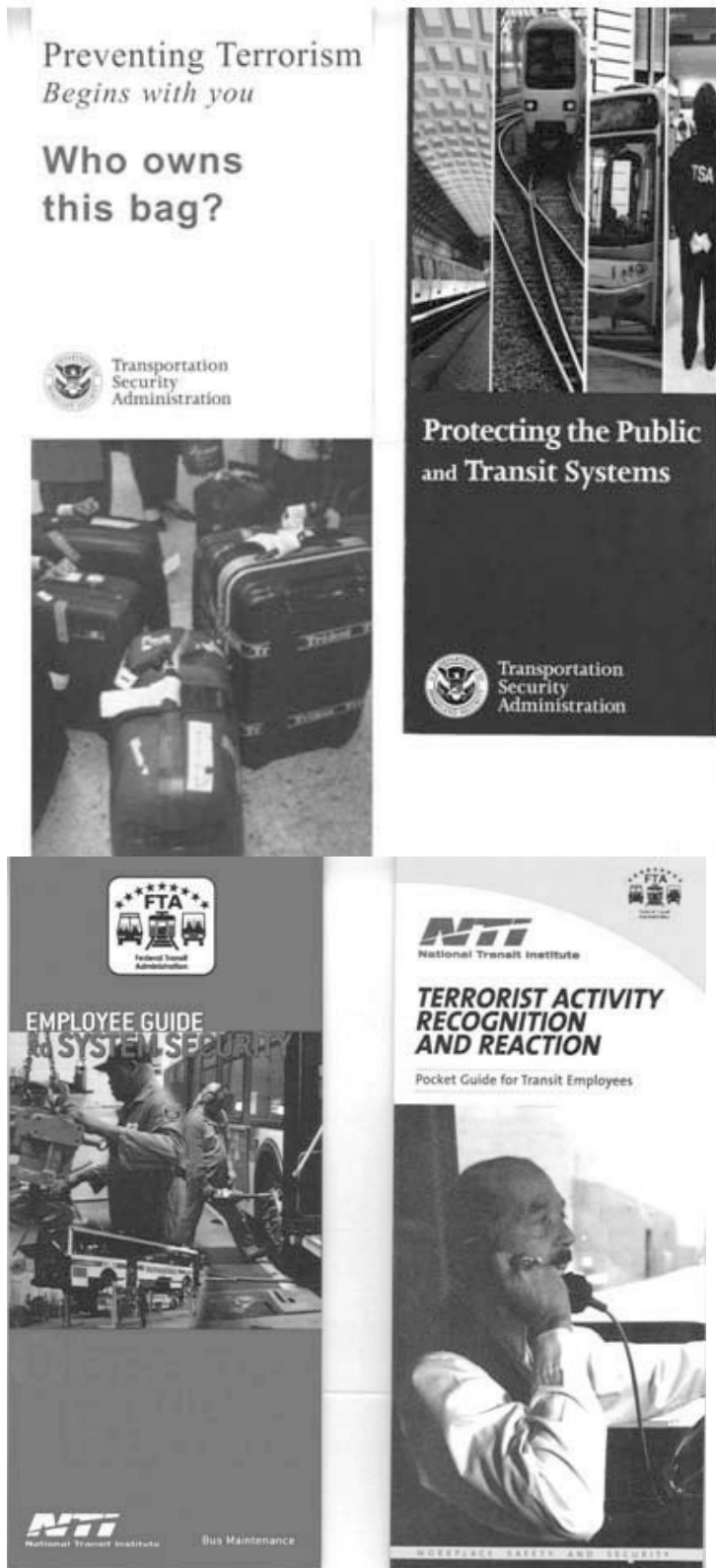
Cookie	Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests (but only once!), and to store shopping lists of items a user has selected while browsing through a virtual shopping mall.
Configuration Management	The process of keeping track of changes to the system, if needed, approving them.
Contingency Plan	A plan for emergency response, backup operations, and postdisaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.
Countermeasures	Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system.
Data-Driven Attack	A form of attack that is encoded in seemingly innocuous data that is executed by a user or a process to implement an attack. A data-driven attack is a concern for firewalls, because it may get through the firewall in data form and launch an attack against a system behind the firewall.
Data Integrity	The state that exists when automated data are the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.
Denial of Service	Result of any action or series of actions that prevents any part of an information system from functioning.
Dial-up Service	The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.
Dictionary Attack	An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.
Digital Signature	Digital signatures are a way to verify that an e-mail message is really from the person who supposedly sent it and that it hasn't been changed. You may have received e-mails that have a block of letters and numbers at the bottom of the message. Although it may look like useless text or some kind of error, this information is actually a digital signature. To generate a signature, a mathematical algorithm is used to combine the information in a key with the information in the message. The result is a random-looking string of letters and numbers.
Distributed Tool	A tool that can be distributed to multiple hosts, which can then be coordinated to anonymously perform an attack on the target host simultaneously after some time delay.
DNS Spoofing	Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.
DSL (Digital Subscriber Line)	Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is only dedicated between your home and the DSL provider's central office—the providers offer little or no guarantee of bandwidth all the way across the Internet.
Encryption	Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.
EULA (End-User License Agreements)	An end-user license agreement (EULA) is a contract between you and the software's vendor or developer. Some software packages state that by simply removing the shrink-wrap on the package, you agree to the contract. However, you may be more familiar with the type of EULA that is presented as a dialog box that appears the first time you open the software. It usually requires you to accept the conditions of the contract before you can proceed.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Flooding	Type of incident involving insertion of a large volume of data resulting in denial of service.
Gateway	A bridge between two networks.
Hacker	Unauthorized user who attempts to or gains access to an information system.
IM (Instant Messaging)	Text message-based communications.
Internet	A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.
Intranet	A network based on TCP/IP protocols (an Internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's websites look and act just like any other websites, but the firewall surrounding an intranet fends off unauthorized access.
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.
ISP	Internet Service Provider.
Malicious Code	Software capable of performing an unauthorized process on an information system.
Management Controls	Security methods that focus on the management of the computer security system and the management of risk for a system.
Mobile Code	Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Malicious mobile code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources.
Operation Controls	Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Filtering	A feature incorporated into routers to limit the flow of information based on predetermined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol-specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network.
Patches (Software Patches)	Updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. Make sure to apply relevant patches to your computer as soon as possible so that your system is protected. Also see Software Assurance.
Pharming	Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial-related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof websites that appear legitimate, pharming "poisons" a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however, will show you are at the correct website, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail, while pharming allows the scammers to target large groups of people at one time through domain spoofing.
Phishing	Phishing attacks use e-mail or malicious websites to solicit personal, often financial, information. Attackers may send e-mail seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.
Probe	An attempt to gather information about an information system for the apparent purpose of circumventing its security controls.
Proxy	Software agent that performs a function or operation on behalf of another application or system while hiding the details involved.
RADIUS	Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Remote Access	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information.
Replicator	Any program that acts to produce copies of itself. Examples include a program, a worm, or virus.
Retro-virus	A retro-virus is a virus that waits until all possible backup media are infected, too, so that it is not possible to restore the system to an uninfected state.
Risk Analysis	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.
Risk Management	Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.
Rootkit	A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.
Security Incident	An adverse event in a computer system or the threat of such an event occurring.
Security Plan	Document that details the security controls established and planned for a particular system.
Security Specifications	A detailed description of the safeguards required to protect a system.
Sensitive Data	Any information that the loss, misuse, modification of, or unauthorized access to could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.
Smart Card	A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Smurfing	Software that mounts a denial of service attack by exploiting IP broadcast addressing and ICMP (Internet control message protocol) ping packets to cause flooding.
Spam	To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. Electronic “junk mail.” Spam can contain worms, viruses, and other malicious code.
Spim	Spam that is sent over Instant Messaging. Like spam, spim can contain worms, viruses, and other malicious code.
Spoofing	Unauthorized use of legitimate identification and authentication data, however it was obtained, to mimic a subject different from the attacker. Impersonating, masquerading, piggy-backing, and mimicking are forms of spoofing.
Spyware	Any software using someone’s Internet connection in the background without their knowledge or explicit permission. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
Threat	Any circumstance or event with the potential to adversely affect an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Trojan Horse	A malicious or harmful code contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.
Virus	Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.
VOIP	Voice over Internet Protocol.

Vulnerability	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, and so on that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.
Web Bugs	Web bugs are HTML elements, often in the form of image tags that retrieve information from a remote website. While the image may not be visible to the user, the act of making the request can provide information about the user. Web bugs are often embedded in web pages or HTML-enabled e-mail messages.
Worm	Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

APPENDIX A SUPPORTING MATERIAL



**IF YOU SEE SOMETHING,
SAY SOMETHING.**

CALL 1-888-NYC-SAFE

You may notice more MTA police officers at stations and on your trains during daytime and evening hours. This increased uniformed police presence is not because there's a renewed threat to your safety. It is simply part of our counter-terrorism strategy of continued vigilance.

IF YOU SEE SOMETHING, SAY SOMETHING.

www.mta.info  Metropolitan Transportation Authority



PLEASE TAKE YOUR THINGS. OR WE WILL.

Tell a cop, an MTA employee, or call 1-888-NYC-SAFE. No matter where you are in the region. The call is free.

IF YOU SEE SOMETHING, SAY SOMETHING.



SubTalk www.mta.info  **New York City Transit** *Going your way*
George C. Papp
 Chairman, State of New York Paul S. Kadane
 Chairman, MTA

MTA HQR 05 648
 "Security 05 - Robot Things"
 Pennan Square
 27" x 27"
 This advertisement prepared by
ROBERT KAY & PARTNERS

ROBERT KAY & PARTNERS		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Approved	Date
Client	Detail	Client	Detail	Client	Detail	Client	Detail	Client	Detail	Client	Detail	Client	Detail	Client	Detail	Client	Detail	
Order	Detail	Account	Detail	Account	Detail	Account	Detail	Account	Detail	Account	Detail	Account	Detail	Account	Detail	Account	Detail	

On-board Subway

Emergency and Evacuation Instructions

Video Available Online at mta.info

See back page for more information.

 New York City Transit

Evacuation information is available in a video on our website at www.mta.info. Go to the New York City Transit homepage and click on "Safety." A CD-ROM version is also available to community organizations by writing to Safety Video, MTA Community Relations, 347 Madison Avenue, 5th Floor, New York, NY 10017.

IF YOU SEE SOMETHING, SAY SOMETHING.

If you see a suspicious package or activity on the platform or train, don't keep it to yourself.

Tell a cop or an MTA employee.
Or call the toll-free Terrorism Hotline at 1-888-NYC-SAFE no matter where you are in the MTA region.

All ads will be kept on hand for the fire and other emergency staff.

 Metropolitan Transportation Authority

 Metropolitan Transportation Authority
Living smart. Moving better.

Subway Rules

Violating any of these rules can result in arrest, fine, and/or ejection.

You will find a complete listing of MTA New York City Transit subway and bus rules at www.mta.info





mta .ny www.mta.info New York City Transit

APPENDIX B LITERATURE REVIEW

Kelling, G. and C. Coles, *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities*, Simon and Schuster, New York, 1997.

The “broken windows” hypothesis put forth by Wilson and Kelling conceptualized that minor problems in the local environment could promote the committing of major crimes. In the mid-1970s, the state of New Jersey announced a “Safe and Clean Neighborhoods Program,” which was designed to improve the quality of community life in 28 cities. As part of that program, the state provided money to help cities take police officers out of their patrol cars and assign them to walking beats. The governor and other state officials were enthusiastic about using foot patrol as a way of reducing crime, but many police chiefs were skeptical. Foot patrol, in their eyes, had been pretty much discredited. It reduced the mobility of the police, who thus had difficulty responding to citizen calls for service, and it weakened headquarters’ control over patrol officers. Five years after the program started, the Police Foundation, in Washington, D.C., published an evaluation of the foot-patrol project. Based on its analysis of a carefully controlled experiment carried out chiefly in Newark, New Jersey, the foundation concluded, to the surprise of hardly anyone, that foot patrol had not reduced crime rates. But residents of the foot-patrolled neighborhoods seemed to feel more secure than persons in other areas, tended to believe that crime had been reduced, and seemed to take fewer steps to protect themselves from crime (staying at home with the doors locked, for example). Moreover, citizens in the foot-patrolled areas had a more favorable opinion of the police than did those living elsewhere. And officers walking beats had higher morale, greater job satisfaction, and a more favorable attitude toward citizens in their neighborhoods than did officers assigned to patrol cars.

In the chapter on “Taking Back the Subway: NYC’s Quality of Life Program,” the authors write that the order restoration initiatives in New York City (NYC) began in the 1970s—the first one was in Times Square and Bryant Park in the late 1970s to regain control of the park. The initiative had a large community and business involvement and ultimately was successful. In the NYC subway system, NYC Transit’s first major initiative was to target graffiti, which had been a seemingly insurmountable problem in the 1980s. The Clean Car Program was established by the NYC Transit president; the program ensured that graffiti artists would never see their “art” on clean trains. Once a train had been cleaned, any additional graffiti would be cleaned within two hours; otherwise, the train would be taken out of service. By removing the trains from service, it eliminated the ability of the vandals to see the results of their work, which had been one of their major motives, and this discouraged further vandalism of transit property.

However, NYC Transit still faced a considerable amount of lawlessness. When William Bratton arrived at NYC Transit and instituted an order restoration policy, the lack of coordination between the court system and the Transit police produced policing challenges. While transit officers were trying to address minor disorder, advocate groups and the NYS judiciary succeeded in decriminalizing quality-of-life offenses. Despite these challenges, the Transit police continued to enforce the code of conduct, performed fare evasion sweeps, and targeted other minor disorder offenses.

The authors write about the benefits of community policing and describe the ways in which this policing was implemented in NYC and other large cities.

McDonald, P.P., *Managing Police Operations: Implementing the NYPD Crime Control Model Using COMPSTAT*. Wadsworth Publishing, New York, 2001.

Dr. McDonald provides a comprehensive description of CompStat and how it was implemented and operated within NYPD to prevent and address crime problems.

To understand the new challenges being placed on law enforcement and transit police and security personnel, it is necessary to understand the changes that have occurred in the history of law enforcement. In the first half of the twentieth century, law enforcement's main focus was on crime prevention and rapid response to calls for service along with random patrols and reactive investigations. In the late 1960s, however, a presidential report and a few research studies questioned the effectiveness of random patrols in deterring crime, and critics started questioning the effectiveness of policing in general. They spawned a widespread belief in the law enforcement community that crime is caused by social issues, such as poverty and drug use, and that not much could be done to actually control crime rates or to prevent crime. The focus of police departments therefore shifted from serious crime to communities and community policing, and strengthening the role of citizens to maintain order.

CompStat is a Crime Control Model that integrates operations, functions, and resources to combat crime. In the past, the New York Police Department (NYPD) did not have up-to-date crime statistics and a centralized information-sharing mechanism. Also, different units were working separately toward different objectives, often in isolation from other units; crime patterns could not be identified and therefore stymied crime-fighting efforts. The five principles of CompStat were based on “integration, organization and coordination,” which, according to Dr. McDonald, “are far more powerful in crime control than are fragmentation, disorganization, and random activities randomly applied.” These five principles are described below:

1. Specific Objectives—Three to five specific objectives (e.g., robbery) are selected by the chief of police. The objectives are never administrative or “output” objectives, such as increasing the number of beat officers in a particular district or increasing the number of arrests. The objectives are “outcome” objectives, such as “drive drug dealers out of the system,” “curb youth violence,” or “reduce fare evasion.” District commanders would be evaluated against the objectives, but no targets are set to avoid discouragement or complacency.
2. Timely and Accurate Intelligence—Timely and accurate information about when, where, and how crimes are being committed is essential to the CompStat process. The most effective way in which this information could be presented and conveyed to all levels of the policing organization was to map the incidents. As the number of crimes increased in a specific area, “hot spots” and crime patterns were identified, tracked, and addressed. Crime statistics could be broken down into various categories of crime by hour of day and day of the week. Correlations that had not been previously identified (e.g., homicides with drug complaints) were discovered. This crime-mapping method provided a ready-made assessment tool of how well particular strategies were working and how effective commanders were.
3. Effective Strategies and Tactics—The development of a strategy to address a crime hot spot or pattern requires regular meetings with officers at all levels of law enforcement and within the various geographic districts in NYC. The meetings have a single focus—to address crime and public safety, and to hold commanders and officers accountable, using crime intelligence and electronic pin maps. The meetings bring together specialized units, such as patrol, investigations, narcotics, and canine, and foster communication and cooperation among units that traditionally worked in isolation. An example of the strategy development process is provided below.
 - Crime analysis—Comprehensive data collection and analysis lead to the identification of hot spots and crime patterns.
 - Strategy and tactic development—The officers and commanders report regularly to their supervisors, and the impact of interventions are evaluated regularly.
 - Organizational location and applications of support units—Support units function with department-wide objectives and priorities in mind. They are part of problem-solving teams to design strategies for hot spots and fill requests for resources.
 - Role of district commander—The district commander is responsible for the development and implementation of strategies to combat crime for a specific area. The commander organizes teams of officers for strategy development.

- Community policing strategy—Sector sergeants work together to identify and address crime patterns across sectors, and district commanders do the same. Beat officers work with the public within their area to solve problems and obtain information regarding crime patterns in beat, sector, district, or city.
 - Criminal investigations—Criminal investigation commanders work with patrol commanders to analyze hot spots and patterns. Detectives and patrol officers engage in proactive activities to reduce and prevent crime.
 - Disorder and quality of life—Identify causes and symptoms of environmental and behavioral disorders (abandoned cars, loud noises, drug dealing). Government agencies and other entities are contacted to help address these issues. Those exhibiting disorderly conduct are detained or arrested and are then questioned to obtain information about serious crimes.
4. Rapid Deployment of Personnel and Resources—After a strategy has been generated and decided upon, personnel and resources are rapidly deployed. The command meetings facilitate this by involving all stakeholders in the decision-making process. When a particular resource such as a canine unit is devoted to a specific area, any issue to be resolved or negotiations can be addressed at the meeting. Once a decision has been made, it will “stick,” because all of the key personnel were present during the decision-making process.
 5. Relentless Follow-up and Assessment—Continual evaluation and follow-up are not used in traditional police management but were considered crucial to the success of CompStat. Qualitative and quantitative assessment techniques were used to evaluate strategies and tactics. Also, factors such as crime patterns and trends, continued existence of hot spots, continued citizen complaints, suspect identification, change of patterns in calls-for-service, and arrests resulting in prosecutions were considered.
 6. Performance Measures—Key criteria for serious crime are Part I crimes and offenders incarcerated; the key criteria for disorder are citizen calls and complaints, and videos of areas; and the key criteria for fear are citizen surveys and victimization surveys. Success measures used for assessment purposes are outcome oriented; these measures include the following:
 - Number of incidences reduced or prevented
 - Number of crime patterns interrupted
 - Number of hot spots resolved

Dr. McDonald notes that “ultimately, cities should use all these measures—serious crime, disorder, and fear—to take the temperature of public safety.”

7. Data Sources—Data sources include calls for service through 9-1-1, arrests, and other police activities. These data are collected and stored within a police management information system (MIS), which also captures response time to calls for service, time expended to handle a call, and reconciliation of the originating call category. Other data sources that may or may not be automatically funneled into the MIS include information reported by the public through means other than 9-1-1, police officers’ intelligence and field interrogation reports, information from other agencies, prisoner debriefings, informants, private security [e.g., closed-circuit television (CCTV)], and police radios being used by private security, citizen patrols, or auxiliary police.
8. Training—Law enforcement managers will need more training in “(a) the ability to analyze data scientifically; (b) the ability to create, develop, and apply a variety of tactics and strategies; (c) an understanding of theories of command; (d) the ability to coordinate resources of several functional units and other government agencies in concert with elements of the community; (e) skills in tracking, monitoring, adjusting, and evaluating singular and multidimensional crime control activities; and (f) the ability to track and draw important conclusions from trend analysis.”

9. **Recommendations**—Specific recommendations arising out of the model were as follows:
 - a. Maintain detailed records of success and failures of individual tactics and strategies and then analyze them at regular time periods to determine which techniques led to success.
 - b. Acquire the services of an academic researcher to assist either by conducting the long-term trend analysis or short-term tactic-specific evaluations.
 - c. Evaluate overall crime trends within a jurisdiction on an annual, semiannual, or monthly basis. This may be considered a report card to the community and can be used for resource allocation and personnel distribution.
 - d. Accumulate demographic and other data that might provide additional information explaining the dynamics of a crime trend to understand why a problem exists or why it is not yielding to suggested tactics.

10. **Legal Issues**—Legal issues needed to be addressed by both NYC and NYC Transit when they instituted order maintenance policies. For example, in *Young vs. NYCTA*, the court banned enforcement for panhandling. However, the public was on the side of NYC Transit, not on the side of homeless advocates and civil rights groups. The MTA appealed the decision and won.

Establishing Accountability

In traditional policing, commanders are not held accountable for results but rather for personnel and administrative issues. Hence, establishing accountability was a challenge and required a change in their mind-sets that executive management of the NYPD had to enact. Some of the ways in which commanders were encouraged to take responsibility for crime levels, and meetings objectives, and to be held accountable for results were as follows:

- a. Holding one commander to task for a longer period of time by asking probing questions to accelerate the learning curve and underline the criticality of the process.
- b. Initially rewarding minimal successes as a positive reinforcer.
- c. Finding behavioral ways to communicate displeasure with performance without verbally assaulting or insulting the commander.
- d. Working with a commander's subordinates to get the job done, in the event that the commander exhibits initial reluctance to get involved.
- e. Seeing that subordinates become invested in the process, with or without the commander; because this will motivate the commander to become involved as a way to reassert command and control.
- f. Addressing criticism directly to performance or behavior rather than to personal qualities of the individual and speaking in harsh tones without demeaning the individual.
- g. Demonstrating that the jurisdiction is receiving praise for its new actions to convince a commander that if he or she does not participate, promotion or other desirable positions will not be an option.

At the CompStat meetings, officers and staff from disparate units come together to develop strategies and tactics to address crime. Also, representatives from related agencies and organizations were invited to the meetings when needed. In addition, the importance of the meetings is emphasized by never cancelling the meetings except in the case of major disasters and by the presence of senior management at the meetings.

Felson, M., et al., “Redesigning Hell: Preventing Crime and Disorder at the Port Authority,” *Preventing Mass Transit Crime*, ed. R. Clarke, Crime Prevention Series, Vol. 6. Criminal Justice Press, Monsey, N.Y., 1996.

The principles of Crime Prevention through Environmental Design (CPTED) were implemented and have been attributed as contributing to the turnaround of the Port Authority Bus Terminal in New York City, a large and busy bus transit transfer facility with multiple pedestrian circulation levels. In the late 1980s, the passenger terminal was plagued with both major and minor crimes that had escalated to an uncontrollable

level—the major crimes included robbery, pick-pocketing, luggage theft, larceny, and assault. Other problems included transients, homeless persons, drug sales, solicitation for prostitution, and public pay phone abuse.

The planning process to implement crime-prevention design strategies began in the early 1990s. The primary strategy was to diminish disorder and discourage transients by addressing nooks and streamlining pedestrian flows. Obstructions to station access areas were removed, and new lighting, improved signage, a renovated food court, and a redesigned ticket area were implemented. At one of the facility's entrances that had little passenger traffic, illegitimate activity had often taken place. This area was addressed by bringing in a coffee shop that changed the nature of the activity to legitimate. Clear glass replaced existing opaque walls of waiting areas, immediately increasing passenger security, and floors were coated with a special sealer. The seating in waiting areas was replaced with less comfortable flip-down seats to discourage their extended use by transients.

The Port Authority's cleaner appearance helped to attract legitimate users and detract criminals and transients. The restroom areas had been taken over by criminals and transients, and passengers were naturally afraid to use them. Fourteen changes including the addition of corner mirrors, the securing of ceiling panels to make ceiling areas inaccessible to transients, and the addition of attendants were instituted to address this problem.

The Operations Unit was responsible for the smooth flow of both buses and passengers, and, with the assistance of CCTV cameras, identified and addressed any bottlenecks or situations that caused delays. Problems were experienced in both rush hour and nonrush hour periods. Rush hour periods contributed to disorder because of the sheer numbers of passengers passing through the terminal, while nonrush hour periods when travelers were few contributed to danger and fear. The bus gate and adjacent waiting areas were of particular concern because they were located away from the main terminal space. The Operations Unit decided to consolidate activities during off-peak periods (public access was limited to four areas from 10 p.m. to 1 a.m. and to one area from 1 a.m. to 5:30 a.m.) and shut down many of the bus gates and waiting areas during those periods.

Three additional information kiosks were constructed within the terminal. The increased number of information kiosks contributed to a more secure environment by providing information to travelers to help them locate their destinations faster and increasing the number of employees watching the area, thereby decreasing the possibility of pick pocketing or other crimes.

The Port Authority worked with existing retailers to enhance lighting and store configurations and provided strategies to reduce illegitimate activity within their stores. The Port Authority filled unused spaces with additional shops or pushcarts and attempted to attract well-known national and regional chain stores.

All of these design and operational changes contributed to a more secure public space and an increase in customer ratings of the bus terminal. Larceny, robbery, pick pocketing, assaults, criminal mischief, and rape diminished starting in 1991. From 1991 to 1994, a 19-point improvement was seen in customer ratings of personal security. The greatest changes in customer perceptions of security attributes occurred in safety walking through the terminal, safety in the restrooms, police effectiveness, and police visibility. In terms of external attributes, safety in streets around the terminal and safety in subways near the terminal both increased as well. Complaints about the homeless, beggars and panhandlers, drunks, and the use of obscene or threatening language decreased significantly. Actual counts of homeless and other transients in the terminal verified the fact that their numbers had decreased significantly, from 55,100 in 1991 to 11,100 in 1994. An examination of crime in surrounding areas revealed that a decline in crime did occur for Manhattan and New York City as a whole but that the decline was much more significant for the Port Authority bus terminal.

Mentioned in the case study is a list of the 62 specific tactics employed by the Port Authority in the turnaround. They are categorized into the following areas:

- Increase Visibility
- Close Nooks and Improve Natural Supervision
- Improve Flows
- Discourage Loitering and Hustling in Other Ways
- Improve Retailing

Clarke, R., ed., *Preventing Mass Transit Crime*. Crime Prevention Series, Vol. 6. Monsey, NY: Criminal Justice Press, 1996.

Other case studies and topics in the book, in addition to the Port Authority turnaround case study, included WMATA Metro's planning process and how WMATA incorporated many CPTED principles into its subway system: the use of bike patrol in Vancouver's park-and-ride lot to prevent motor vehicle theft; the elimination of payphone toll fraud at the Port Authority; and the implementation of target-hardening strategies at a NYC subway station. The target-hardening case study included information about the following:

- A program to move homeless to shelters
- Improved lighting strategy
- A station manager program
- Fare evasion sweeps
- Passenger code-of-conduct enforcement

Some of these strategies targeted minor offenses and disorder to reduce or prevent more serious crimes.

Blumstein, A. and J. Wallman, eds., *The Crime Drop in America*. Cambridge University Press, Cambridge, England, 2000.

The authors compile a series of articles on the potential causes of the national crime drop, including the use of drugs and the drug trade, guns and gun violence, the prison expansion, and the role of demography. They provide an analysis of the national crime statistics, including the characteristics of perpetrators and their victims, as well as limitations of the data, and they discuss the implications of changes in particular categories of data and reporting rates.

Conklin, J.E., *Why Crime Rates Fell*, Pearson Education, Inc., New York, 2003.

Conklin presents reasons for the decline in the crime rate during the 1990s. He argues that New York's crime rate had started to drop before he became the commissioner, and other large cities also experienced reductions in crime. Conklin believes that the national crime decline was composed of many factors including the following: a result of less reporting of crime to the police, a natural cycle in crime rates, more effective policing, more use of incarceration, changes in the drug trade, changes in the attitudes of youths, reduced access to firearms, changes in the age distribution of the population, improved economic conditions, and increased participation in community organizations.

Nelson, K.R., *Policing Mass Transit: Serving a Unique Community*, FBI, Washington, D.C., Jan. 1997.

Nelson suggested using crime, disorder, and fear along with ridership levels as measures of success for law enforcement efforts. He notes that customer perceptions of danger and fear of crime do affect ridership and this "sets in motion an inevitable cycle of deterioration spurred by the declines in revenues and the migration of potential middle-class and affluent riders to other modes of transportation."

To track crime and disorder, he suggests that each transit police department look at a broad range of activities that affect the quality of the transit experience. He notes that causes of ridership changes are

difficult to determine, but large changes in crime levels accompanied by large decreases in ridership would be worth noting. Rider perceptions are also important—to understand rider perceptions, subjective ridership surveys should be conducted to develop a fear index. Changes in the fear index could be used to determine the success of policing activities.

Nelson describes the importance of having legislative support in prosecuting transit cases, especially repeat offenders. For example, TriMet contracted with the Multnomah County District Attorney's Office to hire a prosecutor specializing in transit crime. State legislatures can give police powers supporting their law enforcement efforts (e.g., allowing officers to expel repeat offenders from the system). Without this support from prosecutors, transit officers will find it difficult to make an impact on transit crime even if many arrests are made.

Nelson also describes the juvenile problem and states that studies have found that passengers find even innocent behavior by juveniles within the transit system somewhat disconcerting and even threatening. These perceptions are enhanced for the elderly, women, and parents with small children. He writes that "youthful exuberance, even without criminal intent, can carry large crowds of young people to extremes." The interactions of rival groups or gangs can cause a potentially volatile situation.

Transportation Security Administration (TSA) Reports and Guidance

Transportation Security Administration (TSA) reports and guidance relevant to transit security can be found on their website at www.tsa.gov and include the following:

Transportation Security Administration, *Mass Transit Annex to Transportation Systems Sector Security Plan* [Online]. Available: <http://www.tsa.gov/>.

Published in June 2007, the existing Mass Transit Annex to Transportation Systems Sector Security Plan (TS-SSP), produced in coordination with Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC), Mass Transit Sector Coordinating Council (SCC), and the Transit Policing and Security Peer Advisory Group (PAG), presents a coordinated security-enhancement strategy for public transportation and passenger rail systems.

In September 2005, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Transportation (U.S.DOT) executed an annex on public transportation to the U.S.DOT/DHS Memorandum of Understanding (MOU) executed September 2004. The annex states the Mass Transit Mode's vision for transit security is as follows:

The Mass Transit Mode's vision is a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers and encouraging the expanded use of the Nation's transit services.

Systems-Based Risk Management (SBRM) methodology drives TSA's overall transportation security initiatives, programs, and exercises to enhance operational capabilities and effectiveness. Randomness and unpredictability, smart application of technological tools, and coordinated training and outreach efforts to stakeholders are emphasized for the Mass Transit Mode. The public-private strategy is guided by the following strategies:

- Apply risk-based analysis in making investment and operational decisions
- Avoid giving terrorists or potential terrorists an advantage based on our predictability
- Intervene early based on intelligence and focus security measures on the terrorist, as well as the means for carrying out the threat
- Build and take advantage of security networks
- Invest in protective measures that would mitigate the impact of potential terrorist actions

TSA is mandated by law to develop policies, strategies, and plans to deal with threats to transportation; assess intelligence and identify threats; coordinate countermeasures; issue, rescind, revise, and enforce

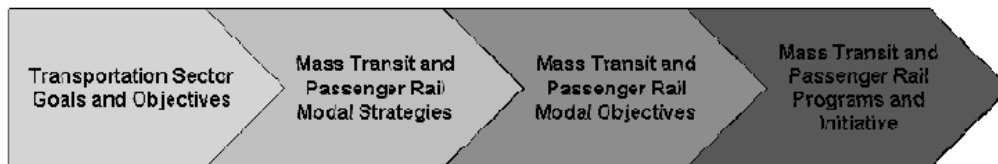
security-related regulations and requirements; and oversee the implementation and ensure the adequacy of security measures. For example, after the attacks on commuter trains in Madrid in March 2004, TSA issued two security directives—SD RAILPAX-04-01 and SD RAILPAX-04-02—to enhance the security of passenger rail and mass transit.

TSA focuses particular attention on the following six Transit Security Fundamentals:

- 1. Protection of high-risk underwater/underground assets and systems.** Because of the consequences of incendiary and explosive device (IED) attacks in an enclosed environment where there may also be large concentrations of riders, protecting riders and the integrity of the transit system against such attacks is essential. Transit agencies should focus countermeasures on programs that can prevent an attack or mitigate the consequences of an incident. Active coordination and regular testing of emergency evacuation plans can also greatly reduce loss of life.
- 2. Protection of other high-risk assets that have been identified through systemwide risk assessments.** It is imperative that transit agencies focus countermeasure resources on their highest-risk, highest-consequence assets. For example, a systemwide assessment may highlight the need to segregate critical security infrastructure from public access. One solution could be an integrated intrusion detection system, controlling access to these critical facilities or equipment. Transit systems should consider security technologies to help reduce the burden on security manpower. For example, using smart CCTV systems in remote locations can help free up security patrols to focus on more high-risk areas.
- 3. Use of visible, unpredictable deterrence.** Visible and unpredictable security patrols have proven to be very successful for instilling confidence and calm in the riding public and, most importantly, in deterring attacks. These kinds of patrols, especially those employing explosives-detection canine teams or mobile-screening or detection equipment, represent effective means to prevent and deter IED attacks. Security patrols should be properly trained in counterterrorism surveillance techniques. An understanding of terrorist behavior patterns helps security patrols more effectively intervene during terrorist surveillance activities or the actual placing of an IED.
- 4. Targeted counterterrorism training for key frontline staff.** Appropriate training enhances detection and prevention capabilities and ensures a rapid, prepared response in the first critical minutes after an attack—steps that can significantly reduce the consequences of the attack. For example, well-trained and rehearsed operators can help ensure that, if an underground station has suffered a chemical agent attack, trains—and the riding public—are quickly removed from the scene, thus reducing their exposure and risk.
- 5. Emergency preparedness drills and exercises.** Experience has taught transit agencies that well-designed and regularly practiced drills and exercises are fundamental to rapid and effective response and recovery. Transit agencies should develop meaningful exercises, including covert testing, that test their response effectiveness and how well they coordinate with first responders. In addition to large regional drills, transit systems should conduct regular, transit-focused drills. Drills should test response and recovery to both natural disasters, as well as, terrorist attacks.
- 6. Public awareness and preparedness campaigns.** Successful security programs in all industries understand the value and power of the public's "eyes and ears." Awareness programs should be well-designed and employ innovative ways to engage the riding public to become part of their "transit security system." Advertisement campaigns, using media and celebrity support have proven to be successful. Including the riding public in preparedness and evacuation drills has been shown to be effective in raising public awareness. A transit agency's awareness campaign should also extend to its employees. Appropriate counterterrorism training, coupled with a strong security awareness campaign, will yield significantly heightened security awareness in transit systems.

The risk to public transit systems is contingent on the type of attack as well as on the form of transportation. While an attack on a bus would be significant in terms of consequences, subway and rail attacks can be more severe in terms of casualties, injuries, and damage, as well as the “enhanced effect of attacks in confined space.” Underwater tunnels are viewed as being even more vulnerable and posing even greater response and recovery challenges.

The following process model is used by the TSA:



Source: Process Model from the Mass Transit Annex, Figure 3-1.

The TSSP goals are (1) preventing and deterring acts of terrorism using or against the U.S. transportation system, (2) enhancing resiliency of the U.S. transportation system, and (3) improving the cost-effective use of resources for transportation security. Mass transit and passenger rail security partners have developed a plan that is aligned with TSSP goals and objectives, and that employs risk-informed decision making to determine specific actions. The plan to enhance security in mass transit and passenger rail is focused on and achieved through the following:

Expanding Partnerships for Security Enhancement

- Regional security collaboration
- Partnerships with state and local law enforcement, fire, emergency medical services
- Coordination with security partners in the region to expand the resources available for employment in random, unpredictable security activities
- Integration of security resources outside the transit agency [local law enforcement patrols, canines, TSA Visible Intermodal Prevention and Response (VIPR) teams] in security-enhancement activities
- Coordination with regional federal officials [Federal Bureau of Investigation (FBI)/ Joint Terrorism Task Force (JTTF), TSA, Surface Transportation Security Inspectors]
- Participation in connecting communities forums (joint FTA/TSA regional security and emergency response seminars)

Continually Advancing the Security Baseline

- Implement continuous improvement process
- Review implementation of security and emergency management plans
- Conduct security assessments and audits—facilitated by TSA surface inspectors, self-assessments, audits by state safety oversight agencies
- Set performance improvement priorities and implementation plans
- Measure progress through continuous improvement process

Building Security Force Multipliers

- Operational deterrence—dedicated antiterrorism teams (large, grant eligible agencies), random and unpredictable security activities
- Employee security training—security awareness, behavior recognition, immediate response to threat/incident
- Exercises and drills—multijurisdictional, cross-functional, system-focused
- Public awareness and preparedness campaigns
- Culture of prevention (terrorism, crime)

Security Information Leadership

- Participation in information sharing and exchange networks (e.g., Homeland Security Information Network, Surface Transportation Information Sharing, and Analysis Center)
- Information sharing with local law enforcement agencies
- Connection to and receipt of products from area FBI/JTTF, State Fusion Center
- Security clearance for security director, general manager
- Public affairs activities pertaining to security program
- Activities to convey deterrent messages

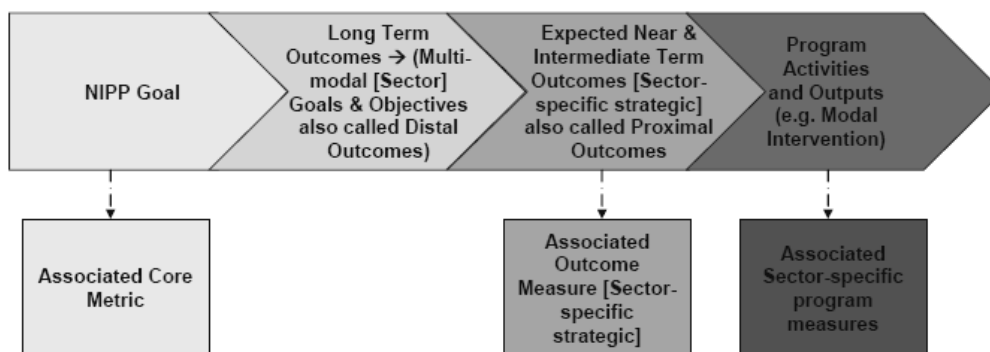
Deploying Tools to Mitigate High-Consequence Risk

- Integration of security activities into employees' daily duties
- Transit Security Grant Program (TSGP) priorities (for eligible agencies)
- Procurement and deployment of security enhancement technologies
- Physical security measures for facilities, such as fencing, lighting, barriers, and locking access gates
- Physical security measures for transit vehicles to prevent unauthorized access when unattended or not in use, including crew or driver areas and storage spaces

Specific programs and the links to Mass Transit objectives and goals are also included in the annex. Information about transit security grants is also provided. The DHS TSGP has provided \$547 million on a risk-based prioritization basis to 60 mass transit and passenger rail systems in 25 states and the District of Columbia.

The importance of performance metrics is noted in the Annex: “Metrics supply the data to affirm that specific goals are being met or to show what corrective actions may be required.” This is the reason that a Measurement Joint Working Group is being formed. The group will operationalize measures; establish data sources, data collection, and verification procedures; set measurement policy for the TSSP; and approve supporting procedures.

Core National Infrastructure Protection Plan (NIPP) metrics are consistent across sectors and measure risk reduction in each sector. Sector-specific strategic metrics also measure the overall effectiveness of mass transit and passenger rail and other modes in meeting TSSP goals and objectives. Sector-specific program measures are aligned with strategic risk objectives for the transportation sector. The Outcomes Monitoring Methodology is presented in figure 3-5 of the annex:



Source: Outcome Model from the Mass Transit Annex, Figure 3-5.

Other TSA resources, many of which may be found on TSA's website, include the following:

- Security and Emergency Management Action Items, FTA/TSA, 2006.
- Guidance on Background Checks, Redress and Immigration Status, TSA, 2007.
- Mass Transit Security Training Program, TSA, 2007.
- TSGP Guidelines, DHS, 2007.
- Effective Employment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail, 2007.
- Transit Tunnel Recommended Protective Measures, TSA, 2007.

FTA Reports and Guidance

The FTA's security website is available through the Volpe Center at <http://transit-safety.volpe.dot.gov/Security/Default.asp>. The website contains information about FTA's security initiatives, Transit Watch program, guidelines and best practices, training tools, and other strategic and research products of interest to transit agencies.



Source: FTA Safety and Security website, <http://transit-safety.volpe.dot.gov/Security/>

Two key reports recently published include the *Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies* and *Transit Agency Security and Emergency Management Protective Measures*.

Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies, Final Report, FTA, Washington, D.C., 2007.

In the FTA's *Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies* project, MOUs were created and signed to ensure agreement upon the handling of security-sensitive information. The Top Security and Emergency Management Technical Assistance Action Items List was created for the following categories:

Management and Accountability

1. Establish written system security programs and emergency management plans
2. Define roles and responsibilities for security and emergency management
3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control
4. Coordinate a security and emergency management plan(s) with local and regional agencies

Security and Emergency Response Training

5. Establish and maintain a security and emergency training program

Homeland Security Advisory System (HSAS)

6. Establish plans and protocols to respond to the DHS HSAS threat levels

Public Awareness

7. Implement and Reinforce a Public Security and Emergency Awareness Program

Drills and Exercises

8. Conduct tabletop exercises and functional drills

Risk Management and Information Sharing

9. Establish and use a risk management process to assess and manage threats, vulnerabilities, and consequences (risk management includes mitigation measures selected after risk assessment has been completed)
10. Participate in an information-sharing process for threat and intelligence information
11. Establish and use a reporting process for suspicious activity (internal and external)

Facility Security and Access Controls

12. Control access to security critical facilities with identification (ID) badges for all visitors, employees, and contractors
13. Conduct physical security inspections

Background Investigations

14. Conduct background investigations of employees and contractors

Document Control

15. Control access to documents of security critical systems and facilities
16. Establish process for handling and access to Sensitive Security Information (SSI)

Security Audits

17. Establish an audit program

The project generated the following gap products:

- SSI guidance document—guidance for transit agencies in terms of proper designation, labeling, and handling of SSI
- Resource links—provision of links to additional resource and guidance documents
- Security forces manpower planning model—development of a scalable security forces manpower planning model

- Testing detailed protective measures implementation—validation testing of the advanced systematic approach for transit agencies to consider when developing their protective measures plans, programs, and protocols

Improvement might be required in the following major areas:

- Transit agencies demonstrate is wide variation in the levels of preparedness, including provision of security awareness training, National Incident Management System (NIMS) and Incident Command System (ICS), employee identification programs, building access control, and technology implementation, most notably CCTVs: most agencies were using some form of CCTVs, but the sophistication and extent to which the cameras were being used varied considerably.
- While different forms of perimeter security were in place such as lighting, CCTVs, and physical barriers, improvements are required. Also, interoperable and backup inter- and intra-agency communications is a concern at some agencies.

The project results also indicated that the top 50 agencies had undertaken the following measures:

- Dedicated security managers participating in regional counterterrorism efforts
- Security information sharing with peers
- Updating critical documents and plans
- Updating CCTV systems and perimeter and access control systems
- Transit Watch Program implementation
- Preemployment background checks
- Interagency safety and security drills

The lessons learned that came out of the project were as follows:

- Transit agencies are experiencing information overload, including intelligence that may not be specific enough for each agency.
- Training materials are disjointed and at times unrelated to the audience. Many agencies due to their limited budgets provide security training only to new employees.
- Transit agencies are seeking cost-effective technologies that are suitable (feasible) for their transit system.
- Transit agencies need more guidance on designing security into transit infrastructure, including stations, transit vehicles, and other transit facilities.
- Transit agencies need emergency management.

Transit Agency Security and Emergency Management Protective Measures. Federal Transit Administration, Washington, D.C., 2006.

This report addresses all aspects of the transit agency's security and emergency management activities in relation to the HSAS threat conditions. The type and extent to which the measures are implemented depend on the HSAS threat level. Specific security measures for each of the six security categories addressed in the study are provided and categorized by HSAS threat level. The benefits of this systematic approach is that it provides a solution to reduce vulnerabilities, detect and deter potential attacks or other criminal activities, respond to active incidents or emergencies, and mitigate the consequences of an incident or emergency.

The six categories of suggested protective measures included in the report are as follows:

- Information and Intelligence
- Security and Emergency Management
- Regional Coordination
- Information Technology and Communications Systems
- Employee and Public Communications

- Contingency and Continuity Plans

The report also contains specific measures in appendix B for each of the six categories.

Table 3 of the Report displays the protective topics categorized by the threat type:

Protective Topics	Specific Threat Type							
	Chemical	Biological	Radiological	Explosives/ Incendiary	Nuclear	Fire Arms/ Armed Assault	Hijack/ Hostage	Cyber/ Info Security
Intelligence/Information Sharing/ Cooperation	X	X	X	X	X	X	X	X
Access Control	X	X	X	X	X	X	X	X
Screening	X	X	X	X	X	X	X	X
Training/Drills/ Immediate Actions	X	X	X	X	X	X	X	X
Public Address System and Signage	X	X	X	X	X	X	X	
Surveillance	X	X	X	X	X	X	X	X
High Visibility Patrols	X	X	X	X	X	X	X	
Sweeps/Inspections	X	X	X	X	X	X	X	
K-9 Teams			X	X		X	X	
Alter Operations	X	X	X	X	X	X	X	
Alarms	X	X	X	X	X	X	X	X
Lighting	X	X	X	X	X	X	X	
Remote Sensors	X	X	X	X	X			
Evacuation and Assembly/Lockdown and Shelter in Place Capability	X	X	X	X	X	X	X	
Control of HVAC Systems and Air Vents	X	X	X	X	X	X	X	
Fire Suppression Equipment	X	X	X	X				
Personal Protective Equipment	X	X	X	X	X	X	X	
Decontamination	X	X	X		X			
Mitigation Equipment			X ^a	X ^a			X ^b	

a. Explosive resistant container is an example of mitigation equipment for this threat.

b. Road spikes or stop strips are examples of mitigation equipment for this threat.

Source: *Transit Security Design Considerations*. FTA, Washington, D.C., 2004.

The report describes key transit assets and their vulnerabilities. It also provides design considerations that can help protect these assets. In addition, access management, systems integration, and communications are

addressed in the report. Some of the design considerations have been incorporated into the Synthesis report text. Information about threats presented in the guide is presented below:

The threats that have the most potential to cause casualties, injuries, and/or property loss are identified and described below:

Arson: Arson is an intentionally set fire and can destroy transit assets within a facility, cause structural damage to the facility itself along with electrical and mechanical systems failure, and cause injuries or fatalities. Toxic fumes produced by burning fuel, oil, plastics, and 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 measures 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: The hazards of an explosive blast include the destruction of assets within a facility, structural damage to the facility itself, and injuries or fatalities. In addition, explosions may start a fire, which may inflict additional material damage, injuries, or fatalities due to direct exposure or to heat, smoke, and fumes. 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 the structure while the fireball may ignite other building materials leading to a larger fire. The strength of a blast depends on the type and amount of explosive material used. A bomb that a person can carry is capable of a smaller blast than an explosive-laden truck.

Weapons of mass destruction (WMD): Weapons of mass destruction (WMD) typically refer to nuclear, radiological, chemical, and biological weapons capable of inflicting mass casualties. WMD can also refer to radioactive materials and other contaminants intended to quickly harm large numbers of people, such as any powders, liquids, gases, and dirty bombs; most of these come in a liquid, vapor, gas, or powder form, and are spread through air movement. The hazards of WMD include fatalities or deleterious health effects, as well as potentially permanent contamination of a facility that may render it unusable. Many agents have little or no plainly discernable characteristics, so symptoms may be the first sign that an attack has occurred. While some chemical agents induce immediate symptoms, other agents will not produce symptoms for hours after the attack. Some biological agents may have an incubation period of up to a few days before symptoms appear.

Violent confrontations/hostage situations: Violent confrontations by terrorists are common on transit systems throughout the world. These include assaults carried out on board transit vehicles or at transit facilities, with the intent of inflicting casualties, property damage, or both. Violent incidents may include the taking of hostages. Transit vehicles are especially vulnerable to hostage situations because of easy public access, remoteness of the vehicle, and available civilians onboard. Such attacks are meant to create widespread fear and apprehension through public displays of violence and the interruption of public services. 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: Tampering with transit facilities' assets may be a means to achieve any of the above events, such as starting a fire or spreading an airborne chemical agent, or it may be a stand-alone act, such as tampering with a track to induce derailment. It can also include the intentional ramming of a facility, with a truck, boat, or airplane, to cause structural damage to a facility or injury to its users. The ramming vehicle may be laden with explosives. Depending on the situation, tampering may lead to asset damage, structural damage, contamination, injuries, and/or fatalities.

Power Loss: Loss of electrical power, either locally or over a broad area, can pose a major problem for transit systems in the form of diminished or suspended operations control, computer-aided dispatch, and radio systems. Loss of electricity could be the result of an intentional attack or unintentional event—either within the agency or in the surrounding environment—but in any case could hinder a transit agency's ability to operate or communicate effectively. Apart from service impairment, loss of power may

inadvertently result in damage to property or persons within the agency, in the service area, or 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 or bridge, into transit infrastructure, or may plant explosives in the vehicle while in the storage yard in hopes of detonating it at a later time. A retired transit vehicle may be an attractive weapon or vehicle for carrying out terrorist operations because of its familiar and innocuous nature.

TCRP and NCHRP Cooperative Research Programs

As reported in the TRB Cooperative Research Programs Security Research Status Report dated May 12, 2008, a wide range of transit and transportation security research has been completed after 9/11 through the TCRP and NCHRP Cooperative Research Programs (CRPs). As of February 2009, 100 security-related projects have been authorized in the CRPs: 76 of these projects have been completed; 15 projects are in progress; and 9 projects have contracts pending or are currently in development. The AASHTO Special Committee on Transportation Security and APTA Executive Committee Security Affairs Steering Committee provide steering direction to the coordinated CRP security research under NCHRP and TCRP, respectively. A technical panel provides all-hazards, all-modes oversight and project selection guidance through NCHRP Project Panel 20-59, Surface Transportation Security Research.

Capsule descriptions of products and links to a variety of security-related products produced by the TRB, other divisions of the National Academies, and other transportation research organizations can be found on the TRB and National Academies' Security-Related Products and Links website at www.TRB.org/NASecurityProducts:

- TRB Security-Related Publications—TRB-published reports at TRB.org/SecurityPubs
- TRB Cooperative Research Programs Security Research Status Report—Updated monthly (in PDF)
- Transportation Security: A Summary of TRB Activities—Updated monthly (slideshow in PDF)
- TRB Transportation System Security Website
- Key Hazards and Security Products of the National Academies—Updated monthly (in Microsoft Word, with live links)
- Slides—Hazards and Security Activities of the National Academies—28 MB in PowerPoint with live links)
- Transportation Security Information Contained in TRB's Transportation Research Information Services Database
- Transportation Security Research in Progress
- Select Non-TRB Transportation Security Information—Material highlighted in past TRB e-newsletters

A list of TCRP and NCHRP security research products is provided below.

TCRP Research Studies

1. Communication of Threats: A Guide
2. K9 Units in Public Transportation: A Guide for Decision Makers
3. Robotic Devices for the Transit Environment
4. Intrusion Detection for Public Transportation Facilities Handbook
5. Security-Related Customer Communications and Training for Public Transportation Providers
6. Applicability of Portable Explosive Detection Devices in Transit Environments
7. Public Transportation Emergency Mobilization and Emergency Operations Guide
8. Continuity-of-Operations (COOP) Planning Guidelines for Transportation Agencies

9. Guidelines for Transportation Emergency Training Exercises
10. Hazard and Security Plan Workshop: Instructor Guide
11. Security Measures for Ferry Systems
12. Making Transportation Tunnels Safe and Secure
13. Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers

NCHRP Research Studies

1. Responding to Threats: A Field Personnel Manual
2. Information Sharing and Analysis Centers: Overview and Supporting Software Features
3. Incorporating Security into the Transportation Planning Process
4. A Self-Study Course on Terrorism-Related Risk Management of Highway Infrastructure
5. Guidance for Transportation Agencies on Managing Sensitive Information
6. Guide for Emergency Transportation Operations
7. System Security Awareness Training for Transportation Employees
8. Continuity-of-Operations (COOP) Planning Guidelines for Transportation Agencies
9. Guidelines for Transportation Emergency Training Exercises
10. A Guide to Transportation's Role in Public Health Disasters
11. Disruption Impact Estimating Tool--Transportation (DIETT): A Tool for Prioritizing High-Value Transportation Choke Points
12. Making Transportation Tunnels Safe and Secure
13. A Guide to Traffic Control of Rural Roads in an Agricultural Emergency

Publication is pending for:

- * Costing Asset Protection: An All-Hazards Guide for Transportation Agencies
- * Security 101: Physical Security Standards and Guidelines
- * An Airport Guide for Regional Emergency Planning for CBRNE Events

TCRP Report 86, Volume 1: Communication of Threats: A Guide. Transportation Research Board, National Research Council, Washington, D.C., 2002.

Because identifying threats is a first step toward protecting transit systems, the threat identification and dissemination mechanism are discussed in detail in the guide. Threat management and consequence mitigation strategies are also mentioned.

TCRP Report 86, Volume 2: K9 Units in Public Transportation: A Guide for Decision Makers. Transportation Research Board, National Research Council, Washington, D.C., 2002.

The research report describes the use of canines in counterterrorism applications at transit systems. The attributes and disadvantages of canines are described in detail in this report. Case studies are also provided.

The key advantages mentioned in the report are as follows:

1. Good for public relations, supports outreach with community and media, and provides strong symbol for public safety.
2. Effective tool for deterrence and order maintenance, passengers generally like K9 unit, criminals are often fearful of trained police dogs.
3. Supports a higher level of officer safety, criminal fear of dogs reduces resistance during apprehension.
4. More effective resource for facility searches, one K9 team can perform the work of four patrol officers.
5. Most effective resource available for nonrepetitive detection of narcotics and explosives, no technology or other resource is better.
6. One K9 team can perform dual functions, supporting both patrol and either drug or explosives detection.
7. Grants are currently available for dual function patrol and drug detection dogs.

The key disadvantages mentioned in the report are as follows:

1. Consequences of poor planning are exacerbated by the importance of initial decision making to program capabilities and performance. Bad decisions cannot easily be overcome.
2. Reliance on outside technical support is often necessary to start a program, a major vulnerability for a system new to this function. Good help is hard to find.
3. High program start-up costs, not averaged evenly over time, places large emphasis on cost savings during the phase of project when spending is most essential.
4. Difficulty of finding good dogs, patrolling the transportation environment places additional strains on K9s, selection testing is critical, but expensive and not readymade for public transportation.
5. 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.
6. Legal and public relations consequences of bites, the public has zero tolerance for what it may perceive as inappropriate force exerted by police dogs.
7. Demands of K9 administration are high for a supervisor with other responsibilities. Scheduling challenges limit availability of K9s for service.
8. Success requires a long-term investment, several months to a year for results.
9. Constant effort is required to ensure that law enforcement and operations personnel are using the resources of the K9 unit.

***TCRP Report 86, Volume 4: Intrusion Detection for Public Transportation Facilities Handbook.* Transportation Research Board, National Research Council, Washington, D.C., 2003.**

This report provides information about the various intrusion detection systems that may be applicable for transit agencies. The following categories of systems are covered in the handbook:

- Fencing Systems
- Barrier Systems
- Lighting Systems
- Video Systems
- Access Control Systems
- Sensor Systems
- Identification Systems
- Data Fusion, Display and Control Systems
- Crisis Management Software
- Other Systems

***TCRP Report 86, Volume 5: Security-Related Customer Communications and Training for Public Transportation Providers.* Transportation Research Board, National Research Council, Washington, D.C., 2004.**

The research produced a video presentation entitled *Being Prepared: Security Training and Communication* and provided recommendations on customer security communications.

***TCRP Report 86, Volume 6: Applicability of Portable Explosive Detection Devices in Transit Environments.* Transportation Research Board, National Research Council, Washington, D.C., 2004.**

The capabilities of existing portable explosive detection devices (EDDs) in a transit environment, including subways and bus station platforms, were addressed along with how EDDs can be used effectively without interfering with efficient operations, scientific and technical expertise in the deployment and operation of portable EDDs, and field operational tests to assess the efficacy of available portable EDDs in transit settings. The testing confirmed the feasibility of trace detection equipment in transit systems.

***TCRP Report 86, Volume 8: Continuity-of-Operations (COOP) Planning Guidelines for Transportation Agencies.* Transportation Research Board, National Research Council, Washington, D.C., 2005.**

COOP helps transportation agencies ensure the performance of critical services during and after emergencies. The guidelines assist transportation agencies in evaluating and modifying existing COOP plans, policies, and procedures, as called for in NIMS, and provide guidelines for agencies to develop, implement, maintain, train for, and exercise COOP capabilities.

***TCRP Report 86, Volume 11: Security Measures for Ferry Systems.* Transportation Research Board, National Research Council, Washington, D.C., 2006.**

The objective of this project is to provide guidance to the ferry operators in selecting security measures. The Excel tool generated from the research contains a detailed list of security measures and five sets of evaluation criteria that are weighted by the user. The evaluation criteria weights are used to calculate the value of each option to the user, thereby enabling the user to compare many alternative options against user-specific criteria. This approach provides the user with a methodology to consider operator-specific requirements using operator-weighted criteria. Part I of this report, "Guide for Evaluating Security Measures for the U.S. Ferry System," is designed to accompany the Excel tool and provide step-by-step guidance for evaluating measures.

The measures include the following:

Fencing/Barriers

- Retractable vehicle barriers/gates
- Fixed vehicle deterrent with pedestrian access
- Fixed, both vehicle and pedestrian deterrent

Access Control

- Credentials
- Locks
- System control

Intruder Sensors

- Perimeter (doors and windows, walls and fences, and buried)
- Volume sensors—motion detectors

Monitoring

- Lighting
- CCTV/video

Procedural/Low Cost Waterside Security

- Surface
- Underwater

Screening

- Passengers and cargo
- Trace detection

Human Observation

- All areas
- Waterside

TCRP Report 86, Volume 12: Making Transportation Tunnels Safe and Secure. Transportation Research Board, National Research Council, Washington, D.C., 2007.

The report addresses countermeasures for transportation tunnels and answers the following questions:

- What natural hazards and intentional threats do tunnel operators face?
- How would they be introduced?
- What are the vulnerable areas?
- How much of a disturbance would there be?
- How can these hazards and threats be avoided?
- How can preparations be taken in case the disturbance occurs?

TCRP Report 86, Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers. Transportation Research Board, National Research Council, Washington, D.C., 2007.

Passenger Security Inspections (PSIs), described in detail in *TCRP Report 86, Volume 13: Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers*, are suspicionless inspections of transit passengers by transit security or staff. Because the Fourth Amendment requires warrants or individualized suspicion to conduct inspections, PSIs are legally permissible only if they can be justified. Therefore, legal and other issues need to be carefully considered by transit agencies before implementation.

The PSI decision-making model recommended in the report is an excellent way in which transit agencies can determine whether to use PSI, which PSI to use, and how to implement it. Risk assessment is the first step in the model because PSIs should be linked to the terrorism risk to justify their use. Next, PSI methods should be evaluated for operational feasibility (such as space and power requirements, available resources/personnel, time to inspect). Legal implications—constitutional, tort, and Americans with Disability Act ramifications, major risks, and mitigation of those risks—need to be carefully evaluated. Fourth Amendment liability can be mitigated by linking PSIs to clearly articulated threats, providing adequate notice of inspections, limiting the scope of inspections to the threat, and providing the opportunity to avoid the inspections. After the agency decides to use PSIs, a written policy describing the purpose and scope of the inspections should be developed along with a written protocol and procedures of how the policy should be implemented. Finally, PSI methods need to be assessed. Specific checklists are provided in the guidance for equipment parameters, personnel parameters, passenger service impact parameters, cost parameters, and operational parameters.

PSIs may be conducted using manual or visual inspections. In manual inspections, the officer opens a passenger's bag and may move the items within the bag. In visual inspections, the officer observes but does not touch the contents. PSI technologies primarily have been used in aviation security but are not considered appropriate for use in the transit environment because of their size and passenger delays caused by the inspections. Portable and handheld versions of the technologies, such as handheld electronic explosives detection equipment, portable trace detectors, and radiation pagers, are being tested or are being used by transit systems. Canine teams with explosives-detection capability are considered the best PSI option by many agencies. This is due to the unobtrusiveness and adaptability of canines to the transit environment. Behavioral assessment is seen as a cost-effective way to identify suspicious behavior, because existing transit staff can be taught how to perform behavioral assessments.

The report appendix contains a Technology Review which includes the following information:

- Operational Issues
- Customer Acceptance
- Health Issues
- Customer Communications
- Costs

Technologies for Bulk Detection

- X-rays
- Backscatter X-rays
- Infrared (IR)
- Terahertz
- Millimeter Wave Imaging
- Neutrons, gamma rays, magnetic resonance and magnetic fields

Technologies for Trace Detection

- Ion Mobility Spectrometry (IMS)
- Mass Spectrometry (MS)
- Surface Acoustic Wave (SAW)
- Optical Infrared Spectroscopy
 - Photoacoustic Infrared Spectroscopy (PIRS)
 - Filter Based Infrared Spectrometry

Nascent Technologies

- MS + Chromatography
- Automated MS
- Environmental Monitoring using MS
- Terahertz Light Wave Hand-held Wand
- Nonlinear Optical
- Micro Electro-Mechanical Sensors (MEMS)
- Biosensors
- Dynamic behavior of an explosive vapor plume
- Electronic “Biosensor”

Canine Teams

Canine teams are seen by some transit systems as a cost-effective way to enhance security. These canine teams are able to detect explosives and clear suspicious packages. Other canine teams already in use at these agencies have been trained to perform one or more of these security and safety-related duties: act as deterrent patrols in stations, platforms, vehicles, transfer centers, and 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 that threaten the handler or other persons; and defend or protect public safety officers or other persons.

***TRB Special Report 294: The Role of Transit in Emergency Evacuation.* Transportation Research Board, National Research Council, Washington, D.C. 2008.**

The report emphasizes the need for local and regional evacuation plans and emergency operations plans to include transit. The report's focus is on major incidents in the largest urbanized areas. The surge requirements and coordination demands of evacuations resulting from such incidents are considered in this report. In addition, the needs and mobility challenges of evacuating the disabled and elderly populations are addressed.

Cyber Threats

Cyber attacks can compromise sensitive information, expend valuable manpower and cause major disruptions to transit service and operations. As increasing numbers of transit systems deploy ITS technologies, such as automatic vehicle location (AVL) and traveler information, the consequences of a single virus can be serious and cause significant economic damage to a transit agency. Hackers have illegally accessed a transit agency's control center network and altered displays on electronic message signs.

Terrorist organizations and other organized crime understand the enormous potential of cyber crime to make money, access sensitive data, and wreak havoc on the U.S. economy ("Cyber-criminals Becoming Increasingly Professional" 2007). Cyber crime against U.S. businesses, government agencies, organizations, and individuals has been increasing at an alarming rate. Annual business losses resulting from cyber crime have risen to \$55 billion (Identify Theft Research Center 2007). In 2006, there were 15 million victims of identity theft, which translates into a new victim every 2 seconds (Acohido 2007). The number of records lost or stolen has increased from 50 million in 2006 to 162 million in 2007 (NewsEdge Corp. 2007).

Cyber criminals have also become increasingly sophisticated and more organized. Hackers have established social networks and actively exchange hacking toolkits and other information to facilitate their illegal activities (Beaver 2007).

Wider attack surfaces have been created by increased automation of systems that introduce new vulnerabilities and more points of entry. Wireless systems, which are inherently more vulnerable to attacks, are becoming more pervasive in all types of applications, including communications, data transfer, and access control and monitoring. The replacement of physical servers with virtual servers and the creation of storage-specific hacking tools that can cause attacks on storage systems to go unnoticed make information security more challenging (Weber 2008).

For transit agencies, IT vulnerabilities not only include employee databases with sensitive HR information but also mission-critical systems, including bus fleet maintenance processes and schedules, rail signal systems, transit command centers, AVL control systems, and electronic signage. Any policing, security-related, or highly sensitive information, such as patrol schedules, is desirable to terrorists and criminals, and this information should be considered vulnerable to attack.

DHS has acknowledged the importance of cyber security and its National Cyber Security Division established the Computer Emergency Readiness Team to defend against cyber attacks. DHS is actively creating security standards and both the Director of National Intelligence and the Overseas Security Advisory Council have stated that cyber security is a primary concern for 2008. However, it may take several years before a national cyber defense system is perfected. Therefore, transit agencies would benefit from a proactive stance on combating cyber crime.

Ferry Threats

All vehicles are subject to screening requirements set by the Maritime Transportation Security Act of 2002 (MTSA). Regulations based on the Act became effective on July 1, 2004—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, new regulations were established 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).

In *TCRP Report 86, Volume 11*, the three major threat categories for ferries, the delivery methods, and acts of force are listed as follows:

- **Incendiary and explosive devices (IEDs)**—for example, planted in a facility or on a suicide bomber, car, truck, underwater mine, or fuel container.
- **Acts of force**—for example, hijacking or commandeering a vessel or facility. Acts of force may include use of firearms, knives, or other weapons or use of physical impact (e.g., ramming) to inflict injury to persons or damage a vessel or facility.
- **Chemical, biological, and radiological (CBR) agents**—for example, chlorine, anthrax, and dirty bombs.

The delivery methods include the following:

- **By person**—including suicide bombers; people setting remotely detonated, time-detonated, or sensor-detonated IEDs; people creating IEDs (e.g., igniting fuel or creating electrical fires); people concealing IEDs in hand baggage, and so forth.
- **By vehicle**—including cars, trucks, or railcars. Vehicles may conceal diesel, fertilizer, liquefied natural gas (LNG), gasoline, and other IEDs. Large cars can accommodate up to about 1,000 pounds of explosives without significant modifications and more with significant modifications of the suspension. Trucks may deliver thousands of pounds of explosive material to destroy buildings, large vessels, and so forth. Delivery by truck (e.g., as in the Oklahoma City bombing, the first World Trade Center bombing, and the Beirut marine barracks) is the most common mode of IED delivery.
- **By vessel**—including boats or other floating vessels (e.g., USS Cole style).
- **Artillery**—including rocket-propelled grenade (RPG) launchers. While RPGs may be legally obtained in the United States, ammunition may enter the country only through illegal means. RPGs may be fired from the shore or from passing boats.
- **Underwater**—includes IEDs that divers attach to the hull, mines that divers place in the path of a ferry, and so forth.
- **Overhead**—including IEDs that are dropped from bridges or cliffs, light aircrafts, commercial airliners, remotely controlled aircrafts, helicopters, and so forth.

Acts of force include the following:

Commandeering—seizing control of a portion or all of a facility or vessel for the purpose of piracy or hijacking. This act is commonly carried out with the use (or threatened use) of firearms; knives; IEDs; CBR agents; or other weapons.

Ramming—driving a vehicle, vessel, or aircraft into a vessel or shore-side facility. A ferry may be rammed or commandeered for ramming. This act may involve the use of IEDs or CBR agents, but the initial portion of the attack—the ramming itself—is an act of force.

Security and Safety Standards Resources

In addition to the information about APTA's initiatives mentioned in the text of the Synthesis, the following are other sources of security and safety standards information:

- The Code of Federal Regulations is developed to comply with the legislative mandates passed by Congress and signed into law by the president. The federal government also issues recommended practices, which are nonregulatory, but provide an awareness of issues and tools to address them.
- The American National Standards Institute is a private nonprofit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
- The Security Industry Association represents a wide range of stakeholders and is developing expected application behaviors and metrics to enable the integration of disparate security products.
- The IEEE is a technical professional association that develops standards applicable to rail vehicles, in addition to other engineering areas.
- The ASTM is a nonprofit organization that provides a forum for the development and publication of voluntary consensus standards for materials, products, systems, and services.
- The ASME is an education and technical organization setting many industrial and manufacturing standards.
- The National Fire Protection Association develops consensus codes and standards intended to minimize the possibility and effects of fire and other life safety risks.
- The FTA has issued fire safety practices for rail transit vehicle material selection and the FRA has issued passenger rail equipment fire safety regulations.
- The SAE develops engineering design and safety standards for the motor vehicle industry, including buses.

Banerjee, R., “The ABCs of TCO (Total Cost of Ownership): The True Costs of IP Video Surveillance.” Video Technology and Applications, Feb. 2008.

Maintenance costs can be important in the Total Cost of Ownership (TCO) for video technology. For larger-scale systems, recording and storage can include 50% to 80% of the capital cost and also have a large impact on maintenance costs. Usually, storage requirements are high when a large quantity of cameras or high video quality is desired or when video needs to be retained for a long period of time. Network video recorders (NVRs) have been replacing digital video recorders (DVRs), because DVR storage is available only within or as an attachment to each camera, and NVRs are able to distribute storage capacity across the network. NVRs, however, require a server platform, which is especially costly in terms of maintenance. An alternative approach reduces TCO by up to 30% by using video recording management software to bypass NVR PCs and have IP cameras stream images directly to the storage. The TCO is estimated to be between 3 and 15 times the purchase price of the server hardware and software. Another disadvantage of the PC-based NVR is the difficulty in increasing video quality or retention time. To do this, additional storage would need to be bought and the camera or NVR would need to be reconfigured.

The alternative approach reduces TCO by up to 30% by using video recording management software to bypass NVR PCs and have IP cameras stream images directly to the storage. By eliminating the NVR servers, hardware, software, and maintenance costs are eliminated as well. The video recording management software would distribute video in 1 GB blocks across the network’s storage units untying each storage unit from the camera to which it is attached.

Interoperable Communications

These interoperable communications initiatives described on the DHS website www.dhs.gov are in addition to the federal initiatives mentioned in the Synthesis report:

- The Office for Interoperability and Compatibility was established in 2004 to assist in the coordination of interoperability efforts across DHS within its Science and Technology Directorate’s Office of Systems Engineering and Development to strengthen and integrate interoperability and compatibility efforts. Project 25 is a standards development process for the design, manufacture, and evaluation of interoperable digital two-way wireless communications products created by and for public safety professionals.
- The DHS-sponsored Multi-Band Radio Project is expected to develop a portable radio allowing emergency responders to communicate with other agencies regardless of radio band.

- DHS and the Emergency Interoperability Consortium have signed an agreement to develop data-sharing standards for the emergency response community and other relevant organizations, government agencies, as well as the general public (DHS 2008).
- DHS Office of Grants and Training's Interoperable Communications Technical Assistance Program provides technical assistance to enhance interoperable communications among local, state, and federal emergency responders and public safety officials as they prevent or respond to a WMD attack, and is associated with Grants and Training's Urban Areas Security Initiative Grant program (DHS).
- SAFECOM's RapidCom initiative ensured that a minimum level of emergency response interoperability would be in place in 10 high-threat urban areas (Boston, Chicago, Houston, Jersey City, Los Angeles, Miami, New York, Philadelphia, San Francisco, and Washington, D.C.). The five "critical success factors" essential to interoperable systems identified in RapidCom were Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage.
- SAFECOM's Radio over Wireless Broadband project is field testing the integration of broadband Push-to-Talk technology and GIS applications with existing Land Mobile Radio systems and standard operating procedures; the project will facilitate the integration of new technologies with existing emergency response communications systems.

A *Homeland Defense Journal* special report on interoperability (Serluco) identified the measures and considerations that should be addressed by agencies for assured communications:

- *Redundant connectivity* is important during emergencies when the public communications infrastructure may be compromised. Critical redundancy considerations include the following:
 - Prioritize access to key data and systems required to conduct essential functions
 - Avoid reliance on terrestrial communications along
 - Consider multijurisdictional dedicated satellite networks
 - Plan for fuel when powering backup generators
- *Continuity planning* including an off-site emergency communications center ensures that emergency operations centers continue operating during emergencies. Critical considerations include the following:
 - Maintain communications capabilities sufficient to support essential operations and to ensure public access to emergency resources
 - Consider entering into a mutual aid agreement with other organizations and agencies to use their facilities for command and control
 - Plan for adequate people space and all that this entails
 - Consider Mobile Emergency Response Operations Centers and Mobile Emergency Communications Vehicles
- *Organizational interdependencies* need to be understood and relationships cultivated, because interagency coordination will result in effective emergency response. Critical considerations include the following:
 - Ensure the ability to collaborate and coordinate voice, data, and video with key stakeholders
 - Know who the stakeholders are and include them as part of the agency's technology, process, and controls planning
 - Map interdependent agencies, departments, systems, processes, data, and controls within the COOP
 - Meet regularly with all stakeholders
 - Regularly test the reliability, timeliness, and accuracy of critical information and analysis flows

Haas, K., *Transportation and Homeland Security: A Critical Issues Guide for Local Officials*. Public Technology, Inc., 2005.

The key topics in this guide include the following:

- Emergency Transportation Planning within the Emergency Planning Framework

- Risk Management Plan Development Guidelines

The guide also answers the following questions:

- Who should develop the emergency transportation plan?
- What threats should a local emergency transportation plan address?
- What are the elements of a local emergency transportation plan?

Taylor, B., et al. “Responding to Security Threats in the Post-9/11 Era: A Portrait of U.S. Urban Public Transit,” *Public Works Management & Policy*, Vol. 11, No. 1, pp. 3–17.

Taylor and his research team performed a survey of transit systems regarding their post-9/11 policies and practices. The researchers found that most of the credible threats were focused on the largest transit agencies. In terms of protective measures, the findings indicated that use of CPTED strategies has increased the most after 9/11.

Despite measurable programmatic progress, however, many respondents believe that meaningfully securing urban transit systems remains a daunting, perhaps insurmountable, challenge.

TCRP Web Document 18: Developing Useful Transit-Related Crime and Incident Data. Transportation Research Board, National Research Council, Washington, D.C., April 2000.

Primary data sources of crime statistics include incident reports filed by transit police or security, reports and complaints called into transit police, and information gathered by local law enforcement.

If transit police are not available to take a report from a passenger or employee, incidents may not be reported, especially minor ones such as fare evasion and theft. In these cases, minor crimes as well as quality-of-life violations will be underreported, cannot serve as good indicators of disorder, and will impede the assessment of policing tactics. The underreporting of quality-of-life crimes also occurs because the FBI’s Uniform Crime Reporting (UCR) reporting guidelines being following by the FTA recommend reporting only those crimes that result in an arrest.

Another crime data issue is the definition of a transit-related crime. If it is not clear, some local police agencies may simply aggregate borderline cases with other crime data and not specify that it is transit-related. This would be a problem for agencies that do not have their own police force. Crime data research conducted for TCRP Project F-6A concluded that, while the definition used by each individual agency was consistent within the agency, “the lack of a generally accepted definition of transit-related crime makes it impractical to compare transit crime rates between agencies, or to obtain a consistent and accurate picture of transit crime trends at a national level.” There is also a lack of uniformity in the definition of the different types of crime. The project report also states that “the only consistent use of defined terms is for the eight serious crimes—homicide, rape, robbery, aggravated assault, burglary, larceny/theft, motor vehicle theft, arson.” In terms of the presentation of the crime data, the study concluded that data tables and charts are not consistent across agencies.

Reed, T.B., et al., *Transit-Passenger Perceptions of Transit-Related Crime Reduction Measures, Transportation Research Record 1731*, Transportation Research Board, National Research Council, Washington, D.C., 2000, pp. 130–141.

In a 1999 Michigan study of violent crimes against public transit bus operators and passengers, transit passenger perceptions of numerous transit-related crime reduction measures—patrol and security, design actions, and technological innovation—were determined via survey. The respondents indicated emergency telephones for passengers and increased lighting as the best crime-prevention measures.

References for the Literature Review Appendix

- Acohido, B., "Theft of Personal Data More Than Triples This Year," *USA TODAY*, Dec. 9, 2007 [Online]. Available: http://www.usatoday.com/money/industries/technology/2007-12-09-data-theft_N.htm.
- Beaver, K., "Locking Down Today's Data Centers," *Security Technology & Design*, Dec. 2007, pp. 30–34.
- "Cyber-criminals Becoming Increasingly Professional," *Government Technology*, 2007 [Online]. Available https://www.govtech.com/gt/print_article.php?id=144372 [accessed Dec. 12, 2007].
- Department of Homeland Security, "Emergency Interoperability Consortium Announce Alliance to Help First Responders." *ISC365.com*, Mar. 26, 2008.
- Department of Homeland Security website [Online]. Available at http://www.ojp.usdoj.gov/odp/ta_ictap.htm.
- Identity Theft Research Center, *Employee Security Connection*, Vol. 19, No. 3, Apr. 30, 2007..Facts and Statistics [Online]. Available: http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics.shtml [accessed Dec. 25, 2007].
- NewsEdge Corp, "Profile of Computer Hackers Changing," *CommwebNews.com*, Dec. 26, 2007.
- Serluco, P., "Special Report: MorganFranklin Guide: Interoperability vs. Assured Communications, Critical Factors for Emergency Managers." *Homeland Defense Journal* [Online]. Available: <http://www.homelanddefensejournal.com>.
- Weber, S., "Cyber Security: Ignore At Your Peril." *Forbes.com.*, Feb. 28, 2008.

APPENDIX C SURVEY QUESTIONNAIRE



Agency Name: _____

National Transit Database ID: _____

Address: _____ **City/State/Zip Code:** _____

Respondent Name: _____

Title: _____

Telephone: _____ **Fax:** _____ **E-mail:** _____

PLEASE NOTE: The information requested for this survey will not be reported in a manner specific to you or your agency. Contact information will be used only for follow-up or clarification by the survey team and agency responses will be held in strictest security and confidentiality. Survey responses will be reported only in the aggregate for the final document.

I. NATURE AND EXTENT OF SECURITY OFFENSES

1. Which of the following are the primary terrorist threats faced by your system? Check all that apply.

- Explosives Radiological
- Chemical Cyber-crimes
- Biological Hijackings
- Sabotage Shootings
- Other—Specify: _____

2. What performance measures does your system use to ascertain security levels, as well as the effectiveness of security interventions? A few example measures follow; if any other or additional measures are used, please indicate the measure, as well as how it is calculated. Please check all that are applicable.

- __ Total security incidents per 10 million passenger trips
- __ Total security incidents per 1 million vehicle-miles
- __ Serious security incidents per 10 million passenger trips
- __ Serious security incidents per 1 million vehicle-miles
- __ Total fatalities caused by a serious security incident per 100 million passenger trips
- __ Total injuries caused by a serious security incident per 10 million passenger trips
- __ Average number of injuries per security incident
- __ Dedicated security personnel per million unlinked annual passenger trips
- __ Percent of security personnel who have completed transit security training
- __ Percent of frontline transit personnel who have completed transit security training

Other—Specify: _____

3. Please indicate the year 2000 and year 2006 values of as many of the preceding measures as are applicable.

Performance Measure	2000 Value	2006 Value	Goal or Preferred Value

4. Please specify the attributes of the perpetrators of major security offenses reported to the National Transit Database, if any, in 2000 and 2006. Please place either a percentage or actual number in the indicated spaces:

Year	Male	Female	Patron	Employee	Other	Gang Member	Member of Terrorist Group
2000							
2006							

5. Please specify the attributes of the perpetrators of minor security offenses reported to the National Transit Database, if any, in 2000 and 2006. Please place either a percentage or actual number in the indicated spaces:

Year	Male	Female	Patron	Employee	Other	Gang Member	Member of Terrorist Group
2000							
2006							

6. During 2000, how many of the following threats or incidents of terrorism occurred? If actual data are not available, please estimate. Please indicate the mode/location, and the number of offenses for each mode/location.

- | <i>Mode</i> | | <i>Location</i> |
|-------------------|------------------|----------------------------------|
| a = Subway/HR | e = Transit Bus | 1 = In-Vehicle |
| b = Light Rail | f = Commuter Bus | 2 = In-Station/
Stop/Terminal |
| c = Commuter Rail | g = Paratransit | 3 = Parking Facility |
| d = AGT | h = Other | 4 = Other |

	MODE/LOC	NO. OFFENSES	MODE/LOC	NO. OFFENSES	MODE/LOC
a. Transit Vehicle Hijacking	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
b. Hostage/Barricade	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
c. Sabotage of Transit Infrastructure	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
d. Sabotage of Transit Property	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
e. Other Sabotage	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
f. Multiple Shootings	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
g. Placement or Detonation of Explosives within System	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
h. Placement or Release of Chem/Bio Contaminants	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
i. Intentional Hoaxes	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
j. Bomb/Explosives Threats	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
k. Other Threats	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____

7. During 2006, how many of the following incidents or threats of terrorism occurred? If actual data are not available, estimate if possible. Please indicate the mode/location, and the number of offenses or incidents for each mode/location.

- | | | | |
|-------------------|------------------|----------------------|--|
| <i>Mode</i> | | <i>Location</i> | |
| a = Subway/HR | e = Transit Bus | 1 = In-Vehicle | |
| b = Light Rail | f = Commuter Bus | 2 = In-Station | |
| | | /Stop/Terminal | |
| c = Commuter Rail | g = Paratransit | 3 = Parking Facility | |
| d = AGT | h = Other | 4 = Other | |

	MODE/LOC	NO. OFFENSES	MODE/LOC	NO. OFFENSES
a. Transit Vehicle Hijacking	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
b. Hostage/Barricade	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
c. Sabotage of Transit Infrastructure	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
d. Sabotage of Transit Property	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
e Other Sabotage	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
f. Multiple Shootings	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
g. Placement or Detonation of Explosives within System	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
h. Placement or Release of Chem/Bio Contaminants	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
i. Intentional Hoaxes	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____
j. Bomb/Explosives Threats	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____

Please describe the above incidents in greater detail, especially if any of these incidents caused any fatalities, injuries, or property damage, or if there were multiple incidents of the same type.

8. Please note any trends for the offenses or incidents listed above; if specific offenses or incidents have undergone an increase or decrease, please list them in the appropriate spaces below:

	Increase	Decrease
a. In the past decade	_____ _____ _____	_____ _____ _____
b. Since Sept. 11, 2001	_____ _____ _____	_____ _____ _____
c. In the past two years	_____ _____ _____	_____ _____ _____

9. Please indicate the total number of cyber-security breaches your agency experienced in 2000 and 2006, excluding viruses:

Year 2000	Instances
a. Unauthorized Access/Hacking Agency Website	
b. Unauthorized Access/Hacking Agency Control Center	
c. Tampering with Rail Signals	
d. Tampering with Electronic Message Signs	
e. Unauthorized Access of Databases	
f. Other, Please Specify:	
Year 2006	Instances
a. Unauthorized Access/Hacking Agency Website	
b. Unauthorized Access/Hacking Agency Control Center	
c. Tampering with Rail Signals	
d. Tampering with Electronic Message Signs	
e. Unauthorized Access of Databases	
f. Other, Please Specify:	

10. Please note any trends in cyber-security breaches; if specific breaches have increased or decreased, please list them below:

	Increase	Decrease
a. In the past decade	 	
b. Since Sept. 11, 2001	 	
c. In the past two years	 	

11. Please specify the attributes of the perpetrators of the cyber-security crimes, if available. Please place either a percentage or actual number in the indicated spaces:

Year	Male	Female	Patron	Employee	Other	Gang Member	Member of Terrorist Group
2000							
2006							

12. Please note any trends in reports of suspicious activity, objects, or persons that have changed in the time periods listed below by checking the appropriate box:

Reports of Suspicious Activity, Objects, or Persons	Increase	Decrease	Remain the Same
a. In the past decade			
b. Since Sept. 11, 2001			
c. In the past two years			

13. System Security Data and Analysis

a. What security data including data used in security planning are collected?

b. What are the sources of data on offenses already listed?

c. What are sources of data on other security matters, including security planning data?

System reports

System reports

Police reports

Police reports

Other—Specify: _____ Other—Specify: _____

d. Using these data, does your system perform crime-mapping, trend analysis, or other security data analysis? Please describe analyses techniques and how the results are used by your agency.

e. What data-related issues or concerns do you have, and why?

14. During the period after September 11, 2001, what happened to the following:

	Increase	Decrease	Remain the Same
a. Patronage			
b. Offenses against passengers			
c. Offenses against workers			
d. Passenger complaints of violence or potential violence			
e. Passenger complaints of excessive security			
f. Passenger requests for increased protection			
g. Worker days lost as a result of violence-related incidents			
h. Violence-related legal actions			

What major changes, if any, have been made at your agency in overall security and security practices since September 11, 2001?

15. a. In which area(s) is your agency currently making security-related investments?

Please rate the investments "high," "medium," "small," "none," or "planned."

- Technology _____
- Security Staff _____
- Employee Training _____
- Customer Outreach and Education _____
- Design (CPTED)/Situational Crime Prevention _____
- Other, Please Specify: _____

b. Have you seen an impact on your system from these investments? Yes No

If yes, what have the impact(s) been?

16. a. What type of security enforcement does your system use? Please indicate the number of staff or full-time equivalents (FTEs):

- Full-time Sworn Officers: System Employees _____
- Full-time Sworn Officers: Contractors _____
- Full-time Nonsworn Officers: System Employees _____
- Full-time Nonsworn Officers: Contractors _____
- Part-time Sworn Officers: System Employees _____
- Part-time Sworn Officers: Contractors _____
- Part-time Nonsworn Officers: System Employees _____
- Part-time Nonsworn Officers: Contractors _____

b. Has there been an increase in security staff hours since September 11, 2001? If so, then please indicate the percent increase. Please provide any details, if possible.

II. SECURITY PRACTICES

Please indicate security practices used by your system, including those to prevent or control violence and confrontational incidents and those to counter terrorism. Also, for each practice, please indicate Purpose, Mode, Location, and Year(s) of Deployment:

<i>Purpose:</i> "C" to address Crime	<i>Mode:</i> 1 = Subway/HR	5 = Transit Bus
"T" to address Terrorism	2 = Light Rail	6 = Commuter Bus
"Q" to address Quality of Life	3 = Commuter Rail	7 = Paratransit
	4 = AGT	8 = Other

Location(s) of Deployment:

Systemwide, all Modes 0

Location List for Bus

- 1 = Bus Stop
- 2 = In-Vehicle
- 3 = Transfer Terminal, Hub, Multimodal Facility
- 4 = Garage, Maintenance Facility, Yard
- 5 = Administrative Facility
- 6 = Other

Location List for Rail

- 7 = Station, Platform
- 8 = In-Vehicle
- 9 = Infrastructure/Right-of-Way
- 10 = Transfer Station or Terminal
- 11 = Maintenance Facility/Yard/Storage Area
- 12 = Administrative Facility
- 13 = Other

Parking Lot

- 14 = Parking or Park & Ride Lot

Other Mode(s)

- 15 = All Locations

Year(s) of Deployment: Please note the primary year(s) in which a measure was implemented. If a measure is in the testing phase, please indicate "T." If a measure is being planned for implementation, please indicate "P."

17. Access Control	Purpose	Modes	Locations	Year(s)
Admission control – biometric				
Admission control – encoded cards				
Admission control – manual verification				
Admission control – memorized code				
Admission control – mechanical lock				
Admission control – electronic locks				
Admission control – turnstiles, floor-to-ceiling				
Admission control – turnstiles, standard electronic				
Fencing and gates – mechanical				
Fencing and gates – electronic, alarm				
Fencing and gates – electronic, no alarm				
Intrusion sensors				
Explosives detector(s)				
Metal detector(s)				
Random ID checks				
Vehicle access control and parking				
Vehicle barriers				
Vehicle check for explosives				
Window (and other openings) alarms				
Wall safeguards				
Other – Specify: _____				

18. Design (CTPED)/Situational Crime Prevention	Purpose	Modes	Locations	Year(s)
Site Selection/Building Placement				
Lighting				
Internal Design/Configuration				
Physical or Natural Barriers				
Other – Specify: _____				

19. Transit Vehicle Design	Purpose	Modes	Location	Year(s)
Transit Vehicle Compartment Locks				
Enhancement of Visibility into/out of the Vehicle				
Vehicle Hardening				
Fire Reduction Measures				
Transit Operator Compartment				
Public Address System				
Silent Alarm and/or Panic Button				
Silent Alarm and/or Panic Button with AVL				
Vehicle Access Control (e.g., key) Specify:				
Other – Specify:				

20. Surveillance and Inspections	Purpose	Modes	Location	Year(s)
CCTVs (images not recorded)				
CCTVs (images are recorded)				
Intelligent Video				
Facial Recognition				
Fare Checkers				
Canine Inspections – explosives				
Canine Inspections – weapons				
Canine Inspections – narcotics				
Undercover/Plainclothes Officers				
Behavioral Assessment by Transit Staff				
Behavioral Assessment by Security Staff				
Manual/Visual Inspections of Persons/Baggage				
Electronic Inspections of Persons/Baggage				
Random Sweeps				
Roving Patrols with Canine Inspections				
Roving Patrols without Canine Inspections				
Other – Specify:				

21. Operational Strategies	Purpose	Modes	Location	Year(s)
Limiting station access (hours/access points)				
Rerouting buses away from high-profile targets				
Strategic location of bus stops				
Modifying hours of service				
Modifying pretrip inspections				
Fleet management/vehicle-tracking				
Inventory control strategies				
Modification of dispatcher responsibilities				
Parking lot, vehicle flow/ placement reconfiguration				
Other – Specify:				

22. Technology	Purpose	Modes	Location	Year(s)
Automatic Train Control/Monitoring				
AVL				
Emergency Alert for Employees				
Emergency Phones/Call Boxes for Passengers				
Intelligent Video to ID Suspicious Activity				
CCTV – for surveillance				
CCTV – for recording incidents, passenger traffic				
Public Address System				
Radio Communications for Staff				
RFID for inventory control				
Intrusion Sensors and Alarms				
Biological Detector				
Chemical Detector				
Explosives Detector (portable, tabletop)				
Explosives Detector (walk-through)				
Metal Detector				
Radiological Detector/Pager				

23. Communications Security	Purpose	Modes	Location	Year(s)
Redundancy				
Power Supply Backup				
Network Security				
Other— Specify: _____				

24. Security and Policing Management

The following questions relate to specific aspects of security and policing management.

a. Budgeting

What was your total security budget for 2006? \$ _____

What percentage was expended on:

Capital ___% Labor ___% O&M ___% Training ___%

By how much has your total annual security budget changed since September 11, 2001? _____

b. Human Resources Practices

Which of the following HR practices have changed since September 11, 2001?

- Background checks on new hires
- Performance appraisal
- Other

Please specify: _____

c. Security Planning

Does your system have an up-to-date:

- Security Plan? Yes No
- Emergency Plan? Yes No
- Incident Response Plan? Yes No
- Continuity-of-Operations Plan? Yes No

Has the Incident Command System been integrated into the Plans? Yes No

d. Assaults on Employees and Passengers

Which of the following techniques are used to address and mitigate assaults on employees and passengers (committed by passengers or the general public), or to reduce and/or prevent confrontations? Please check all that apply.

- Presence of Security or Transit Personnel
- Roving Security Patrols
- Verbal Techniques
(e.g., verbal judo/transactional analysis)
- Nonverbal Techniques
(e.g., body language)
- Restraining Techniques
- Passenger Codes of Conduct
- Community Policing
- Other—Specify: _____

25. Outreach, Education, Training, and Awareness Strategies

What types of outreach, education, training and awareness strategies does your agency employ, excluding training courses provided to your employees?

- Transit Watch Program
(or similar Awareness program for employees and customers)
- Crime Prevention Program
- Toll-Free Number
(to report suspicious activity and packages)
- Evacuation Instructions
- Other
- Please describe: _____

26. Employee Security and Policing Training

What training courses does your agency provide to your police, security staff (whether in house or contracted out), and employees?

Please describe the courses below:

Course Title: _____					
Provider: (In-house, NTI, TSI, APTA, other) _____					
Delivery Method:					
Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/>					
Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>					
Delivered to:		Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff	<input type="checkbox"/>	_____%	_____	_____	_____
Frontline Employees	<input type="checkbox"/>	_____%	_____	_____	_____
Supervisory Employees	<input type="checkbox"/>	_____%	_____	_____	_____
Management	<input type="checkbox"/>	_____%	_____	_____	_____

Course Title: _____					
Provider: (In-house, NTI, TSI, APTA, other) _____					
Delivery Method:					
Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/>					
Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>					
Delivered to:		Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff	<input type="checkbox"/>	_____%	_____	_____	_____
Frontline Employees	<input type="checkbox"/>	_____%	_____	_____	_____
Supervisory Employees	<input type="checkbox"/>	_____%	_____	_____	_____
Management	<input type="checkbox"/>	_____%	_____	_____	_____

Course Title: _____ Provider: (In-house, NTI, TSI, APTA, other) _____ Delivery Method: Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/> Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>					
Delivered to:		Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff	<input type="checkbox"/>	____ %	_____	_____	_____
Frontline Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Supervisory Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Management	<input type="checkbox"/>	____ %	_____	_____	_____

Course Title: _____ Provider: (In-house, NTI, TSI, APTA, other) _____ Delivery Method: Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/> Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>					
Delivered to:		Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff	<input type="checkbox"/>	____ %	_____	_____	_____
Frontline Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Supervisory Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Management	<input type="checkbox"/>	____ %	_____	_____	_____

Course Title: _____ Provider: (In-house, NTI, TSI, APTA, other) _____ Delivery Method: Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/> Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>					
Delivered to:		Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff	<input type="checkbox"/>	____ %	_____	_____	_____
Frontline Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Supervisory Employees	<input type="checkbox"/>	____ %	_____	_____	_____
Management	<input type="checkbox"/>	____ %	_____	_____	_____

Course Title: _____				
Provider: (In-house, NTI, TSI, APTA, other) _____				
Delivery Method:				
Classroom <input type="checkbox"/> Workshop <input type="checkbox"/> Online, w/Instructor <input type="checkbox"/> Online, w/o Instructor <input type="checkbox"/> Video/DVD <input type="checkbox"/> Interactive CD <input type="checkbox"/> CD <input type="checkbox"/>				
Delivered to:	Percent of Staff	Hours/ Session	Times/ Year	Evaluation Method
Transit Police/Security Staff <input type="checkbox"/>	_____ %	_____	_____	_____
Frontline Employees <input type="checkbox"/>	_____ %	_____	_____	_____
Supervisory Employees <input type="checkbox"/>	_____ %	_____	_____	_____
Management <input type="checkbox"/>	_____ %	_____	_____	_____

27. Drills and Exercises

Please specify how often your agency holds the following drills, exercises, simulations or tabletop exercises/workshops:

- Field Exercises/Drills, Interagency 0/year 1–2/year 3–4/year >5/year
- Field Exercises/Drills, Intra-agency 0/year 1–2/year 3–4/year >5/year
- Simulations or Tabletop Exercises/Workshops 0/year 1–2/year 3–4/year >5/year
- Other, Please specify: _____ 0/year 1–2/year 3–4/year >5/year

28. Covert Testing

Does your agency perform covert testing of any kind? Yes No

If yes, please describe the purpose and method by which testing is performed.

29. Cooperative Relationships with Other Stakeholders

Please indicate whether your agency has cooperative relationships with other units or agencies. Check all that apply:

- Within Agency
- External Agencies/Entities
- Intelligence Sharing

30. Cyber Security

Please indicate your cyber-security measures, excluding virus protection software. Check all that apply.

- Firewall installation
- Network/PC access control
- using passwords
- using biometrics
- Other, Please Specify: _____

III. SECURITY MEASURES BEST PRACTICES

31. Effective Security and Policing Measures

Please list (up to) the top five most effective CRIME-PREVENTION AND DETECTION measures used by your system.

Please provide a cost-benefit ratio for each measure, if possible:

Please list (up to) the top five most effective COUNTERTERRORISM measures used by your system.

Please provide a cost-benefit ratio for each measure, if possible:

32. Is the usefulness of technological or other interventions being evaluated? If so, please describe the evaluation method and results, if available:

33. If your system employs any of these security measures in an innovative manner, or is pursuing an innovative policy, program, or technology research, please describe it here:

34. Obstacles in Security and Policing Management

What are the three greatest obstacles faced by your agency in security and policing management?
Please check up to three of the items listed below:

- Lack of Resources
- Lack of Qualified Workers/Technical Expertise
- Lack of Management Support
- Lack of Customer Support
- Lack of Tested, Market-ready Technology Solutions
- Other, Please Specify: _____

THANK YOU for completing the survey!

Please return the survey by mail, e-mail, or fax to:

Dr. Yuko J. Nakanishi
 Nakanishi Research and Consulting LLC
 93-40 Queens Blvd. #6A
 Rego Park, NY 11374
 Email: ynanish@aol.com
 Fax: (347) 789-7711

APPENDIX D

LIST OF SURVEY RESPONDENTS

Transit Agency	Location
Alaska Railroad Corporation	Anchorage, AK
Annapolis Department of Transportation	Annapolis, MD
Bay Area Rapid Transit (BART)	San Francisco, CA
Ben Franklin Transit	Richland, WA
Bremerton-Kitsap Transit	Bremerton, WA
Capital District Transportation Authority (CDTA)	Albany, NY
Capital Metro	Austin, TX
Central Puget Sound Regional Transit Authority	Seattle, WA
Champaign-Urbana Mass Transit District	Urbana, IL
Charleston Area Regional Transportation Authority	Charleston, W. VA
Community Transit (Snohomish County Public Transportation)	Everett, WA
Connecticut DOT (Shore Line East)	Hartford, CT
Connecticut Transit	Connecticut
Hampton Roads Transit	Hampton, VA
Hillsborough Area Regional Transit Authority (HART)	Hillsborough County, FL
Long Beach Transit	Long Beach, CA
Massachusetts Bay Transportation Authority (MBTA)	Boston, MA
MetroLink (SCRRA)	Pomona, CA
Metropolitan Transit Authority of Harris County	Harris Couty, TX
Milwaukee County Transit	Milwaukee, WI
Niagara Frontier	Buffalo, NY
Orange County Transportation Authority	Orange, CA
Pennsylvania Department of Transportation (PennDOT)	Philadelphia, PA
Public Transit Division, Honolulu Public Transit Authority	Honolulu, HI
Regional Transportation District (RTD)	Denver, CO
Santa Clara Valley Transportation Authority	San Jose, CA
Santa Cruz Metropolitan Transit District	Santa Cruz, CA
South Florida Regional Transportation Authority	Florida
Southwest Ohio Regional Transit Authority (SORTA)	Cincinnati, OH
Sun Metro	El Paso, TX
Transit Authority of River City (TARC)	Louisville, KY
Utah Transit Authority (UTA)	Salt Lake City, Utah
VIA Metropolitan Transit	Texas
Virginia DOT Ferries	Virginia
Virginia Railway Express (VRE)	Wash., D.C.

Note: Agencies that were reluctant to complete the survey were informed that the contact information sheet did not need to be completed with the exception of modal information to ensure complete anonymity.

APPENDIX E

SUMMARY OF SURVEY RESULTS

Survey respondents: Of the 45 respondents, 35% were multimodal transit agencies including rail-only agencies, 58% were bus-only agencies, and 7% were ferry systems. If a specific question received fewer than 10 responses, the question was excluded from this survey summary.

Threats (Q1, 35 responses: 13 multimodal/ferry, 22 bus)

In terms of threats, multimodal agencies considered a greater range of potential threats to be threats than bus agencies considered. All multimodal agencies and most bus agencies indicated that explosives, shootings, and hijackings were the primary threats. Many multimodal agencies also indicated that chemical/biological releases and sabotage were considered to be primary threats. Fewer than 10% reported that radiological and cyber crimes were considered to be primary threats.

Multimodal Agencies		Bus Agencies	
Explosives (100%)	Radiological (8%)	Explosives (86%)	Radiological (5%)
Chemical (92%)	Cyber crimes (8%)	Chemical (14%)	Cyber crimes (5%)
Biological (92%)	Hijackings (85%)	Biological (14%)	Hijackings (95%)
Sabotage (77%)	Shootings (85%)	Sabotage (68%)	Shootings (91%)

Performance Measures (Q2–Q3, 17 responses)

Agencies were asked to list the security performance measures being used. Most agencies (82%) reported that they do not use performance measures. Of the agencies that did, they used crimes per 100,000 passengers; crimes per 100,000 unlinked trips (one agency); security personnel per 1 million unlinked passenger trips; and percent of frontline personnel who have completed transit security training.

Attributes of Perpetrators (Q4–Q5)

These questions did not yield many responses.

Number of Threats/Incidents and Trends for These Threats/Incidents (Q6–Q8)

These questions did not yield many responses. These responses included the following:

Sabotage:

One commuter rail system reported that many tie clips had been removed from the rail infrastructure in 2006. The same system had experienced tampering with rail signals (5 instances in 2000 vs. 10 in 2006), and tampering with electronic message sign (5 instances in 2000 vs. 10 in 2006).

Bomb threat:

A subject boarded a bus with a black bag in March 2006 and announced he was going to blow up the bus; no injuries occurred.

Suspicious bags periodically left at a transportation center required evacuation. No bombs were found.

Cyber Security, Trends, and Attributes of Perpetrators (Q9–Q11)

These questions did not yield many responses.

Reports of Suspicious Activity (Q12, 22 responses)

Changes in suspicious activity reports are shown below:

	Increase	Decrease	No change
In the past decade (since 1997)	60%	0%	40%
Since September 11, 2001	86%	0%	14%
In the past two years	9%	48%	43%

System Security Data and Analysis (Q13)

a) Security Data Used for Security Planning (33 responses): The security data collected in addition to Part I and Part II crimes include threats, suspicious activity, persons, and items; results of threat and vulnerability assessments; number of security personnel by location; the number of security checks by location and average response time of security personnel; ingress and egress at all facilities; calls for service data by location; training data; location of transit centers; number of vehicles; contact information for personnel; public comments; accident data; and landscaping information.

b) Sources of Data on Offenses Already Listed in the Survey (33 responses):

System reports (87%)
 Police reports (73%)
 Other (0%)

c) Sources of Data on Other Security Matters (33 responses):

System reports (87%)
 Police reports (70%)
 Other: Online news (3%)

d) Crime Mapping, Trend Analysis, or Other Data Analysis (12 responses):

Crime trend analyses and crime trend analyses by location (75%); some report that they use this information for resource allocation purposes.
 Crime mapping (25%)
 Threat/vulnerability analysis (8%)

e) Data-related issues or concerns (11 responses)

The following data-related issues or concerns were identified by the respondents:

- Notification and documentation on all relevant incidents from frontline personnel
- Development of security metrics
- Development of a more consistent way to compare crime and security incidents
- Creation of more accurate data (e.g., data can be incorrectly categorized)
- Combination of safety and security data for analysis purposes
- Elimination of transit security funding from the federal government

Changes since September 11, 2001 (Q14a–h, 33 responses)

Post 9/11:	Increase	Decrease	No change	Unknown
Patronage?	33%	7%	40%	20%
Offenses against passengers?	20%	0%	53%	27%
Offenses against workers?	13%	0%	73%	13%
Passenger complaints of violence or potential violence?	33%	7%	53%	7%
Passenger complaints of excessive security?	0%	7%	53%	40%
Passenger requests for increased protection?	40%	0%	47%	13%
Worker days lost as a result of violence-related incidents?	13%	0%	67%	20%
Violence-related legal actions?	7%	0%	60%	33%

Major Post-9/11 Changes in Security Practices: (Q14-second part, 32 responses)

The majority of responding agencies (91%) reported implementing Transit Watch or a similar employee and passenger outreach program and increased security training for frontline employees and counterterrorism training for their security personnel. Many (75%) reported increasing the number (or hours) of security personnel; some (53%) reported adding personnel to locations where there were none—patrols onboard transit vehicles and adding access control to bus depots and rail yards and other transit facilities; a few reported initiation of undercover efforts. Many agencies reported undergoing threat and vulnerability assessments and receiving intelligence information from federal agencies (66%); some agencies reported engaging in local and regional counterterrorism committees, and intelligence information-sharing with local responders and neighboring transit agencies. A few agencies reported a change from contract security to an in-house police force. Other agencies reported using CPTED (Crime Prevention through Environmental Design) techniques—lighting, surveillance/video, video deployment within buses, access control, fencing, and landscaping—and CPTED in planning, design, construction, operations, and disposal phases; configuration management; explosives detection canine teams, mandatory identification (ID) badges for employees; review and revisions to their emergency plans and operating procedures; Memorandums of Understanding with local law enforcement; initiation of undercover assignments; participation in drills; hiring officers dedicated to cyber security; advisory system based on the Homeland Security Advisory System; increased regional collaboration; designation of Sensitive Security Information; use of audio technology; and heightened sense of awareness of suspicious activity and higher likelihood of reporting it.

Current Security Investments and Impacts (Q15, 33 responses)

- a) Transit agencies reported making medium to high investments in the following areas:

- Technology (85%)
- Security Staff (39%)
- Employee Training (85%)
- Customer Outreach and Education (82%)
- Design (CPTED)/Situational Crime Prevention (91%)
- Other: Interaction with Local Public Safety Agencies (3%)

- b) In terms of the impact that prior security investments have had, practically all agencies reported that security investments have had a positive impact on crime mitigation, terrorist deterrence and detection capabilities, and the public/passenger perception of security. Agencies also reported that 9/11 attacks combined with their public outreach efforts raised passenger and employee awareness, improved employee preparedness, and increased security in terms of both deterrence and detection. Some agencies reported results of specific strategies, such as a drop in vehicular burglaries and theft after passenger education efforts about not leaving valuables in vehicles. Other agencies reported a marked decrease in crime after implementing increased surveillance of transit facilities.

Security Personnel (Q16)

a) Type of Security Enforcement (25 responses; 10 multimodal, 15 bus)

	Multimodal*	Bus*
1. Full-time Sworn Officers: System Employees	73%	33%
2. Full-time Sworn Officers: Contractors	2%	26%
3. Full-time Non-Sworn Officers: System Employees	16%	12%
4. Full-time Non-Sworn Officers: Contractors	2%	15%
5. Part-time Sworn Officers: System Employees	3%	5%
6. Part-time Sworn Officers: Contractors	4%	9%
7. Part-time Non-Sworn Officers: System Employees	0%	0%
8. Part-time Non-Sworn Officers: Contractors	0%	0%

*Percents shown are the percent of the total security personnel reported by responding agencies.

b) Post-9/11 Increase in Security Staff Hours (18 responses; 9 multimodal, 9 bus)

All multimodal responding agencies reported that they have moderately or significantly increased either the number of their security personnel or security staff hours after 9/11. One-third of bus agencies reported that they had not altered their security staff size or hours. The rest had increased either the number of their security personnel or security staff hours after 9/11 by a small or moderate percentage.

Security Measures

Survey respondents were asked the purpose(s) for which measures had been implemented—crime, terrorism, and/or quality of life. For all measures, 73% of respondents reported that crime reduction was the purpose, 52% indicated counterterrorism, and 49% indicated improvement of quality of life. Crime reduction was a major objective for all of these measures. Responses by category ranged from 58% to 86% with access control and surveillance/inspection receiving the highest percentages of responses. For counterterrorism, the responses were mixed—ranging from 25% (transit vehicle design) to 75% (surveillance/inspection). For quality of life, the responses ranged from transit vehicle design (31%) to communications (65%).

	Crime	Terrorism	Quality of Life
Access Control	86%	54%	36%
CPTED	64%	32%	55%
Transit Vehicle Design	68%	25%	31%
Surveillance/Inspection	83%	75%	46%
Operational Strategies	81%	44%	50%
Technology	58%	67%	58%
Communications	70%	55%	65%
<u>All (Wtd. Avg.)</u>	<u>73%</u>	<u>52%</u>	<u>49%</u>

Years of deployment: Only about half of those who had responded to these questions indicated the year or years of deployment, but those who did respond stated that some of the measures had been implemented long before 2001, while others had been recently implemented.

Access Control (Q17, 22 responses)

Transit agencies reported having admission control using encoded cards, manual verification, memorized code, mechanical lock, and/or electronic locks. No agency reported having a biometric admission control

system in place. Fencing and gates used by agencies were mechanical, electronic without an alarm, or electronic with an alarm. Agencies also used explosive detectors, intrusion sensors, random ID checks, vehicle access control, and parking measures and vehicle barriers. Responses were evenly distributed among these access control measures.

CPTED/Situational Crime Prevention (SCP) (Q18, 22 responses)

Most (91%) respondents employed internal design/configuration and lighting to enhance security; 32% indicated that site selection/building placement and 27% indicated that physical or natural barriers were used.

Transit Vehicle Design (Q19, 16 responses)

Transit vehicle design measures are typically considered to be a subset of CPTED/SCP measures. The majority of respondents, 87%, stated that public address systems were used in their systems, 69% stated that their system used a silent alarm and/or panic button, and 25% stated that their system used a silent alarm and/or panic button with AVL (Automatic Vehicle Location). The remainder was distributed among the other design measures: 19%, enhancement of visibility; 6%, transit operator compartment; and 6%, vehicle access control. They were implemented over a wide range of years starting from the pre-1970s to the present.

Surveillance/Inspection (Q20, 24 responses)

Closed-circuit television (CCTVs) with recorders was the surveillance/inspection measure used by 92% of responding agencies (a few agencies reported using CCTVs without recorders); 92% also reported that they used undercover or plainclothes officers; 37% conduct roving patrols without canine inspections and 17% use roving patrols with canine inspections; and 29% of agencies practice behavioral assessment by transit staff or security staff. Other respondents reported that they practice random sweeps; conduct explosives or narcotics canine inspections; employ fare checkers; and perform manual, visual, or electronic inspections of persons/baggage.

Operational Strategies (Q21, 16 responses)

Operational strategies used by transit agencies were as follows:

- Fleet Management/Vehicle Tracking
- Inventory Control
- Limiting Station Access
- Modification of Dispatcher Responsibilities
- Modifying Pre-Trip Inspections
- Modifying Hours of Service
- Parking Lot, Vehicle Flow/Placement Re-Configuration
- Strategic Location of Bus Stops

The responses were evenly distributed among the strategies.

Technology (Q22, 24 responses)

Public address system and radio communications for staff were used by 92% of the respondents; 79% of agencies used CCTV either for surveillance or for recording incidents/passenger traffic; 58% also had an emergency alert system for employees. The remainder of the measures received fewer than 10 responses.

Surveillance or Inspection measures used by transit agencies were as follows:

- Automatic Train Control/Monitoring
- AVL
- Biological Detector
- CCTV: for surveillance
- CCTV: for recording incidents, passenger traffic
- Chemical Detector
- Emergency Alert for Employees
- Emergency Phones/Call Boxes for Passengers
- Explosives Detector: Portable, Tabletop
- Intelligent Video to ID Suspicious Activity
- Intrusion Sensors and Alarms
- Public Address System
- Radio Communications for Staff

Communications Security (Q23, 20 responses)

95% of responding agencies reported that they have network security; 90% have power supply backup; and 70% have redundant communications systems. One respondent implemented access control for their dispatch control center.

Security and Policing Management (Q24)

a) Budgeting (Too few responses)

b) Human Resources Practices (22 responses)

100% of responding agencies reported that they have implemented background checks on new hires; 50% reported they have updated their performance appraisal system since September 11. A few agencies reported initiating fingerprinting of employees since September 11. Others reported that they already had these practices before September 11.

c) Security Planning (24 responses; 13 multimodal, 11 bus)

100% of responding multimodal agencies and the majority of all responding agencies indicated that they have up-to-date security-related plans. Of bus agencies, 18% indicated that they do not have an up-to-date security plan or an up-to-date Continuity of Operations Plan; 9% indicated that they do not have an up-to-date emergency plan or incident response plan; 9% also indicated that they have not yet integrated an incident command system into their plans.

d) Assault Mitigation Techniques (22 responses)

100% of responding agencies reported that they practice some type of technique to mitigate conflict; 100% reported that they have passenger codes of conduct and presence of security or transit personnel to mitigate assaults. Half of responding agencies indicated that their personnel use verbal techniques and a much smaller percentage, 14%, indicated that they use nonverbal techniques to resolve and mitigate conflicts; only two of the responding agencies indicated that they use restraining techniques for conflict mitigation. Nearly half, 45%, of responding agencies indicated that they practice community policing and have roving security patrols; other agencies (41%) indicated that they provide specific training in conflict resolution techniques; 18% of the agencies responded that they participate in school outreach efforts to discourage juvenile offenders; a few agencies responded that cameras installed for other purposes also act as a deterrent to conflict escalation.

Passenger Outreach, Education/Training, and Awareness Programs (excluding employee training) (Q25, 35 responses):

Transit Watch Program	77%
Crime Prevention Program	51%
Toll-Free Number	11%
Evacuation Instructions	48%
Other	

Training (Q26, 195 responses from 39 agencies)

41% of training occurred in-house, 38% was through NTI, 5% through APTA, 5% through TSI, and 10% through other sources. 76% of training was delivered using the classroom method, 23% through a workshop, and the rest was a combination of video/DVD, interactive CD or online training without an instructor. The audience was evenly distributed among frontline personnel, security personnel, and supervisory personnel. The duration for 69% of the training classes was between 1 and 4 hours, while the remainder was 8 hours or more. The following classes titles were mentioned by the respondents:

- Transit Watch
- System Security Awareness for Transit Employees
- System Security of Operators
- Security Awareness Train-the-Trainer
- Recognizing Terrorist Activity
- Terrorist Recognition and Response
- Strategic Counterterrorism for Transit Managers
- The Mark (Video/DVD)
- Other NTI Transit Security DVDs
- Behavior Recognition Train-the-Trainer
- Incident Response to Terrorists
- Terrorism Awareness
- Transit Terrorist Tools and Tactics
- Transit System Security and Design Review
- National Incident Management System (NIMS) Incident Command System (ICS) 100, 200, 300, 400, 700, and 800
- Homicide/Suicide Bomber
- Domestic Preparedness
- Emergency Management
- Transit Emphasis Inc. Management Service
- Transit Vehicle Emergencies
- Crime Prevention
- CPTED
- Firearms, arrest control technique, taser, baton, pepper spray
- Peace Officers Standards and Training (POST)
- First Aid/CPR
- Customer Service/Customer Relations

Drills and Exercises (Q27, 22 responses)

- 82% of responding agencies reported that they conduct 1–2 interagency drills/exercises per year; 9% reported that they do not conduct any; and the rest reported that they conduct more than 1–2 per year.
- 82% reported that they conduct one or two intra-agency drills/exercises per year; 9% reported that they do not conduct any; and the rest reported that they conduct more than one or two per year.
- 23% reported that they conduct one or two simulations or tabletop exercises/workshops per year; 41% reported that they do not conduct any; and the rest reported that they conduct more than one or two per year.

Covert Testing (Q28, 16 responses)

Most agencies (81%) responded that they do not perform any type of covert testing of their security personnel or frontline workers. A few agencies reported that they do perform covert observations of operators with respect to safety and security, including pretrip inspections along with passenger relations, Americans with Disabilities Act (ADA) compliance and on-time performance. One agency reported that they perform hostage drills on buses once a year; another reported that night-time entry into transit facilities is tested; and another reported that transit vehicle panel/compartment door access is checked randomly to verify adherence to standard operating procedure.

Cooperative Relationships (Q29, 26 responses)

100% of responding agencies reported that they have cooperative relationships with external agencies and a majority (85%) reported that they have cooperative relationships with other units within the agency itself; some (42%) reported that they engage in intelligence-sharing.

Cyber Security (Q30, 16 responses)

100% of responding agencies reported that they have a firewall for their computer network; most (94%) have access control using passwords and only two have access control using biometric technology. Other measures that were reported by agencies included access control to the server room, power backups and redundancy, and constant backup of data.

Effective Security and Policing Measures (Q31, 37 responses)**The Five Most Effective Counterterrorism Measures Named by Respondents**

1. Transit Police Officers/Security Personnel Patrols/Sweeps (90%)
2. Security Training for Transit Employees and Police/Security Personnel (88%)
3. Video Technology (85%)
4. Public Education/Transit Watch and Outreach (80%)
5. Intelligence Information (60%)

Other effective counterterrorism measures mentioned included access control, perimeter security, presence of transit employees, fare checking, plainclothes officers, threat detectors, local counterterrorism groups, Surface Transportation Joint Operation Network to share operations with local agencies, passenger security inspections, signage, station design, lighting, building and facility design, interagency/interoperable communications, pretrip inspections, HSAS, drills, and transit police dispatch linkage to statewide police and emergency communications.

The Five Most Effective Crime Prevention Measures Named by Respondents

1. Transit Police Officers or Security Personnel Patrols/Sweeps (90%)
2. Plainclothes Officers/Undercover Vehicles (83%)
3. Video Technology (74%)
4. Presence of Transit Employees (60%)
5. Lighting and Visibility (60%)

Other effective crime prevention measures mentioned included the enforcement of passenger codes of conduct, officer training, driver training, fare checking, perimeter security, access control, data collection/analysis, school outreach efforts, radio communications, bait car program/undercover cars, public education at park-and-ride facilities, employee reward for reporting crimes, intelligence-sharing with local law enforcement, employee ID, and canine inspections.

Evaluations of Security Interventions/Measures (Q32, 17 responses)

Evaluations of security interventions or measures are performed by 82% of the respondents by measuring their impact on the problem at hand. Specific testing and evaluations of new equipment were also performed.

Innovative Practices or Measures (Q33, 26 responses)

Following are the responses to the question on measures being practiced in an innovative way or any innovations in policy, program, or research:

- Passenger Security Inspections—Behavioral Assessment
- Passenger Security Inspections—Passenger Bag Inspections
- Passenger Security Inspections—Explosives Detection Canine Teams
- Training for first responders provided by the transit agency
- Development of Tactical Operations Guide to train first responders
- Interactive Crime Statistics Map
- Use of administrative employees to augment officers at rail stations
- Video cameras linked to motion detection
- Video cameras linked to alarms
- School outreach, with the transit system considered to be an extension of the school so that school disciplinary rules apply to the students using the system
- Use of blast mitigating trash receptacles
- Use of clear trash receptacles
- Emergency response team
- Placement of report cards with crime statistics on vehicles in park and ride facilities
- Gang violence training for bus drivers
- Bus drivers training to assist the public when necessary
- Advertised presence of undercover officers
- None (38%)

Obstacles in Security and Policing Management (Q34, 35 responses)

The greatest obstacle in security and policing management that was reported by survey respondents was by far the lack of resources to implement desired security measures.

- Lack of resources (91%)
- Lack of customer support (40%)
- Lack of qualified workers or technical expertise (31%)
- Lack of management support (6%)
- Lack of customer support (9%)
- Lack of tested, market-ready technology solutions (6%)
- Other responses included the following:
 - Intelligence received is often too general to be of specific use to their system
 - Motivation of transit employees in implementing security practices
 - Motivation of officers in performing ordinary crime assignments, because antiterrorism assignments are viewed as being more prestigious and desirable than ordinary crime-related assignments
 - Unionized transit workers are reported to be concerned about the increased time needed to perform security-related tasks
 - Two transit agencies expressed the need for the development of a Memorandum of Understanding with TSA regarding the federal Visible Intermodal Prevention and Response (VIPR) program. Currently, confusion as to the composition of the VIPR team and their responsibilities diminishes the effectiveness of the program within the agencies.

Abbreviations 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