

## Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

### DETAILS

---

104 pages | 8.5 x 11 | PAPERBACK

ISBN 978-0-309-30881-6 | DOI 10.17226/22115

### AUTHORS

---

Ernest "Ron" Frazier

BUY THIS BOOK

FIND RELATED TITLES

### Visit the National Academies Press at [NAP.edu](http://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.

**TRANSIT COOPERATIVE RESEARCH PROGRAM**

---

---

**TCRP REPORT 180**

---

---

**Policing and Security Practices  
for Small- and Medium-Sized  
Public Transit Systems**

**Ernest “Ron” Frazier, Sr.**

COUNTERMEASURES ASSESSMENT AND SECURITY EXPERTS, LLC  
New Castle, DE

*Subject Areas*

Public Transportation • Security and Emergencies

---

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

---

**TRANSPORTATION RESEARCH BOARD**

WASHINGTON, D.C.

2015

[www.TRB.org](http://www.TRB.org)

## TRANSIT COOPERATIVE RESEARCH PROGRAM

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

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

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

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

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

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

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

## TCRP REPORT 180

Project F-18  
ISSN 1073-4872  
ISBN 978-0-309-30881-6

© 2015 National Academy of Sciences. All rights reserved.

### COPYRIGHT INFORMATION

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.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by the Transportation Research Board and approved by the Governing Board of the National Research Council.

The opinions and conclusions expressed or implied in this report are those of the researchers who performed the research and are not necessarily those of the Transportation Research Board, the National Research Council, or the program sponsors.

The Transportation Research Board of the National Academies, the National Research Council, and the sponsors 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 object of the report.

*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. Upon 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. C. D. Mote, Jr., 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, upon its own initiative, to identify issues of medical care, research, and education. Dr. Victor J. Dzau 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. C. D. Mote, Jr., 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](http://www.TRB.org)**

**[www.national-academies.org](http://www.national-academies.org)**

# COOPERATIVE RESEARCH PROGRAMS

## **CRP STAFF FOR TCRP REPORT 180**

**Christopher W. Jenks**, *Director, Cooperative Research Programs*

**Stephan A. Parker**, *Senior Program Officer*

**Megan Chamberlain**, *Senior Program Assistant*

**Eileen P. Delaney**, *Director of Publications*

**Scott E. Hitchcock**, *Editor*

## **TCRP PROJECT F-18 PANEL**

### **Field of Human Resources**

**Jeanne Krieg**, *Eastern Contra Costa Transit Authority, Antioch, CA (Chair)*

**William C. Fleming**, *Massachusetts Bay Transportation Authority Police, Braintree, MA*

**Aston T. Greene**, *Metropolitan Atlanta Rapid Transit Authority (MARTA) Police Dept., Ellenwood, GA*

**Bobby J. Griffin**, *Griffin and Associates, Flower Mound, TX*

**Glenn Hansen**, *Howard County (MD) Police Department, Ellicott City, MD*

**Evangelos I. Kaisar**, *Florida Atlantic University, Boca Raton, FL*

**Sue F. Knapp**, *KFH Group, Inc., Bethesda, MD*

**Keith Bryan Leaird**, *Concord, NC*

**Nancy Norris**, *TransIT Services of Frederick County, Frederick, MD*

**Richard Gerhart**, *FTA Liaison*

**Patricia Monahan**, *National Rural Transit Assistance Program Liaison*

**Stephen J. Andrie**, *TRB Liaison*

**Jennifer L. Weeks**, *TRB Liaison*

## **AUTHOR ACKNOWLEDGMENTS**

The research project, TCRP Project F-18, “Policing and Security Practices for Small- and Medium-Sized Public Transit Agencies” came about because transit industry practitioners accurately perceived a distinction in the security risk, profile, and needs of smaller agencies. As observed in the commentary of the TCRP Project F-18 project panel, post 9/11 government and industry security risk reduction prioritization was focused toward the “top 100 transit agencies.” While this approach was most appropriate and consistent with concepts of risk management from an industry perspective, there was additional work to be done to assist other smaller agencies to define their specific security conditions and requirements. The author acknowledges his appreciation for the efforts and energy undertaken by the F-18 subject matter expert panel to bring this project to fruition.

  
FOREWORD

By **Stephan A. Parker**

Staff Officer

Transportation Research Board

*TCRP Report 180: Policing and Security Practices for Small- and Medium-Sized Public Transit Systems* broadens the current state of practice and identifies and responds to the specific challenges and issues associated with the security of small- and medium-sized transit agencies. Following the five stages of protection activity (prevention, mitigation, preparedness, response, and recovery), the report provides baseline options and identifies potential security countermeasures that could be deployed by both small- and medium-sized transit agencies. This information is contained in numerous tables including specific information about (1) existing countermeasures in place at small- and medium-sized agencies, (2) an exhaustive and scalable list of prospective countermeasures that are available for deployment, and (3) spotlighted best practices that transit agencies are using to reduce security-related risks. For the purpose of this report, a small transit agency is defined as serving a population of less than 50,000 people whereas a medium agency serves a population of between 50,000 and 100,000 people. *TCRP Report 180* is a reference document, intended primarily for transit agency personnel without a security background whose work requires them to address, perform, or supervise security activities as a part of their overall job responsibilities.

---

Managers of small- and medium-sized transit systems considering enhancements to or establishment of formal security programs want to know the following: (1) Are my peers doing formal security needs assessments? (2) What practical security measures are in use? (3) What practical security measures are recommended? (4) How does one set a security budget? (5) How does one justify a security budget?

In the research effort led by Countermeasures Assessment & Security Experts, LLC, 180 small- and medium-sized public transit agencies from across the United States were surveyed about their assets, identified and historic security risks, as well as physical and operational countermeasures. Questions about assets included size of fleet by mode, physical structures (e.g., office buildings, maintenance garages), infrastructure (e.g., bridges, tunnels), and security personnel. For comparative purposes, 106 large agencies were also surveyed. Risk questions pertained to the incidence of homeland security-related events, felony and misdemeanor crimes, and quality of life offenses committed within the past year. Agencies were also asked to report on incidents of suspicious activity, packages, or persons, bomb threats, and evacuations based on these suspicious circumstances. In terms of countermeasures, agencies were asked about access control, barriers, berms, surveillance equipment, security public awareness campaigns, and security planning.

The research conducted supports an initial hypothesis that there are significant differences between the security risks, needs, and issues facing smaller agencies when compared

to those of large metropolitan transit systems; police and security problems at small- and medium-sized systems occur with much less frequency or magnitude of severity. A survey of large, medium, and small transit agencies disclosed that the smaller the system, the less probable it is for the agency to experience significant levels of crime or disorder. Homeland security- or terrorism-related threats rarely occur on smaller systems. However, the potential for serious crime and major security events always exists, even for these smaller systems.

Irrespective of the size of the agency, transit security problems fall into the following categories: (1) passenger security, (2) employee security, (3) revenue security, (4) transit equipment and property protection, (5) fraud, and (6) homeland security-related threats and vulnerabilities. The highest consequence security issue that small- and medium-sized transit agencies must confront on a daily basis is the potential for employees to be assaulted while performing their duties. Although lesser crimes or violations may occur more frequently, by and large the most significant criminal threat outside of homicide that the transit agency will face is as an aggravated assault committed against an employee.

This project created two products that are available on the TRB website ([www.TRB.org](http://www.TRB.org)) by searching for “TCRP Report 180”: (1) this report, and (2) a PowerPoint presentation describing the entire project.



# CONTENTS

1	<b>Summary</b>
3	<b>Chapter 1 Security Risk Management and Assessment Processes</b>
3	Risk
3	Risk Management
5	Security Risk
5	Homeland Defense/Homeland Security—The Risk of Terrorist Attack
7	Felony or Misdemeanor Crime—The Risk of Crime and Criminal Activity
8	Violent Crime
8	Overview
9	Property Crime
9	Overview
10	Minor Offenses and Disorder
11	Perceptions of a Lack of Security
12	<b>Chapter 2 Small- and Medium-Sized Transit Agency Security Environment</b>
13	Small-Sized Agencies
13	Medium-Sized Agencies
17	<b>Chapter 3 Transit Agency Security Risk Profiles</b>
19	Security Risk Profile—Small-Sized Transit Agencies
21	Security Risk Profile—Medium-Sized Transit Agencies
23	Relative Risk Profile Comparative Findings/Summary Section
24	Countermeasures Deployment Comparative Findings/Agency Utilization Rates
25	<b>Chapter 4 Crime, Statistics, and Reporting Procedures</b>
25	Crime and Security Data
27	Crime Rates in Transit
30	<b>Chapter 5 Transit Crime and Security Problems</b>
30	Passenger Security
30	Homicide
31	Aggravated Assault, Simple Assault, and Harassment
31	Robbery
31	Rape and Sex Offenses
32	Employee Security
32	Type 1 Violence
33	Type 2 Violence
33	Homicide
34	Aggravated Assault, Simple Assault, and Harassment
37	Revenue Security



37	Transit Equipment and Property Protection
37	Internal Theft
39	External Theft
40	Vandalism and Graffiti
43	Fraud Prevention
43	Homeland Security Issues
<b>45</b>	<b>Chapter 6 Police and Security Staffing</b>
45	Security Forces
<b>52</b>	<b>Chapter 7 Security Countermeasures</b>
53	Protecting People On Board
54	On-Board Vehicle Countermeasures
54	Prevention
55	Deterrence
55	Response
58	Other On-Board Vehicle Incidents
59	Protecting People at Bus Stops
61	Protecting Transit Properties
62	Vehicles and Conveyances
65	Other Transit Property
65	Buildings and Other Facilities
<b>74</b>	<b>Chapter 8 Security Plan Implementation and Management</b>
79	Establish Priorities
80	Organization, Roles, and Responsibilities
81	Countermeasures and Strategies
81	Plan Maintenance
<b>83</b>	<b>Chapter 9 Conclusions</b>
83	Key Points Summary
83	Risk Factors
83	Small- and Medium-Sized Agencies Security Risk Profile
84	Homeland Security
84	Crime and Disorder
85	Workplace Violence
86	Security Countermeasures
<b>88</b>	<b>References</b>
<b>91</b>	<b>Appendix A Agencies Participating in the F-18 Study of Agency Size—Large, Medium, Small</b>

  
S U M M A R Y

# Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

TCRP Project F-18, “Policing and Security Practices for Small and Medium-Sized Public Transit Agencies” has been directed toward broadening the current state of practice and identifying and responding to the specific challenges and issues associated with the security of small- and medium-sized transit agencies. For the purpose of this report, a small transit agency is defined as serving a population of less than 50,000 people whereas a medium agency serves a population of between 50,000 and 200,000 people. This is an introductory reference document with an anticipated primary user group of transit agency personnel without a security background whose work requires them to address, perform, or supervise security activities as a part of their overall job responsibilities.

The F-18 research supports an initial hypothesis that there are significant differences between the security risks, needs, and issues facing smaller agencies when compared to those of large metropolitan transit systems. Police and security problems at small- and medium-sized systems occur with much less frequency or magnitude of severity. A survey of large, medium, and small transit agencies revealed that the smaller the system the less probable it is for the agency to experience significant levels of crime or disorder. Similarly, homeland security- or terrorism-related threats rarely occur on smaller systems. However, serious crime, including violent crime does occur infrequently, on smaller systems. There is also the potential for major security events or crises.

Commensurate with the reduced risk that smaller agencies are facing, small- and medium-sized agencies spend less time and resources on security, employ fewer dedicated security personnel—87% of small-sized transit agencies and 83% of medium-sized transit agencies report having no dedicated security staff—and depend to a much higher degree on obtaining assistance from local area police and occasionally contract security forces. Fewer agencies maintain security plans or deploy security countermeasures to minimize risk, with 91% of small agencies indicating no budget or budget under \$25,000 set aside for security. Forty-four percent of medium-sized agencies have no security budget and an additional 34% spend less than \$25,000 per year.

The chapters that follow provide small- and medium-sized agencies with important information about the security risks that are typically present for transit agencies of similar size and operations. The risk of terrorism and homeland security, crime problems, and order-maintenance issues are all discussed in extensive detail with a concentration on major areas of concern for surface transportation operators. Countermeasures, plans, and strategies are then described for each of the identified areas of concern.

Chapter 1 starts with an overview of risk management and distinguishes security risk from the other types of hazard and safety concerns that may impact smaller transit agencies.

## 2 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

There is an overview of security and crime occurring in the United States followed by a description of commonly reported incidents occurring in public transit systems.

Chapter 2 depicts the critical assets and infrastructure of a typical large, medium, and small transit system. As disclosed in a survey conducted by the research team small- and medium-sized transit agencies generally fall into the category of single service bus-only, or van transportation providers.

Chapter 3 presents further survey information about small- and medium-sized agencies summarized into comparative tables. For the purpose of this report, a small transit agency is defined as serving a population of less than 50,000 people whereas a medium agency serves a population of between 50,000 and 200,000 people. Data obtained from representative agencies is included in individualized small- and medium-sized agency profiles that document (1) agency critical assets, (2) terrorism and homeland security incident occurrences, (3) crime rates for violent offenses as well as lesser property crimes, (4) quality-of-life problems, and (5) countermeasures and other security measures commonly in use to reduce security vulnerabilities. Relative risk analysis is also categorized for each agency type.

Chapter 4 provides data tables that compare public transit crime statistics from 30 years ago with current crime rates. There is also a discussion about reporting procedures and gaps in information caused by continuing difficulties in data collection and analysis.

Detailed information about security problems specific to small- and medium-sized transit agencies is provided in Chapter 5. Subject areas of coverage include (1) passenger security, (2) employee security, (3) revenue security, (4) transit equipment and property protection, (5) fraud, and (6) homeland security-related threats and vulnerabilities. An in-depth description of topics such as robbery, aggravated assault against transit operators, fare evasion, and vandalism of transit properties is highlighted.

Chapter 6 begins the discussion of security countermeasures. Options associated with police and security staffing are described along with security force planning models and tools for use by small- and medium-sized transit agencies.

In Chapter 7, fundamental aspects of security strategy and countermeasures directly focused toward the specific security risks of small- and medium-sized agencies are discussed in the context of the profiled and identified security problems, issues, and vulnerabilities. These identified security risks include ensuring the protection of (1) vehicles in transit on highways, rural and suburban city, borough, and township streets, or other roadways; (2) infrastructure such as unstaffed bus shelters or bus stops, vehicle storage depots, bus stations, and maintenance facilities necessary to support these conveyances; (3) employees who operate the conveyances; (4) administrative and management staff; and (5) the passengers who use the agency's transportation services.

Chapter 8 examines security planning objectives and highlights the core components or elements needed to ensure that a comprehensive plan is developed. The survey of small- and medium-sized transit agencies confirmed that just under half of small and two-thirds of medium-sized agencies have previously conducted risk assessments and developed security plans. To assist readers of this report, the following security planning tools are identified and referenced, including (1) Transportation Security Administration (TSA)/Federal Transit Administration (FTA) Security and Emergency Management Action Items for Transit Agencies; (2) TSA Baseline Assessment and Security Enhancement (BASE) Program; (3) The Public Transportation System Security and Emergency Preparedness Planning Guide; (4) *TCRP Report 86: Public Transportation Security, Volume 10, Hazard and Security Plan Workshop: Instructor Guide*; and (5) APTA Recommended Practice Series for Security.

# Security Risk Management and Assessment Processes

## Risk

**Risk** in the broadest sense is defined as “the possibility of loss or injury.” When an asset or something of value is identified as “at risk” there is a presumption that the asset has been placed in a state or condition that creates or suggests the chance of loss or peril. *In the public transit environment the most significant assets are the passengers who use the system, the employees who deliver the transportation services, and indirect participants who interface with transit systems such as station vendors, other building tenants or occupants, delivery persons, or those with homes or businesses in proximity to transit facilities or infrastructure.*

All of these individuals through either a decision to use public transportation or indirectly through the formation of a common boundary with transit assets have been placed at some level of risk. In addition, based on common law precedent as well as statutory enactments in some cases, those individuals who choose to be passengers on public transit systems are owed a “duty of care” by the transportation operator or carrier. Under such circumstances when loss or injury occurs there is often a determination of greater liability to the injured party.

In addition to human assets, public transit agencies have an extensive range of property- or infrastructure-related assets as well as intrinsic or intangible assets such as goodwill. Transit vehicles—buses, trolleys, trains—are the most recognizable of transit’s infrastructure; however, there are also stations owned or operated by transit agencies, stops or shelters, office buildings, maintenance facilities, parking lots, information systems, communications huts, and other types of property used to support services.

The Department of Homeland Security (DHS) in the latest version of the *National Infrastructure Protection Plan* (DHS 2013) describes the 3 protection program areas for critical infrastructure—Physical, Cyber and Human. See Figure 1.1.

*Transit Security Design Considerations* (Rabkin 2004) published by the FTA further delineates public transit agency infrastructure and system assets. Note that “people” are at the center of the graphical representation. See Figure 1.2.

## Risk Management

**Risk Management** consists of those activities that a business or agency can take to resolve identified risks. The list of activities includes *risk avoidance*, accomplished by eliminating the source of the risk, *risk reduction* characterized by the implementation of actions that lower the risk to the agency, *risk spreading* through the distribution of risk across various program areas or activities, *risk transfer* by the use of insurance to cover costs that would be incurred as the result of a loss, and *risk acceptance*, which is necessarily based on the knowledgeable determination that a risk is best managed by taking no action at all. See Figure 1.3.

4 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

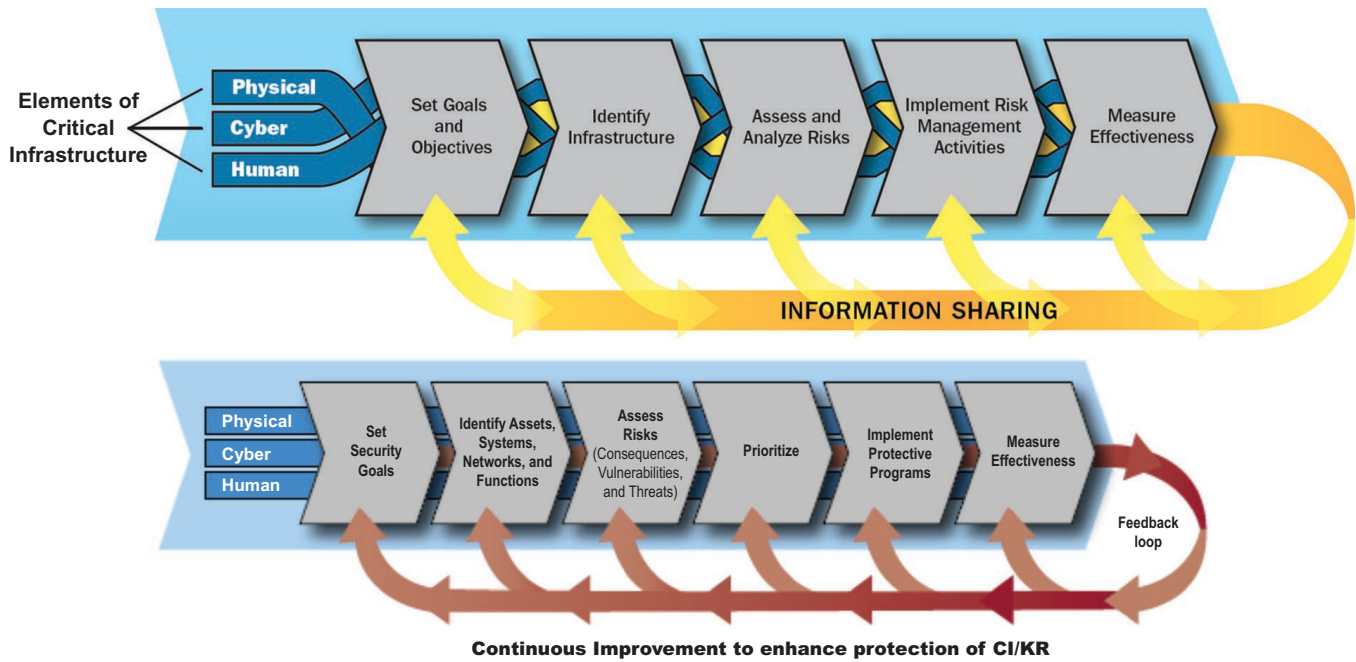


Figure 1.1. Protection program areas for critical infrastructure—Physical, Cyber and Human (DHS 2013).

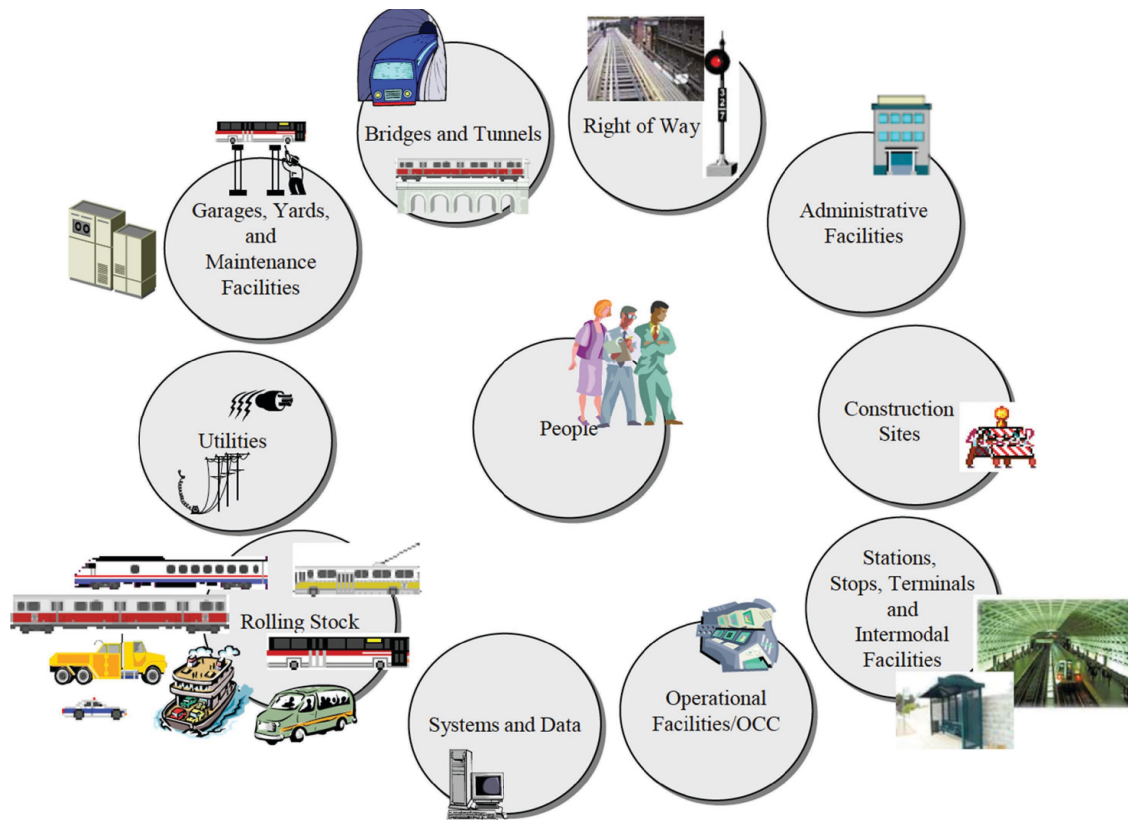
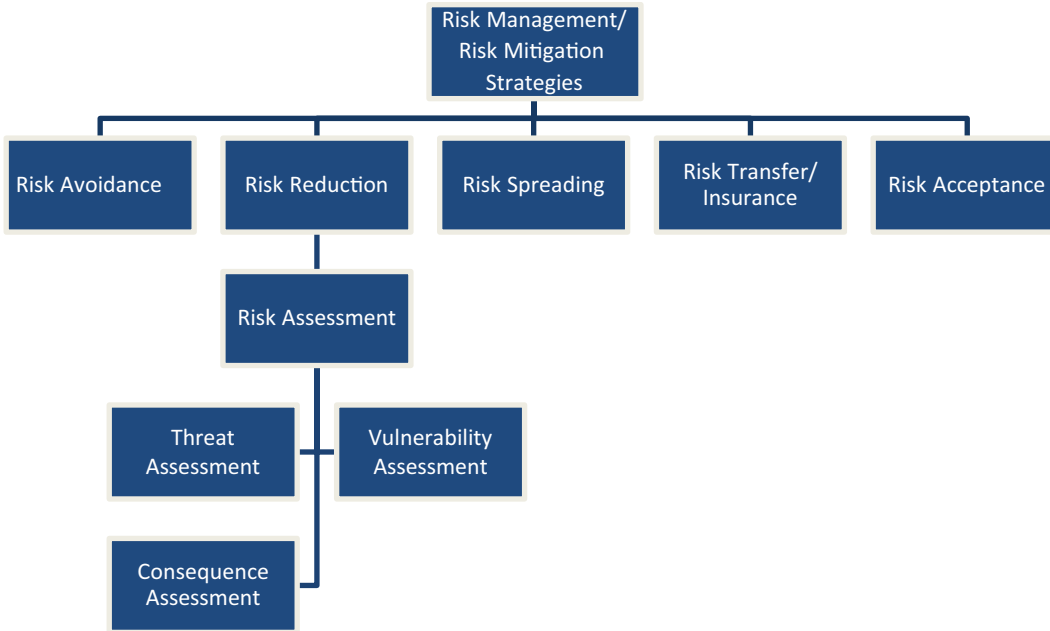


Figure 1.2. Public transit agency infrastructure assets (Rabkin 2004).



**Figure 1.3. Risk management/mitigation strategies.**

## Security Risk

**Security Risk** consists of the much narrower category of possible loss events that result from the intentional harmful acts of other persons. It requires an actor, motivation to do harm, and to constitute actual risk, there must be a capability or opportunity to accomplish the adverse act. The crime of robbery is a good example. For a robbery to be considered to have occurred there must be an actor with the intent to take something of value by force from a victim. Assume the robber has a gun and threatens to shoot the victim if he doesn't turn over his or her money. There is a criminal actor, the verbal threat to shoot indicates there is motivation to do harm, and the gun represents the capability to commit the act.

Comparatively, a much broader *safety*-related risk may consist of a potential accidental release of a chemical substance into the atmosphere or bad weather causing a hazardous condition such as icy roads. In such cases there was no intent by an individual to harm another.

Security risk is “threat based” as opposed to “hazard based.” *Avoiding, reducing and mitigating security risk at small- and medium-sized public transit agencies is the specific topic of this research.* Safety and security are both considered under the universal term “All Hazards.”

Public transit agencies should be aware of the following 3 types of security risks.

## Homeland Defense/Homeland Security—The Risk of Terrorist Attack

From a worldwide perspective, transportation assets moving by air, land, or sea have long been a primary target of focused attacks by hijackers, pirates, anarchists, or terrorists. Such attacks have occurred on virtually every inhabited continent: Asia, Europe, Africa, South America, Central America, North America; and in developed and developing nations including Japan, France, Spain, United Kingdom, Ethiopia, Israel, Egypt, Iraq, Lebanon, Libya, Somalia, South Africa, Soviet Union, India, Indonesia, Algeria, Venezuela, and the United States.

## 6 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

Specific to public transit, terrorist attacks have been launched directly against intercity and over-the-road buses, subways, elevated trains, passenger trains, trolleys, ferries, and other types of conveyances. Stations and depots have been targeted and right-of-way infrastructure including rail and highway bridges and tunnels have all been attacked and are considered by experts to be high-value attractive assets.

However, in the United States, public transit's increased focus on homeland security risk crystallized after the attacks of September 11th, 2001. In the 40 plus years prior to 2001, there were no major terror incidents or attacks on public transit assets in the United States. A few notable 20th century exceptions include the "Mad Bomber" and "Sunday Bomber" incidents in New York City. The "Mad Bomber" George Metesky placed over 30 bombs in locations such as Grand Central Station and the Paramount Theater; and the "Sunday Bomber" set off a series of bombs in New York City subways and ferries during Sundays and Holidays. There was also the intentional derailment of Amtrak's Sunset Limited in Hyder, AZ, in October 1995. A group calling itself the "Sons of Gestapo" left 3 notes at the scene claiming responsibility in retaliation for "Waco and Ruby Ridge." Although the case was never solved, this incident is often referred to as an early incidence of domestic terrorism against passenger rail.






In 2001, the TSA, was created under the Aviation and Transportation Security Act (ATSA). Under ATSA, TSA was given "*the primary federal role for security in all modes of transportation.*" Within a year and a half after the September 11th attacks, Congress passed the Homeland Security Act of 2003, a sweeping piece of legislation that established the DHS as a cabinet level department of the federal government. The responsibilities of the new department included "preventing terrorist attacks within the United States, reducing the vulnerability of the United States to terrorism at home, and minimizing the damage and assisting in the recovery from any attacks that may occur." In 2003 when the DHS was created, TSA transferred from U.S.DOT to the new department along with 21 other federal agencies.

The Homeland Security Act created the position of the Secretary of Homeland Security to be appointed by the president with the consent of the Senate. Whereas the Department of Defense works in the military sphere, DHS was dedicated to work in the civilian sphere to protect the United States within, at, and outside its borders.

As mentioned above, the establishment of DHS resulted in a massive reorganization of federal agencies. In total over 22 federal departments or agencies including FEMA, Secret Service, and the U.S. Coast Guard, TSA, and the Immigration and Naturalization Service were moved under the new department. With regards specifically to transportation, Title IV of the Act expressly created the Undersecretary for Border and Transportation Security (BTS) whose primary duties include (1) preventing the entry of terrorists and the instruments of terrorism into the United States; (2) *securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States*; (3) administering the immigration and naturalization laws of the United States, including the establishment of rules governing the granting of visas and other forms of permission to enter the United States to include individuals who are not citizens or lawful permanent residents; (4) ensuring the customs laws of the United States; and (5) ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce in carrying out these responsibilities.

TSA, in addition to carrying out its many responsibilities, provides timely and continuous intelligence information to public transit agencies, specifically as it pertains to threats of terrorism. Among other methods, TSA's Office of Intelligence and Analysis disseminates quarterly reports containing assessments regarding the risk of an attack. The following are excerpts from the unclassified/for official use only (U//FOUO) quarterly mass transit assessment covering June to September 2013:

(U//FOUO) The Transportation Security Administration's Office of Intelligence and Analysis (TSA-OIA) assesses terrorists will continue to view attacks on U.S. transportation systems as an effective means for inflicting economic and psychological damage on the United States. Violent extremists continue to attack

(U//FOUO)	Aviation	Mass Transit	Freight Rail	Highway	Pipeline
					
	<b>HIGH</b>	<b>MODERATE</b>	<b>LOW</b>	<b>LOW</b>	<b>LOW</b>

(U//FOUO) Individual Modal Threat Levels remain the same as reported in the first quarterly Multi-Modal Threat Assessment. 30463-06a

**Figure 1.4. Transit mode terrorist threat levels.**

the aviation, mass transit, highway, pipeline, and freight rail modes abroad. TSA-OIA is not aware of any attack planning against these modes in the Homeland.





(U//FOUO) TSA-OIA assesses with high confidence that the terrorist threat to the U.S. mass transit mode is moderate, based on current intelligence reporting and analysis of worldwide attacks and plots. [See Figure 1.4.]

(U//FOUO) TSA-OIA assesses the preferred terrorist tactics used against transportation systems in the Homeland are likely to be improvised explosive devices (IEDs) and armed assaults. Additional, but less frequently used, tactics that have been effective in recent attacks against transportation modes include improvised incendiary devices and arson. The graphic below [Figure 1.5] illustrates, for the period of this report, actual terrorist attacks on all transportation modes (in red) and preoperational information about possible future attack methods (in yellow).

### Felony or Misdemeanor Crime—The Risk of Crime and Criminal Activity

The nation’s mass transit systems and the people who use these systems are susceptible to the occurrence of felony (major) and misdemeanor crime, including both crimes against persons and crimes against property. However, the extent of the problem is difficult to measure or evaluate.

(U//FOUO) Tactics Used Against Transportation Modes Worldwide  
(16 Jun 2013 - 15 Sept 2013)

		IEDs	VBIEDs	Suicide Bomber	IEDs	Armed Assault	Arson	Sabotage	Kidnapping	Hijacking	MANPADS	Chemical	Cyber Exploitation	Cyber Attack
	Aviation/ Air Cargo	●				●			●		●			
	Highway	●	●	●		●		●						
	Mass Transit/ Freight Rail	●	●			●	●							
	Pipeline	●												

● Pre-operational information indicating possible future terrorist tactics      ● Attacks

The Jane's Terrorism and Insurgency Center Database, intelligence, and open source reporting.

(U//FOUO)

**Figure 1.5. Actual attacks on all transportation modes.**



## 8 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

State and local police agencies who are responsible for recording crime rates typically do not categorize crime incidents by industry sector, markets, or commodity. The FBI, the national repository for crime statistics, also cannot distinguish whether a criminal incident occurred inside a transit vehicle, on a city street, or in a shopping mall. Transportation-related crime is reported in a manner that is similar to that of all other crimes. As such, the statistics specific to mass transit become lost amidst the jurisdictional crime rates of a given location, city, county or state.

However, observation of the larger set of national crime statistics discloses that overall both violent and property crime in the United States is declining per capita.

### Violent Crime

*Violent Crime*—In the FBI’s Uniform Crime Reporting (UCR) Program, violent crime is composed of 4 offenses: *murder and non-negligent manslaughter, forcible rape, robbery, and aggravated assault*. Violent crimes are defined in the UCR Program as those offenses that involve force or threat of force. Only the most serious offense in a multiple-offense criminal incident is counted.

### Overview

In 2012, an estimated 1,214,462 violent crimes occurred nationwide, an increase of 0.7 percent from the 2011 estimate. When considering 5- and 10-year trends, the 2012 estimated violent crime total was 12.9 percent below the 2008 level and 12.2 percent below the 2003 level. There were an estimated 386.9 violent crimes per 100,000 inhabitants in 2012, a rate that remained virtually unchanged when compared to the 2011 estimated rate. See Figure 1.6.

Aggravated assaults accounted for 62.6 percent of violent crimes reported to law enforcement in 2012. Robbery offenses accounted for 29.2 percent of violent crime offenses, rape accounted for 6.9 percent, and murder accounted for 1.2 percent. Information collected regarding types of weapons used in violent crime showed that firearms were used in 69.3 percent of the nation’s murders, 41.0 percent of robberies, and 21.8 percent of aggravated assaults.

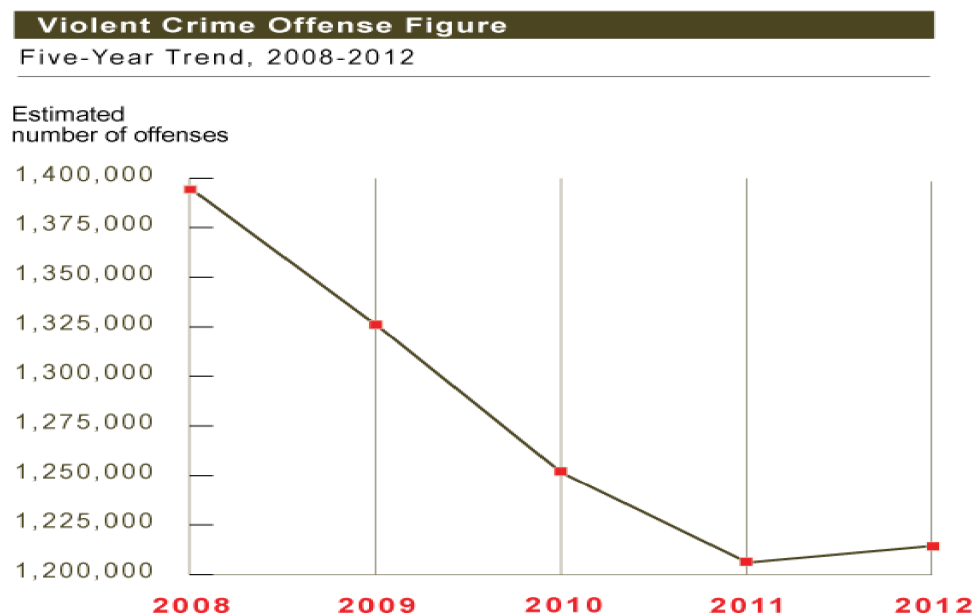


Figure 1.6. Violent crime (FBI 2013).

## Property Crime

*Property Crime*—In the FBI’s UCR Program, property crime includes the offenses of burglary, larceny-theft, motor vehicle theft, and arson. The object of the theft-type offenses is the taking of money or property, but there is no force or threat of force against the victims.

### Overview

In 2012, there were an estimated 8,975,438 property crime offenses in the nation. The 2-year trend showed that property crime declined 0.9 percent in 2012 when compared to the 2011 estimate. The 10-year trend showed that property crime offenses declined 14.1 percent in 2012 when compared to the 2003 estimate. In 2012, the rate of property crime was estimated at 2,859.2 per 100,000 inhabitants, a 1.6 percent decrease when compared to the 2011 estimated rate. The 2012 property crime rate was 11.1 percent less than the 2008 estimate and 20.4 percent less than the 2003 estimate. Of all property crimes in 2012, larceny-theft accounted for 68.5 percent. Burglary accounted for 23.4 percent and motor vehicle theft for 8.0 percent. Property crimes in 2012 resulted in losses estimated at \$15.5 billion. See Figure 1.7.

The types and frequency of crime occurring on public transit varies from that occurring in other environments. For example, the pickpocketing of a wallet from a passenger on a crowded bus platform can occur relatively often in transit whereas a home invasion burglary, defined loosely as the breaking and entering of a dwelling in the nighttime, is not at all likely.

Public transit is multidimensional and consists of a complex infrastructure. Large volumes of people interact in various settings including on vehicles (buses, trains, and trolleys), in facilities (stations and platforms, stops, parking lots, transfer points) and in both crowded and sparse environments in urban, suburban, and rural settings. Certain types of crime are more or less likely to occur depending on the specific characteristics of a location, or perhaps even the particular geographic vicinity of a given transit route. Critical assets of the system itself are also at a risk of loss.

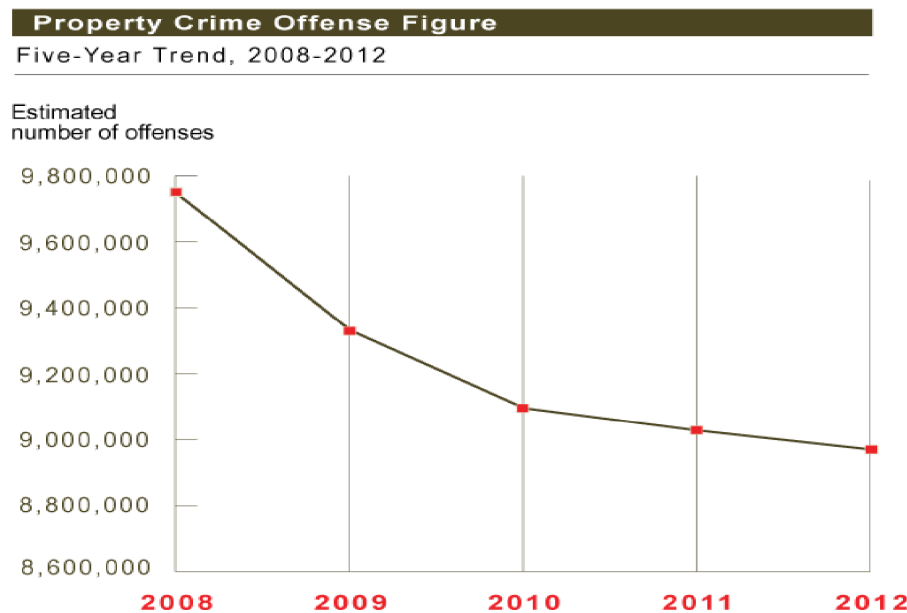


Figure 1.7. Property offenses (FBI 2013).

The following information provides the commonly reported crimes occurring in public transit systems. The definitions of offenses were obtained from either National Transit Database (NTD) or FBI web sites:

*Larceny*—According to the NTD definition, larceny refers to the unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another. Larceny refers specifically to theft *without* the use of violence, force, or fraud. Examples of larceny include a wide range of potential thefts from pickpocketing to stolen transit property. Larceny can contribute to a sense of insecurity among passengers and transit officials, in addition to causing physical and economic damage.

*Robbery*—While similar to larceny, robbery refers to the taking or attempting to take anything of value from the care, custody, or control of a person or persons *by force or threat of force or violence and/or by putting the victim in fear*. Potential consequences of robbery are similar to those of larceny, but likely more severe if violence is indeed used to procure the object of the robbery.

*Aggravated Assault*—The definition of an aggravated assault may differ between states, but it generally refers to an unlawful attack by a person upon another in which the attacker attempts to cause serious harm. According to the UCR definition, this type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm. Aggravated assaults may involve passengers or transit employees. Besides the potential physical harm to people, a repeated pattern of aggravated assaults may instill a culture of fear in a transit agency in which passengers are afraid to use the system or operators are afraid to come to work. Damage to property and scheduling may also occur as a result of an aggravated assault.

*Simple Assault*—A simple assault is similar to an aggravated assault (see definition above) except that the intent to cause harm is typically less severe and usually does not involve a weapon.

*Vandalism*—As it pertains to mass transit, vandalism refers to the willful or malicious destruction or defacement of transit property or vehicles. Examples of vandalism range from graffiti on transit vehicles or stations, to slashed fabric of bus seats, to the defacement of subway maps or advertisements. Potential consequences of vandalism include injury to passengers or transit employees, economic loss, and a diminished ability for passengers to use and enjoy the system.

*Motor Vehicle Theft*—According to the FBI's UCR definition, a motor vehicle theft is defined as the theft or attempted theft of a motor vehicle. In the UCR Program, a motor vehicle is a self-propelled vehicle that runs on land surfaces and not on rails.

On public transport fear of crime and concerns for personal security are clearly a limiting factor to patronage and levels of usage. Similarly the design of transit facilities, and the internal (inside a vehicle) and external (that a vehicle traverses) environments may all influence the level of crime experienced on the system.

## **Minor Offenses and Disorder**

*Fare Evasion*—Fare evasion refers to the unlawful use of transit facilities by riding without paying the applicable amount. Sometimes a passenger may deliberately evade a fare by jumping over a turnstile or sneaking by a bus operator on a crowded vehicle. In other instances, a passenger may passively evade fare payment such as when a passenger neglects to purchase a train ticket and the conductor never checks for compliance. While fare evasion is considered a minor offense, repeated occurrences can result in the loss of significant revenue and contribute to a culture of irresponsible passenger behavior. If the transit agency enforces rules in a lax manner, individuals intending to commit a crime may perceive the agency as a relatively easy target.

*Trespassing*—Trespassing, as it relates to mass transit, is defined as the unauthorized entry of transit-owned land, structure, or other real property not intended for public use. Trespassing can result in serious harm or injury to passengers, especially if the trespassing involves entering a transit vehicle or right-of-way. Other consequences include economic loss, damage to property, or disruption to timetables.

*Drunk and Disorderly Conduct*—While definitions may vary between states, “drunk and disorderly conduct” is often used as a catch-all term to describe unruly or inappropriate behavior that includes but is not limited to, public displays of drunkenness, loitering, disturbing the peace, using obscene language or gestures, or engaging in generally violent or tumultuous behavior. This kind of behavior holds the potential to not only make passengers and transit employees uncomfortable, but also to cause harm to people or property.

*Vagrancy*—The term vagrancy is typically used to refer to the condition of being homeless in a place where loitering is explicitly prohibited. The UCR definition of the term refers more specifically to the violation of a court order, regulation, ordinance, or law requiring the withdrawal of persons from the streets or other specified areas. Anti-vagrancy laws can also prohibit people from remaining in an area or place in an idle or aimless manner or prohibiting people from going from place to place without visible means of support. In terms of transit safety and security, persistent vagrancy can be associated with a negative perception of the transit system, which causes passengers to feel unsafe or uncomfortable.

*Drug Violations*—Drug violations refer to the breaking of laws that prohibit the production, distribution, and/or use of certain controlled substances. These laws vary between states. Drug violations by transit vehicle operators are especially serious because illegal and/or controlled substances can alter the operator’s state of mind and put the vehicle and passengers at serious risk. Additionally, passengers who violate drug laws can also cause harm to fellow passengers, employees, or property.

## **Perceptions of a Lack of Security**

In addition to the 3 types of security risks identified above—homeland security/terrorism, felony or misdemeanor crime, and minor offenses and disorder, a very real fourth set of security complexity must be considered by transit agencies. As stated in the text, *Making the Nation Safer, the Role of Science and Technology in Countering Terrorism*, National Research Council (2002), “The advent of effective security initiatives depends not only on good research pertaining to transportation operations but also on an understanding of human factors.” When people respond to crisis situations there are many factors that can influence their behaviors. These include, among others, factors such as (1) adequacy of preparedness, (2) effectiveness of warnings, and (3) confidence in agencies designated to deal with crisis. In the case of a transit agency, preparedness involves the actions of both transit authorities and the population they serve. Both groups must settle upon an acceptable level of crisis response capability for managing security events. The transit agencies ability to perform required emergency management functions will be considered by the public as only just as good or worse as the last significant security incident that received press or notoriety. When the 2 groups are at odds with one another, or, more pointedly, when transit officials give the appearance that they are unready or unprepared to effectively manage a security-related crisis, an adverse impact on ridership and goodwill will result. Similarly, a failure to warn riders about known dangers, for example, theft of electronic devices or late night robberies occurring on certain routes, can cause a lasting negative blowback when “unaware” passengers are subsequently injured.



## CHAPTER 2

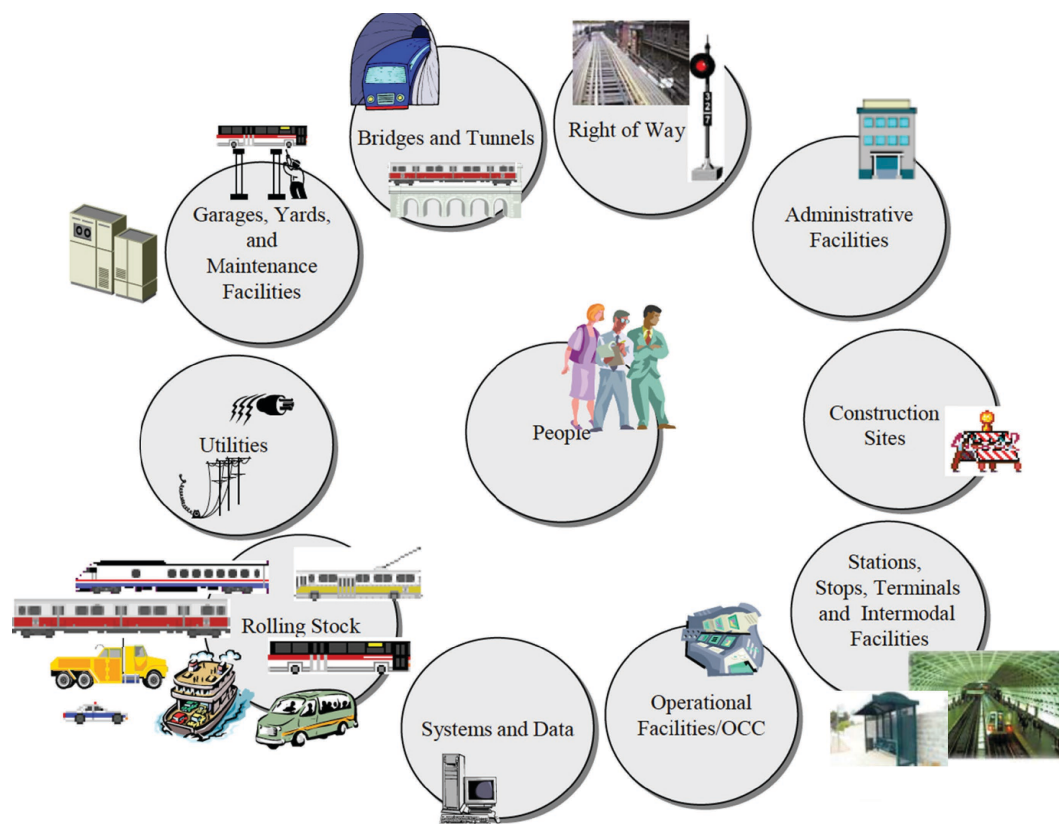
## Small- and Medium-Sized Transit Agency Security Environment

Figure 2.1 and Table 2.1 depict the critical assets and infrastructure of a typical large transit system. Depending on the size and operating characteristics of the agency, the listing of these assets can be quite complex. At one end of the continuum is multimodal transit systems consisting of multiple types of services: commuter rail, light rail, city bus, perhaps trolley, and paratransit and specialty transportation services. These types of systems tend to have significant infrastructure including numerous stations; stops and intermodal facilities; administrative buildings and operations centers; maintenance yards; garages and vehicle storage depots; bridges, tunnels, right-of-way support assets, including electrical and communications substations, repair shops, and various types of rolling stock, rail cars, trains, buses, vans, autos, ferries, trucks, etc.

At the other end of the spectrum are singular service transportation providers who generally are limited to bus-only or automotive and van types of conveyances. These smaller types of agencies have minimal infrastructure with few fixed assets. Often any major station stops serviced by this group are either leased or co-located within multimodal transit centers. Repair and maintenance support services are leased; there are no rights-of-way, tunnels or bridges and in general terms it can be stated that the sole critical assets needing security protection for these small systems are their vehicles and the passengers they transport. Obviously the absence of critical assets reduces the requirements for security. If there are no major stations to protect, or rights-of-way, tunnels, bridges, or maintenance facilities to worry about, the agency's responsibilities are basically limited to what happens on their vehicles to their staff and passengers. Of course this may in some cases be an oversimplification of the problem because of the existence of bus stops, transit shelters, or perhaps even public rest rooms, which may also fall under the direct control of the agency.

Ninety-three (93%) percent of the small- and medium-sized transit agencies surveyed during this project fall into the category of single service bus-only, or van transportation providers. The exceptions were 3 medium-sized agencies who indicated having both train and bus service, and 14 who included trolleybus. Virtually all of the bus agencies also reported that they were running paratransit. See Figures 2.2, 2.3, 2.4, and 2.5.

The assets needing protection for both small and medium-sized agencies are remarkably similar, consisting principally of rolling stock and the passengers and employees on board transit agency vehicles. Simply put, the activities occurring on board vehicles requires the greatest attention from a crime control standpoint. Although ostensibly the security of passengers waiting at bus stops would add to these concerns, typically crime, at these locations, would be the direct responsibility of local police. Parking lots would also usually represent an area of security vulnerability; however, these as well are rarely within the area of responsibility of small- or medium-sized transit agencies. Along with buses and paratransit vehicles, the protection of any administrative facilities, owned stations, bus storage depots or facilities, or other properties



**Figure 2.1. Public transit agency infrastructure assets (Rabkin 2004).**

occupied by agency personnel represents the usual extent of security responsibility for smaller agencies.

## Small-Sized Agencies

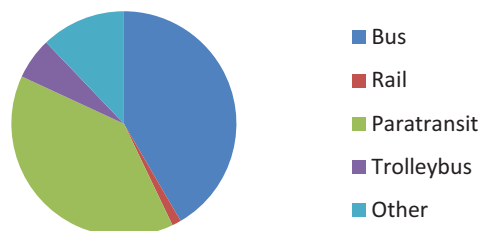
Table 2.2 lists the types of agency infrastructure assets that were considered in the survey of small-sized transit agencies conducted during this research project. Small agencies typically (1) occupied one administrative building/facility (90%); (2) maintained one bus garage or repair facility (82%); (3) operated through one or fewer passenger terminals (82%); operated through one or fewer intermodal facilities (100%); and owned virtually no elevated structures, tunnels, bridges, or subways, private rights-of-way, or substations. The data collected do not include rolling stock.

## Medium-Sized Agencies

Table 2.3 lists the types of agency infrastructure assets that were considered in the survey of medium-sized transit agencies conducted during this research project. Medium-sized agencies typically (1) occupied one administrative building/facility (80%); (2) maintained one bus garage or repair facility (79%); (3) operated through one or fewer passenger terminals (77%); operated through one or fewer intermodal facilities (90%); and owned some elevated structures, tunnels, bridges, or subways, private rights-of-way, or substations. The data collected do not include rolling stock.

**Table 2.1. Transit agency assets.**

Transit Agency Assets
<ol style="list-style-type: none"> <li>1. Transit Stations—facilities used for boarding and alighting of transit passengers, and fare collection; they can be below-grade, at-grade, or elevated. Their high profile, large volumes of pedestrian traffic, and central locations integrated with surrounding uses, make them more likely targets for terrorist attack.</li> <li>2. Transit Stops—usually smaller and more open than transit stations. They are typically on public land, where passengers can board buses and light rail vehicles; these include everything from elaborate shelters to mere signposts. Transit agencies often lack control over these sites, which, combined with their high level of accessibility, makes them difficult to secure against attack.</li> <li>3. Administrative Facilities and Operations Control Centers (OCCs)—used for the operations and administration of the transit system and may be co-located on a site with non-transit uses. Although most administrative facilities are not open to the public and can therefore maintain stricter access control, they have a critical role in the transit system and have value as strategic targets.</li> <li>4. Vehicle Maintenance Facilities—used for the repair and storage of transit vehicles; they include vehicle garages, yards, and repair facilities. They often contain a large number of assets to be protected, including some high-risk elements such as fuel storage areas or containers. Maintenance facilities can be designed to allow transit vehicles and maintenance staff to enter and exit freely, while preventing access by unauthorized vehicles and people.</li> <li>5. Elevated Structures—all above-grade bridges and track structures, including pedestrian bridges and overpasses. Their high visibility and structural complexity present particular challenges to securing them against terrorist attack.</li> <li>6. Tunnels—used for the passage of transit vehicles underground and, in limited cases, underwater. They are more secure when designed to prevent unauthorized access from passenger platforms and at-grade entrances, while allowing transit vehicles to pass freely. Proper design can also facilitate evacuation in an emergency.</li> <li>7. Right-of-Way, Track, and Signals—includes all land and equipment dedicated to the movement of transit vehicles between stations. Like tunnels, a design goal is to allow transit vehicle movement while preventing access by unauthorized people or vehicles.</li> <li>8. Remote and Unmanned Structures—all other physical assets. This category includes power substations, communications relays, and the like, which are not necessarily located on rights-of-way or in stations. These may be owned or controlled by other agencies or companies. Design features that take into account their remote locations and lack of consistent or continuous staff presence can improve their security.</li> </ol>



**Figure 2.2. Small- and medium-sized transit agencies service type.**

What type of service does your agency provide?					
Answer Options	Yes	No	Unsure	Rating Average	Response Count
Bus	151	12	0	1.07	163
Rail/Fixed Guideway	3	100	0	1.97	103
Para-transit	140	20	1	1.14	161
Trolleybus	14	90	1	1.88	105
Other	26	70	0	1.73	96
<i>answered question</i>					178

Figure 2.3. Service type.

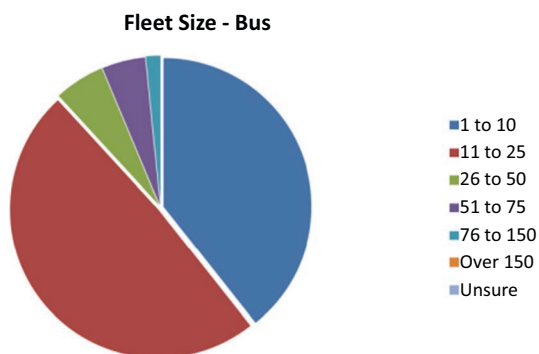


Figure 2.4. Fleet size—bus.

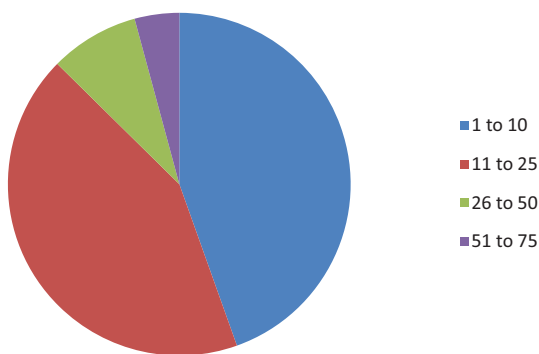


Figure 2.5. Fleet size—paratransit.



**Table 2.2. Types of agency infrastructure assets for small-sized transit systems.**

Asset Type	Number of Assets			
	0	1	2-6	7-12
Administrative Buildings/Facilities	1	58	5	0
Maintenance Facilities (Rail Yard and Bus Garage)	6	40	3	0
Passenger Terminals/Stations	10	18	3	3
Intermodal Centers	10	12	0	0
Elevated Structures	Yes (1)			
Tunnels, Bridges, and Subways	No			
Private Right-of-Way	Yes (2)			
Substations	No			

**Table 2.3. Number of agency infrastructure assets for medium-sized transit systems.**

Asset Type	Number of Assets			
	0	1	2-6	7-12
Administrative Buildings/Facilities	8	83	12	0
Maintenance Facilities (Rail Yard and Bus Garage)	10	79	7	0
Passenger Terminals/Stations	14	39	14	2
Intermodal Centers	18	27	4	1
Elevated Structures	Yes (8)			
Tunnels, Bridges, and Subways	Yes (7)			
Private Right-of-Way	Yes (5)			
Substations	Yes (2)			



## CHAPTER 3

# Transit Agency Security Risk Profiles

The following chapter presents profiles of the 2 types of agencies surveyed for this research—small- and medium-sized transit agencies. For the purpose of this report, a small transit agency is defined as serving a population of less than 50,000 people whereas a medium agency serves a population of between 50,000 and 200,000 people. (See Figure 3.1.)

As noted in Figure 3.1, 180 small- to medium-sized public transit agencies from across the U.S. were surveyed about their assets, identified and historic security risks, as well as physical and operational countermeasures. Questions about assets included size of fleet by mode, physical structures (e.g., office building, maintenance garage), infrastructure (e.g., bridges, tunnels), and security personnel. One hundred and six (106) large agencies were also surveyed for comparative purposes; however, completing profiles for these agencies was outside the scope of the research.

Risk questions pertained to the incidence of homeland security-related events, felony and misdemeanor crimes, and quality-of-life offenses committed within the past year. Agencies were also asked to report on incidents of suspicious activity, packages, persons, bomb threats, and evacuations based on these suspicious circumstances. In terms of countermeasures, agencies were asked about access control, barriers, berms, surveillance equipment, security public awareness campaigns, and security planning. Forty-two (42%) percent of small-sized and 44% of medium-sized transit agencies do not have an annual budget for security operations. Comparatively only 10% of large agencies report not having a budget for security operations. (See Figure 3.2.)

Survey questions varied from yes/no, Likert Scale, to short answer. The results discussed are based on significant answers; agencies that responded “unsure” were not included. Researchers received 70 responses from small transit agencies and 110 responses from medium-sized transit agencies. (See Tables 3.1–3.5.)

18 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

Agency Information: What is the size of your community, as measured by the population of your service area?		
Answer Options	Response Percent	Response Count
Small (serving a population less than 50,000)	38.9%	70
Medium (serving a population 50,000 - 200,000)	61.1%	110
Large (serving a population over 200,000)	0.0%	0
Unsure	0.0%	0
<b>answered question</b>		<b>180</b>
<b>skipped question</b>		<b>0</b>

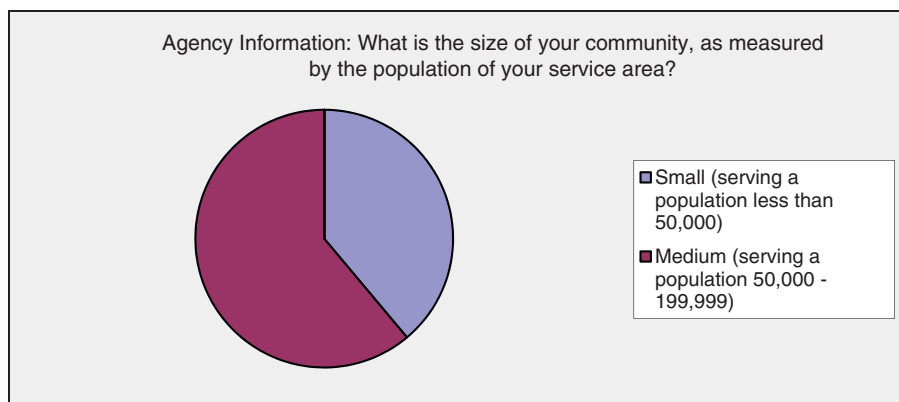


Figure 3.1. Agency size.

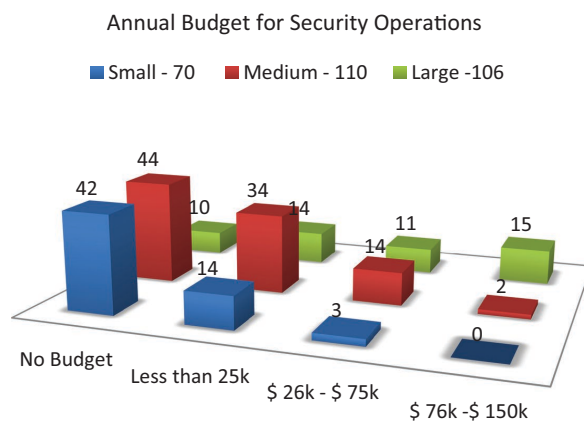


Figure 3.2. Security operations budget.

Table 3.1. Survey groups.

	Size of Area (Population)	Number of respondents
Survey Group 1 (Large)	Greater than 200,000	106
Survey Group 2 (Medium)	Between 50,000 – 200,000	110
Survey Group 3 (Small)	Less than 50,000	70

**Table 3.2. Security risk profile—small-sized transit agencies.**

Profile	Survey Response	
Population Served	Small transit agencies are defined as serving a population of less than 50,000 people	
Service Area	48.6% of the small transit agencies reported 0-100 square mile service areas	
Passenger Miles	The majority of agencies (64%) served less than 250,000 passenger miles one-way annually, with 37% serving less than 100,000 passenger one-way miles.	
Fleet Size	Small transit agency respondents in the survey largely reported having a fleet of 1-10 buses, fewer than 25 paratransit vehicles, no rail or trolley buses	
Buildings	One administrative building, 1 maintenance facility, and sometimes a station or an intermodal center	
Other Infrastructure	Most small agencies did not report owning infrastructure. None of the small transit agencies reported owning tunnels, bridges, subways, or power substations	
Security Budget/Staffing	69% of small transit agencies report that they do not have a budget for security. An additional 23% have security budgets under \$25,000. A majority of small transit agencies reported no dedicated security personnel (87%).	
<b>Terrorism and Homeland Security—Risk Characterized As Very Low</b>		
Arson	No reported incidents with a connection to terrorism or homeland security. Ninety-six (96%) percent of small agencies indicated no reports of suspicious activity of any kind were received from passengers or employees within the past year. Agencies listed zero evacuations due to suspicious activity in the past year. Small-sized agencies most frequently reported relationships with the state/local authorities (81%) and FTA (76%). Some reported relationships with DHS, TSA, FBI, and the FRA.	
Explosives		
Weapons of Mass Destruction (WMDs)		
Violent Confrontations/ Hostage Situations		
Tampering		
Power Loss		
Transit Vehicle as a Weapon		
Network Failure/Cyber Attack		
<b>Felony Crime—Risk Characterized As Very Low</b>		
Homicide		Major crimes occur infrequently on small transit systems. One respondent reported a homicide in the past year. Three respondents reported robberies, 2 on board buses and 1 in a parking lot. Four respondents reported felony aggravated assaults, 2 on board buses and 2 in stations.
Robbery		
Rape		
Aggravated Assault		
Larceny		
Auto Theft	Only a handful of small transit agencies report having an in-house computerized crime reporting system (4%), or crime-mapping (3%). Half of agencies surveyed did report providing crime data to law enforcement (50%) and management (53%). One-third reported crime to the NTD (32%).	
Arson		
Burglary		
<b>Other Crime—Risk Characterized As Very Low</b>		
Pick Pocket/Snatch and Grab	Lesser Crimes involving theft from passengers rarely occur on small transit systems. Only 3 agencies reported any incidents. Theft of company property was reported at 19% of the agencies. Metal thefts were low.	
Theft of Company Property		
Theft from Vehicle	Fare evasion incidents occur at about half of the agencies; however, 15% of those reporting indicate repeated incidents ranging from a low of 11 to a high of 100.	
Scrap or Metal Theft		
Fare Evasion		
Trespassing	Minimal drug activity.	
Drug Offense		

*(continued on next page)*

**Table 3.2. (Continued).**

Quality-of-Life Offenses—Risk Characterized as Low	
Disorderly Persons	Although infrequent unruly, disorderly, or aggressive behavior incidents repeatedly occur at the majority of small transit agencies. 56% percent report between 1 and 10 incidents of disorderly conduct annually. About 1/3 of the agencies have a minor homeless issue consisting of less than 10 incidents occurring annually. Vandalism is reported as low, with 59% reporting no incidents.
Homeless/Vagrancy	
Drunkenness/Liquor Law Violations	
Smoking/Eating/Littering/Loud Music	
Graffiti/Vandalism	
School Related Disorder	
Countermeasures	
Security Lighting	Many small transit agencies (76%) incorporated lighting as security support and crime deterrence. Typically street lights, flood lights, and building lights around office buildings, maintenance facilities, in bus garages, and parking lots. Most agencies (61%) recorded no berms or barriers as an access control to restricted areas/nonpublic places. Small transit agencies used fences (63%) in these areas, primarily chain-link with some barbed wire, often 6-10 feet tall.
Barriers and Berms	
Fencing	
Video Surveillance	
Intrusion Detection	About half of small transit agencies use close-circuit television (CCTV) video surveillance on their properties, primarily at office buildings, parking lots, on board buses and paratransit vehicles. Agencies mostly used cameras to record without monitoring or for a playback function/storage. A few agencies monitored the cameras and recorded the video stream.
Physical Sweeps or Inspections	
Passenger Screenings for Firearms, Explosives, WMD	
Access Control	
Security Signage	Some small transit agencies employ electronic security systems or routine security practices as another means of protection and prevention. Several agencies listed intrusion detection equipment at office buildings, stations, and maintenance facilities—mostly audible alarms and video motion detection. 61% of agencies reported conducting security sweeps, generally at garages, parking lots, on buses, paratransit, and in office buildings. Agencies also reported access control at buildings, garages, and parking lots, most frequently fences, key cards, key locks, and key pads. Over half of small transit agencies reported not having emergency phones available (53%). Those agencies that did have emergency phones placed them largely at office buildings.
Emergency Telephones, Duress Alarms, Assistance Stations	
Dedicated Security Staffing	
Security Awareness Training for Employees	
Security Training, Drills and Exercises	Though many small transit agencies used the “see something, say something” public awareness security campaign, most agencies reported not having public awareness security signage in place (79%). Despite the aforementioned countermeasures, many small transit agencies lack security personnel, training procedures, a dedicated security budget, or a formal security plan. A majority of small transit agencies reported no dedicated security personnel (87%). Many small transit agencies reported having a security plan (48%) though most were unsure when it was last updated (58%). Most agencies did not provide security training (68%). When agencies did report training it was provided to front-line employees, administrators, operators, dispatchers, and supervisors; focused on security awareness, behavior recognition, and emergency operating procedures. 89% of agencies perform background investigations of employees, however this number falls to less than 40% for contractors granted access to transit property.
Security Plan or Risk Management Framework	
Risk and Vulnerability Assessment	
Background Investigations for Employees	
Background Investigations for Contractors	

**Table 3.3. Security risk profile—medium-sized transit agencies.**

Profile	Survey	
Population Served	Medium-sized transit agencies are defined as serving a population of between 50,000 and 200,000 people	
Service Area	52% of medium-sized transit agencies reported 0-100 square mile service areas; 16% between 100 and 300; 9% between 300 and 500; and 15% over 500 miles.	
Passenger Miles	Approximately 27% of survey respondents reported their transit agency provided over 750,000 one-way annual passenger miles, 20% between 101,000-250,000 and the remainder providing 251,000-750,000 (28%). 5% were less than 100,000.	
Fleet Size	The medium-sized transit agencies reported larger fleets—most frequently 11-25 buses (46%) and paratransit vehicles (40%). One of these agencies reported having a fleet of 26-50 railcars, and 11 agencies reported having a fleet of 1-10 trolley buses. The majority provided bus (94%) and paratransit (92%).	
Buildings	Most agencies reported having one administrative building (81%) or 2 to 6 buildings (12%). Agencies also reported 1 maintenance facility/rail yard/bus garage (82%) or 2 to 6 facilities (7%). Many agencies had at least 1 passenger station/terminal (56%) and/or intermodal center (54%).	
Other Infrastructure	Some agencies had elevated structures, bridges, and private right-of-way. One agency reported owning a tunnel and 2 others had power substations (likely for rail traction power)	
Security Budget/Staffing	44% of medium-sized transit agencies report that they do not have a budget for security. An additional 34% have security budgets under \$25,000. 17% report dedicated security staff.	
<b>Terrorism and Homeland Security—Risk Characterized as Very Low</b>		
Arson	No reported incidents with a nexus to terrorism or homeland security. Only 3 agencies reported receiving bomb threats—1 bus threat, and 2 agencies reported receiving station bomb threats and other threats.  88% of medium-sized agencies indicated no reports of suspicious activity of any kind were received from passengers or employees within the last year. The most frequently reported was suspicious persons (11), packages (9), and trespassing (6). In fact, out of 110 medium-sized agency respondents, only 7 reported evacuations due to suspicious activities. Of those, six agencies reported 1 bus evacuation, and 1 agency reported 3 evacuations. Six agencies also reported 1 station evacuation, and 1 agency reported 2 evacuations. One agency each reported a train, paratransit, and trolley evacuation.  Medium-sized agencies most frequently reported relationships with the state/local authorities and FTA. Some reported relationships with DHS, TSA, FBI, and the FRA. 64% of agencies reported providing suspicious activity information to the DHS.	
Explosives		
WMDs		
Violent Confrontations/ Hostage Situations		
Tampering		
Power Loss		
Transit Vehicle as a Weapon		
Network Failure/Cyber Attack		
<b>Felony Crime—Risk Characterized as Low to Very Low</b>		
Homicide		Major crimes occur infrequently on medium-sized transit systems. None of the medium-sized agencies reported incidents of homicide or rape. 85% of agencies reported no incidents of robbery. Of the agencies that had robberies, 90% reported between 1 and 3 incidents per year. 76% of the agencies reported no aggravated assaults. Similarly many agencies reported no instances of auto thefts (91%), arson (96%), or burglaries (94%).  When the crimes were considered by location, agencies reported the most incidents on buses. Agencies reported 1-10 assault incidents per year against operators (19%) and passengers (29%). Aggravated assault, robbery, and larceny were also reported at stations. Agencies also reported auto theft from parking lots, some larceny, robbery, aggravated assault, and burglary.  Few medium-sized transit agencies report having an in-house computerized crime reporting system (12%), or crime-mapping (10%). Agencies did report providing crime data to law enforcement (60%), management (70%), and the NTD (72%).
Robbery		
Rape		
Aggravated Assault		
Larceny		
Auto Theft		
Arson		
Burglary		

(continued on next page)

**Table 3.3. (Continued).**

Other Crime – Risk Characterized as Low	
Pick Pocket/Snatch and Grab	<p>Lesser Crimes involving theft from passengers infrequently occur on medium-sized transit systems. Ten of the agencies reported incidents. Theft of company property was reported at 17% of the agencies. 12% reported thefts from vehicles. Metal thefts were low.</p> <p>Fare evasion incidents occur at 64% of the agencies. 20% of those reporting indicated repeated incidents ranging from a low of between 11 and 25 (10 agencies) to a high of greater than 100 (2 agencies).</p> <p>23% of agencies reported at least 1 incident of trespassing per year including some reports of 4-7 incidents, 8-12 incidents, and over 12 incidents of trespassing. Agencies reported assault against passengers and trespassing in stations, as well as trespassing and drug offenses in the parking lots.</p>
Theft of Company Property	
Theft from Vehicle	
Scrap or Metal Theft	
Fare Evasion	
Trespassing	
Drug Offense	
Quality-of-Life Offenses – Risk Characterized as Medium to Low	
Disorderly Persons	<p>Medium-sized transit agencies occasionally to frequently face incidents of unruly, disorderly, or aggressive behavior. 64% percent report between 1 and 10 incidents of disorderly conduct annually. 56% of the agencies have homeless issues with 5 agencies reporting between 11 and 25 incidents, 3 between 26 and 50, 2 between 51 and 100, and 2 with over 100 incidents annually. Half the agencies experience drunkenness/liquor law violations (49%), smoking, eating, littering, and loud music (46%). Incidents of graffiti or vandalism are reported at approximately 60% of the agencies.</p> <p>Much of the quality-of-life offenses occurred on buses; especially disorderly persons (77%) and drunkenness (56%). The most commonly reported paratransit quality-of-life crimes included disorderly conduct (28 agencies) and smoking/eating/littering/loud music (12 agencies). 78 of 108 agencies reported no incidence of quality-of-life crime on paratransit. Of the few agencies with trolley buses, 4 reported drunkenness incidents, and 3 had homelessness/vagrancy incidents. Numerous agencies reported quality-of-life crimes at stations, though fewer incidence of loud music than any other category.</p>
Homelessness/Vagrancy	
Drunkenness/Liquor Law Violations	
Smoking/Eating/Littering/Loud Music	
Grffiti/Vandalism	
School Related Disorder	
Countermeasures	
Security Lighting	<p>Most agencies (85%) reported using lighting to support security inspections, patrols, passenger and employee awareness, and deterrence. These agencies mostly reported lighting outside office buildings (93%), and maintenance facilities (83%), some stations (66%), and parking lots (59%). The type of lighting was generally building light (91%) and streetlights (85%), with some lampposts (56%), floodlights (56%), and a few motion detection lights (17%). Of the agencies with barriers and berms, most reported using natural barriers and landscaping, bollards, and planters. Agencies located these dividers predominantly outside maintenance facilities (77%), office buildings (55%), parking lots (34%), and stations (32%). 79% of agencies reported using fences for access control, most frequently around maintenance facilities (80%), office buildings (49%), parking lots (48%), and some stations (22%). Agencies with fences generally reported using chain-link (84%), 6-10 ft tall (83%), and some with barbed wire (22%).</p> <p>Less than half of the agencies used electronic systems to control access to restricted areas (40%). Systems generally included key-card use, fencing/gates, key locks, and key pads. Agencies with these systems reported using access control in office buildings, maintenance facilities, and a few at stations.</p> <p>76% of medium-sized transit agencies used CCTV, most with playback storage, some monitored and recorded, others recorded but not monitored. Agencies reported predominantly fixed camera, some pan-tilt-zoom, and night vision cameras as well. Agencies reported using CCTV on buses (75%), at office buildings (73%), maintenance facilities (71%), stations (59%), on paratransit (48%), and in parking lots (47%).</p>
Barriers and Berms	
Fencing	
Video Surveillance	
Intrusion Detection	
Physical Sweeps or Inspections	
Passenger Screenings for Firearms, Explosives, WMDs	
Access Control	
Security Signage	
Emergency Telephones, Duress Alarms, Assistance Stations	
Dedicated Security Staffing	

**Table 3.3. (Continued).**

Security Awareness Training for Employees	<p>44% of medium-sized transit agencies reported using intrusion detection devices, predominantly audible alarms. Agencies with intrusion detection devices reported locating them at office buildings (93%), maintenance facilities (75%), and stations (36%). Most intrusion detection devices were for office buildings (98%), perimeters (47%), and internal security (35%). The most frequent type of duress alarm was driver address, followed by call boxes, panic alarms, and intercoms.</p> <p>Half of the agencies conduct some form of public awareness campaigns. 58% of agencies provided security training to employees. Training generally included security awareness (97%), emergency operating procedures (95%), and behavioral recognition (62%). Most agencies had a security plan, and updated the plan within the past 12 or 36 months. Approximately half of these agencies had an employee responsible for implementing the plan. Additionally, many agencies conducted a risk vulnerability assessment and had updated it within the past 12 or 36 months.</p> <p>Though 95% of agencies conducted background checks on employees, significantly fewer (28%) conducted checks on contractors.</p>
Security Training, Drills and Exercises	
Security Plan or Risk Management Framework	
Risk and Vulnerability Assessment	
Background Investigations for Employees	
Background Investigations for Contractors	

**Table 3.4. Relative risk profile comparative findings/summary section.**

Security Risk Profile	Small-Sized Agencies	Medium-Sized Agencies
Terrorism/Homeland Security	Risk characterized as <b>very low</b>	Risk characterized as <b>very low</b>
Felony Crime	Risk characterized as <b>very low</b>	Risk characterized as <b>low to very low</b>
Other Crime	Risk characterized as <b>very low</b>	Risk characterized as <b>low</b>
Quality-of-Life Offenses	Risk characterized as <b>low</b>	Risk characterized as <b>medium to low</b>



**Table 3.5. Countermeasures deployment comparative findings/agency utilization rates.**

Security Measure	Small-Sized Agencies				Medium-Sized Agencies			
	VL	L	M	H	VL	L	M	H
Security Lighting				x				x
Barriers and Berms		x				x		
Fencing			x					x
Video Surveillance		x						x
Intrusion Detection	x					x		
Physical Sweeps or Inspections		x					x	
Passenger Screenings for Firearms, Explosives, WMDs	x				x			
Access Control	x					x		
Security Signage	x					x		
Emergency Telephones, Duress Alarms, Assistance Stations		x				x		
Dedicated Security Staffing	x				x			
Security Awareness Training for Employees				x				x
Security Training, Drills and Exercises		x				x		
Security Plan or Risk Management Framework		x					x	
Risk and Vulnerability Assessment		x					x	
Background Investigations for Employees				x				x
Background Investigations for Contractors	x					x		

KEY: Very Low (VL) = 0-25% Low (L) = 26-50% Medium (M) = 51-75% High (H) = 76-100%

# Crime, Statistics, and Reporting Procedures

## Crime and Security Data

The reporting of criminal incidents in the United States has been centralized under the FBI's UCR Program. UCR consists of a series of designator codes that categorize crime for statistical purposes. Basically, once collected, offense data is categorized into a predetermined set of "major" Part I crimes or Part II offenses. Today, 4 annual publications, *Crime in the United States*, *National Incident-Based Reporting System*, *Law Enforcement Officers Killed and Assaulted*, and *Hate Crime Statistics* are produced from data received from over 18,000 city, university/college, county, state, tribal, and federal law enforcement agencies voluntarily participating in the program. The platform used for the collection of the crime information is the National Incident-Based Reporting System (NIBRS).

Transit police, railroad police, and other transportation industry law enforcement must submit their crime occurrence data through a state UCR Program. Although the option of direct reporting to the FBI is available, the transportation industry has not undertaken to report in this manner. This is mainly because NIBRS has been designed to be generated as a byproduct of local, state, and federal law enforcement automated records systems.

Since the transportation industry does not directly provide industry crime statistics, the FBI is not able to separate or segment the criminal offenses that occur on transit systems. Transit-related incidents are typically reported in batch form by local law enforcement agencies that have geographic jurisdiction over the location of occurrence. These agencies of jurisdiction are identified through use of an NIBRS-authorized ORI (originating agency) number. When a criminal incident happens at a particular location, i.e., a transit station or maintenance facility, the occurrences can only be officially captured through reporting to state or local law enforcement.

State and local law enforcement does not generally possess the means to isolate crime data by industry. Most automated crime incident reporting systems are address based meaning that a look-up performed for a crime occurrence will be identified through street number and name. Locations identifiable as transit infrastructure make it possible to obtain limited crime statistics; however, further analysis and segmentation would be required to obtain an accurate determination of crime occurring on a given transit system. The problem with obtaining transit-specific crime data is sometimes made more difficult because of the agency's service area, which often operates across a multi-jurisdictional law enforcement coverage area with different police agencies providing public safety services both independently and concurrently. Operating through one or more counties, cities, townships, or boroughs can cause an intractable difficulty in determining an accurate picture of crime occurring on a given transit system. In such circumstances, the transit agency must engage in a significant effort to outreach, coordinate, collect, and analyze information from multiple law enforcement agencies.

There is a federal level crime incident data collection effort, FTA's NTD, in place for transit. However, the system is based on transit agency direct reporting and not the FBI UCR/NIBRS system. The NTD mirrors the UCR in using Part I, Major Crimes and Part II, Offenses criteria; however, there are different characterizations, and additional descriptive designators that have been included in the NTD (see Table 4.1). Reporting to the NTD is mandatory for all transit agencies that receive FTA formula funds.

**Table 4.1. Part I and Part II offense categories and definitions contained in the NTD.**

Part I Major Crimes	
Homicide	The killing of one or more human beings by another, including the following: <ul style="list-style-type: none"> <li>• Murder and non-negligent manslaughter—the willful (non-negligent) killing of 1 or more human beings by another.</li> <li>• Negligent manslaughter—the killing of another person or persons through gross negligence.</li> </ul>
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 attempt to take anything of value under confrontational circumstances from the care, custody, or control of another person by force or threat of force, 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.
Part II Offenses	
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 attempted attack 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.
Other NTD Security Incident Categories	
Bombing	The unlawful and intentional delivery, placement, discharge, or detonation of an explosive or other lethal device.
Bomb Threats	A 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	The unlawful and intentional delivery, placement, discharge, or detonation of a biological, chemical, or nuclear lethal device.

**Table 4.1. (Continued).**

Cyber Incident	Involves the targeting of transit facilities, personnel, information, computer, or telecommunications systems associated with transit agencies. Proscribed activities include the following: <ul style="list-style-type: none"> <li>• Denial or disruption of computer or telecommunications services, especially train control systems.</li> <li>• Unauthorized monitoring of computer or telecommunications systems.</li> <li>• Unauthorized disclosure of proprietary or classified information stored within or communicated through computer or telecommunications systems.</li> <li>• Unauthorized modification or destruction of computer programming codes, computer network databases stored information, or computer capabilities.</li> <li>• Manipulation of computer or telecommunications services resulting from fraud, financial loss, or other criminal violations.</li> </ul>
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.

Source: Adapted from *TCRP Synthesis 80: Transit Security Update* (Nakanishi 2009).

In *TCRP Synthesis 80: Transit Security Update*, Nakanishi (2009) commented,

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 2 or more persons, property damage equal to or exceeding \$25,000, an evacuation owing to life safety reasons, or a main-line 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.

Also,

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 reporting 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.

Given the NTD transit agency self-reporting crime database issues described above, the concept of separating out transportation-/transit-related crime into its own relational database is worthy of consideration. Presently there is no method to capture the extent of transit-related criminal activity or the associated security risk that is inherent in the operation or utilization of the nation’s transit systems.

## Crime Rates in Transit

The September 1982 issue of *Transportation* featured an article titled, “Crime in Public Transit Systems: An Environmental Design Perspective” (Pearlstein and Wachs 1982). The article included information about a statistical analysis of criminal incidents occurring over a 10-year

**Table 4.2. Frequency of crime by transit system size (1984).**

Category of Crime	Size of Transit System		
	Large (>100 million passengers)	Medium (20-100 million passengers)	Small (<20 million passengers)
Murder	##	#	#
Rape	##	##	#
Aggravated Assault	####	###	##
Other Sex Offenses	####	##	##
Robbery	#####	###	##
Simple Assault	#####	##	##
Larceny	#####	#####	##
Drunk and Disorderly Conduct	#####	#####	####
Local Ordinance Violations	#####	#####	#####

Legend

Common(a)	#####	Infrequent	###
Very Frequent	#####	Very Infrequent	##
Frequent	#####	Rare(c)	#
Occasional(b)	####		

(a) More than 10 per day

(b) Approximately one per week

(c) Less than one incident per year

Source: (Mauri et al. 1984)

period on the Southern California Rapid Transit District of Los Angeles. The analysis disclosed that crime on transit occurs at a rate approximately in proportion to transit ridership. Further that, “most crimes occur on routes which traverse areas having high crime rates in general.” Similarly, in 1984 the U.S. Department of Transportation Research and Special Programs Administration (RSPA) Transportation Systems Center published a comprehensive report titled, *Transit Security: A Description of Problems and Countermeasures* (Mauri et al. 1984). To gain an overview on transit security issues, the research team conducted site visits at 13 U.S. transit systems. Systems were selected to represent a variety of sizes, geographical locations, and modes (bus/light rail/heavy rail). The abstract stated,

The report examines transit security problems in the following areas: crimes against passengers and employees; crimes involving revenues, including fare evasion by patrons and revenue theft by employees; and crimes against transit property, including vandalism and graffiti.

The RSPA report came to an important conclusion about transit crime at individual transit systems in general:

... the level of mass transit crime mirrors the crime rate of the surrounding area. Mass transit systems located in high crime areas generally experience high levels of transit crime. In addition, transit systems servicing broad metropolitan areas will experience their most severe crime problems in those areas where crime is most prevalent. In that the largest transit systems typically service the most densely populated and crime-ridden areas, it follows that these systems will have the greatest crime problems.

Table 4.2 discloses that with the exception of *Drunk and Disorderly Conduct* or *Local Ordinance Violations* that crime occurs “very infrequently” on small systems and “infrequently” on medium-sized systems. These 1984 findings are consistent with the survey conducted by the F-18 project team in 2013 (see Table 4.3). Results tend to support that the larger the transit agency in terms of ridership the more likely it is that crime will occur on the system.

**Table 4.3. Frequency of crime by transit system size (2013).**

Category of Crime	Size of Transit System		
	Large (>100 million passengers)	Medium (20-100 million passengers)	Small (<20 million passengers)
Murder	##	#	#
Rape	#	#	#
Aggravated Assault	#####	####	##
Other Sex Offenses	##	#	#
Robbery	#####	####	##
Simple Assault	#####	###	##
Larceny	#####	####	##
Drunk and Disorderly Conduct	#####	#####	###
Local Ordinance Violations	#####	#####	####

Legend

Common <sup>(a)</sup>	#####	Infrequent	###
Very Frequent	#####	Very Infrequent	##
Frequent	#####	Rare <sup>(c)</sup>	#
Occasional <sup>(b)</sup>	####		

(a) More than 10 per day

(b) Approximately one per week

(c) Less than one incident per year



## CHAPTER 5

# Transit Crime and Security Problems

Irrespective of the size of the agency, in general terms, transit security problems fall into a small group of categories: (1) passenger security, (2) employee security, (3) revenue security, (4) transit equipment and property protection, (5) fraud, and (6) homeland security-related threats and vulnerabilities.

### **Passenger Security**

Understanding the crime and security threats associated with passenger security starts with recognition that the operating characteristics of transit systems create inherent vulnerabilities and in some cases can optimize the opportunity for crime victimization. The use of public transit creates circumstances in which large numbers of people are often crowded together into enclosed spaces or concentrated into confined areas. As stated in FTA's *Security Design Considerations* (Rabkin et al. 2004) "the high concentrations of people in contained spaces—whether it be a full bus crowded with standees, or a downtown subway platform at rush hour—make transit facilities inviting targets and provides another significant challenge for agencies to address." In contrast, the potential isolation or limited occupancy of transit facilities or vehicles at certain times can result in people becoming targets of opportunity for criminals who seek to avoid detection or apprehension.

Whether caused by large crowds, confined numbers of people in enclosed spaces, or isolated areas, the target attractiveness of transit's operating venues or occupied conveyances is exacerbated by the necessity of openness and the requirement to maintain public access. Transit systems must remain open and accessible to thousands of daily customers, sometimes 24 hours a day and 7 days a week. And comingled among these law-abiding fare-paying passengers is a criminal element whose goal is to commit crimes by taking advantage of targets of opportunity.

Crimes against persons include homicide, aggravated and simple assault, robbery, rape, sex offenses, and harassment. Each transit system experiences its own unique blend of these types of crimes in terms of frequency and severity. For example, most small- and medium-sized transit agencies will never experience a homicide, but it is also possible for a relatively minor type of robbery to go horribly wrong resulting in a fatality.

### **Homicide**

There are differing circumstances and types of murder that occur in society, ranging from premeditated first degree murder that requires malice aforethought to accidental, negligent, reckless manslaughter. In general, in the latter the homicide has occurred without intent. Both small- and medium-sized transit agencies should rarely see any form of homicide on their systems.

However, even these systems may not be immune to isolated incidents where murder is caused by conflict between primary or non-primary family, friends, or acquaintances. Similarly, strangers in pursuit of gain or some other rational or irrational motivation may commit murder either concurrent with the commission of a felony, or as a result of mental deficiency.

### **Aggravated Assault, Simple Assault, and Harassment**

Assault crimes are generally impulsive, emotionally-based—typically anger—and can result from conflict occurring between known relations or strangers. However, there are also incidents where an aggressor “lies in wait” to attack the victim. These types of occurrences of assault are premeditated in conjunction with some form of preconceived motive, including robbery. Assault crimes are charged based on “degrees” of consequence or through determination of weapon types whether used or possessed. Simple assault or harassment may occur based solely on a nonviolent offensive touching, for example, spitting on another individual, while aggravated assault would be charged in circumstances where a weapon is brandished in commission of a felony or an individual is severely beaten with lasting injuries. Along this violent or perceived violent continuum, victims who suffer injury are categorized and offenders are charged with either a felony or misdemeanor offense. Small- and medium-sized transit agencies can expect to have some form of assault on passengers occur periodically, but usually along the lesser side of the continuum. However, it should be noted that because few, if any, transit systems screen passengers for weapons in common areas of stations, at depots, and on board vehicles, there is a potential for more violent consequences.

### **Robbery**

In the transit environment simple robbery incidents have traversed in terms of valuables of choice stolen from stealthy pick pocketing and wallet grabs, to purse snatching, gold chain snatching, and more recently to cell phone, tablet, laptop computer, and electronics theft. The nature of attacks has also become more brazen with continual media coverage of scenes of transit passengers primarily on city buses or trains somewhere in the United States being robbed at gunpoint, or suffering vicious assaults at the hands of one or more assailants. Unfortunately passengers occupying the enclosed space of a bus or train car represent a captive group for would-be assailants. Incidents of robbery also occur in station and at transit stops. Both small- and medium-sized transit agencies must be prepared to contend with the commission of robberies against their passengers although incidents of violent attacks remain infrequent.

### **Rape and Sex Offenses**

Rape and other felony-related sex offenses rarely occur on transit systems. Victimization occurs when passengers become targets of opportunity. For example, during late night hours at an unoccupied, sparsely attended or closed station, or in a transit-operated parking lot, a perpetrator may take advantage of the seclusion to prey upon an unescorted passenger. Sexual harassment types of offenses may occur more frequently and in fact occurrences may be underreported. Riders are subject to being ogled, flashed, groped or even sexually assaulted. In 2009, Metropolitan New York Transit Authority reported that close to 600 sex offenses occurred on board the subway resulting in 417 arrests. Time of occurrence was usually rush hour either in the morning—roughly 8:00 am to 10:00 am—followed by the afternoon rush—between 4:00 pm and 6:00 pm. More recently the availability of cell phone cameras to record either photographs or video has resulted in an increase in complaints regarding the secret and unauthorized taking of “upskirt” photos of women on public transit. In Boston, Massachusetts, in 2014, the Supreme Judicial Court overruled a lower court that had upheld charges against a suspect who was arrested by transit police. Police set up a sting after getting reports that the suspect was using his cell phone to take



photos and video up female riders' skirts and dresses. State law "does not apply to photographing (or videotaping or electronically surveilling) persons who are fully clothed and, in particular, does not reach the type of up-skirting that the defendant is charged with attempting to accomplish on the MBTA," the court said. In response to the ruling the Massachusetts state legislature took swift action passing new legislation; "anyone who photographs, videotapes or electronically surveils another person's sexual or intimate parts without that person's consent would face a misdemeanor charge and a maximum penalty of two-and-a-half years in jail and a \$5,000 fine." The crime becomes a felony with a maximum penalty of 5 years in prison and a \$10,000 fine for photographs or recordings of a child under 18. Distributing such photos would carry a maximum punishment of 10 years in prison and a \$10,000 fine. Other jurisdictions hold that "Peeping Tom" laws that are typically on the books to protect people from being photographed in dressing rooms and bathrooms when nude or partially nude, or laws against secretly recording intimate parts of individuals represents sexual harassment do apply under such circumstances.

## Employee Security

Like transit passengers, transit employees, especially bus drivers, are potential victims of transit crime. When crimes against persons involving employees occur during working hours, the events are properly categorized as workplace violence incidents. The accepted typology for workplace violence incidents is described by the Federal Bureau of Investigations in the report, *Workplace Violence: Issues in Response* (Rugala/Isaacs 2002) (see Figure 5.1):

The National Crime Victimization Survey (NCVS) collects information on violent crimes against persons in the workplace. Workplace violence is defined as nonfatal violence (rape/sexual assault, robbery, and aggravated and simple assault) against employed persons age 16 or older that occurred while they were at work or on duty. Attempted crimes are included along with completed victimizations. Homicide crime is captured and reported separately through the Bureau of Labor Statistics Census of Fatal Occupational Injuries.

Between 1993 and 1999 the average annual workplace victimization for "all violent crime" types reported was 1,744,300. The majority of workplace violence incidents that occur are lesser cases of assaults, domestic violence, stalking, threats, harassment (including sexual harassment), and physical and/or emotional abuse (Figure 5.2).

Of the 4 types of workplace violence categories, Type 1—Crime Related and Type 2—Service-Provider Related, are the main areas of concern to transit and transit employees. This is not to say that worker on worker violence or domestic types of assaults do not occur, rather that there is an employee performance or duty-based component associated with Type 1 and Type 2.

### Type 1 Violence

According to the FBI, "violence by criminals unconnected to the workplace accounts for the vast majority—nearly 80 percent—of workplace homicides. In these incidents, the motive is

Type 1	Violent acts by criminals who have no other connection to the workplace, but enter to commit robbery or another crime
Type 2	Violence directed at employees by customers, clients, patients, students, inmates or any others for who an organization provides services
Type 3	Violence against coworkers, supervisors, or managers by a present or former employee
Type 4	Violence committed in the workplace by someone who doesn't work there, but has a personal relationship with an employee—an abusive spouse or domestic partner

**Figure 5.1.** *Workplace violence topology (Rugala and Isaacs 2002).*

**Average annual number, rate, and percent of workplace victimization by type of crime, 1993–99**

Crime Category	Average annual workplace victimization	Rate per 1,000 persons in the workforce	Percent of workplace victimization
All Violent Crime	1,744,300	12.5	100%
Homicide	900	0.01	0.1
Rape/Sexual assault	36,500	0.3	2.1
Robbery	70,100	0.5	4.0
Aggravated assault	325,000	2.3	18.6
Simple assault	1,311,700	9.4	75.2

Sources: Homicide data are obtained from the Bureau of Labor Statistics Census of Fatal Occupational Injuries. Rape and sexual assault, robbery, aggravated assault, and simple assault data are from the NCVS.

**Figure 5.2. Average annual number, rate, and percent of workplace victimization by type of crime, 1993–99 (from Rugala and Isaacs 2002).**

usually theft, and in a great many cases the criminal is carrying a gun or other weapon, increasing the likelihood that the victim will be killed or seriously wounded.”

## Type 2 Violence

These cases typically involve assaults on an employee performing occupational tasks committed by a customer, patient, *passenger*, or someone else receiving service.

## Homicide

In 2012, there were 767 workers killed as a result of violence and other injuries by persons or animals, including 463 homicides and 225 suicides. The work-related suicide total for 2012 declined 10 percent from the 2011 total and the homicide total was also slightly lower. Shootings were the most frequent manner of death in both homicides (81 percent) and suicides (48 percent). Of the 338 fatal work injuries involving female workers, 29 percent involved homicides. Bureau of Labor Statistics Census of Fatal Occupational Injuries, *TABLE A-1, Fatal Occupational Injuries by Industry and Event or Exposure, All United States, (2012)*, disclosed that 60 fatalities occurred under the category of “Transit and Ground Passenger Transportation” with 35 of these incidents recorded as “Violence and Other Injury by Persons or Animals.”

Incidents of Type 1 violence perpetrated against transit employees by criminals who are motivated to commit theft or robbery occur at a much lower rate than in the past mainly because of the industry’s changeover to exact fare collection systems. *Transit Security: A Description of Problems and Countermeasures* (Mauri et al. 1997) described the changeover and what prompted transit companies to switch to a system in which drivers were no longer required to carry cash:

Prior to the introduction of exact fare systems, the cash that bus drivers carried was an invitation to driver assault. Robbery of bus drivers reached epidemic proportions during the 1960s. From 1963 to 1968, the nation’s bus systems experienced a five-fold increase in bus driver robberies and a tenfold increase in driver deaths. In Washington, DC during one month in 1968, one driver was shot during a robbery and another was murdered in a robbery attempt. The immediate response to these events in Washington, DC was to enact an exact fare procedure which was effective in sharply reducing robbery attempts. Under pressure from the Amalgamated Transit Union, the exact fare procedure was quickly adopted by many bus systems around the country, and a major cause of attacks on drivers was eliminated.

Of course, station or depot ticket sales employees working in locations that are sparsely attended or at times absent passengers or other staff may yet be targeted by criminals. However, it should be

noted that there is a continuing major trend toward cashless fare collection systems and the placement of automated ticket dispensing machines in transit centers that is further removing the opportunity for criminals to obtain cash through dangerous confrontations like hold-ups or robberies.

Fare collection though remains a leading contributor to Type 2 violence in transit. Unfortunately passengers can become quite upset about a dispute associated with their transportation. Most common reasons for fare disputes are arguments over transfers, dispute as to proper fares, expired or invalid passes, and arguments about reduced fare authorizations. But violent reactions by passengers are not limited solely to disputes about money. Anger at the quality of service or denial of service, transportation delays, or some other precipitating event may easily cause unpredictable and dangerous behavior to occur. Similarly mental health issues, abuse of alcohol or drugs, or perhaps even unrelated anxiety over personal circumstances can trigger an argument between a passenger and a transit operator that sometimes can have fatal outcomes.

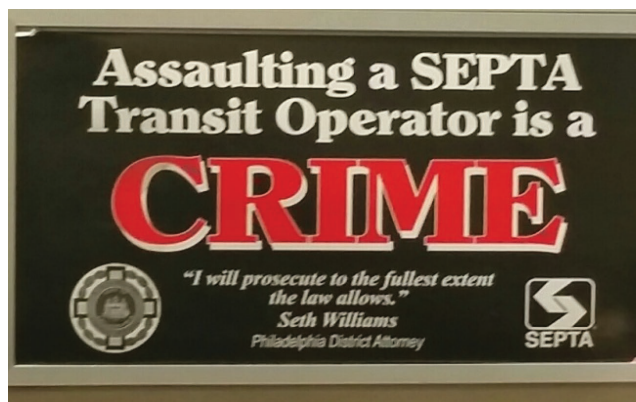
### **Aggravated Assault, Simple Assault, and Harassment**

The highest consequence security issue that small- and medium-sized transit agencies must confront on a daily basis is the potential for employees to be assaulted while performing their duties. Although lesser crimes or violations may occur more frequently, by and large the most significant criminal threat outside of homicide that the transit agency will face is as an aggravated assault committed against an employee. See Figure 5.3.

Based on the service profiles described previously, small- and medium-sized agencies are typically bus-only, or a combination of bus, trolley, van, and other non-railed vehicles, including paratransit. These conveyances are driven by an operator who is the public-facing point of contact for the transit agency. Transit operators engage the public, both law-abiding citizens and criminals alike, on a continuing basis. They are also confronted with mentally disabled persons who may or may not exhibit hostile behaviors. Transit operators are almost always alone on board a vehicle without any secondary response personnel to provide timely aid or assistance. In 2012 the Amalgamated Transit Union (ATU) developed a factsheet for local unions entitled *Preventing Violence against Bus Operators* (ATU 2012).

The fact sheet listed the following risk factors associated with operator assaults:

- Interacting directly with the public.
- Working alone or in isolated areas.



**Figure 5.3. Assault prevention (SEPTA = Southeastern Pennsylvania Transportation Authority).**

- Having a mobile workplace.
- Working late night or early morning hours.
- Working in high-crime areas.
- Providing services to people who may be experiencing frustration (for example, with fare increases or service reductions).
- Having a workplace where access is uncontrolled.
- Handling money or fares.
- Having enforcement responsibilities.
- Having inadequate escape routes.

Transit Cooperative Research Program Project F-21, “Tools and Strategies for Eliminating Assaults Against Transit Operators” (Countermeasures Assessments & Security Experts, LLC forthcoming), a route-factor threat and vulnerability matrix, was created consisting of 3 risk categories with associated considerations: (1) environmental, (2) operational, and (3) response (Table 5.1). Note that, in particular, the second category of “operational considerations” describes potential causal effect vulnerabilities that may result from problem conditions. The research,

**Table 5.1. Route factors, environmental considerations.**

ROUTE FACTORS	Threat	Vulnerability
Environmental Considerations		
1. Population Density Along the Route		X
2. Bars and Nightclubs		X
3. Past Incidents of Assault	X	
4. Route and Vehicle Capacities and Passenger Ridership Rates		X
5. Entertainment Venues Along the Route (stations, events, places of congregation)		X
6. Proximity to Crime Hotspots		X
7. Temporal Effects		X
8. Juvenile Crime	X	
9. Gang Activity	X	
10. Prostitution and Vice	X	
11. Drug Trade	X	
Operational Considerations		
12. Known Threats	X	
13. Measures in Place to Address Apparent Security Risks – Vehicle Security Countermeasures		X
14. Measures in Place To Address Apparent Security Risks – Operator Assault Security Countermeasures		X
15. Training and Skill Level of Operators and Crew/Development and Enforcement of Operator Safety-Related Rules and Policies	X	X
16. Delays in Schedule		X
17. Fleet Condition and Maintenance		X
18. Incident Reporting and Management Systems		X
19. Fare Structure and Disputes		X
20. Workplace Violence Policy and Procedure		X
Response Considerations		
21. Measures in Place To Address Apparent Security Risks – Security Personnel		X
22. Police or Security Response Capability Along The Route		X
23. Relationship with Local Law Enforcement		X
24. Passenger Security Inspections, Random Searches, Presence of Uniformed Personnel		X
25. Displacement of Crime	X	

which remains a work in process, looks at the presence or absence of threats, vulnerabilities, and assault reduction safeguards.

Subject to change, the following definitions are associated with the TCRP Project F-21 matrix:

- **Threat:** Natural or human-made occurrences, individuals, entities, or actions that will damage the system, its facilities, or its patrons. Security threats include any actions that detract from overall security. They range from the extreme of terrorist-initiated bombs to more common events such as theft of services, pickpocketing, graffiti, and vandalism. *Threats* for purposes of the TCRP Project F-21 are defined as specific activities that will cause harm to the transit system, its facilities, or its patrons. Generally, threat also considers the intent and feasibility of a specific type of attack (e.g., scenario).
- **Vulnerability:** The susceptibility of the system to a particular type of security hazard. Vulnerabilities can be corrected, but in the face of limited resources, a risk analysis is required to prioritize mitigation measures. Because transit systems may cover a vast amount of territory that is unprotected, aspects of the system may be vulnerable to terrorist attack. It is generally assumed that a system is vulnerable to a natural hazard event (earthquake, tornado, etc.) because the natural hazard cannot be prevented regardless of the countermeasure deployed.
- **Environment:** The human-made or human-altered space in which individuals live out their daily lives, through which transit navigates.
- **Operational:** A collection of activities that together assure that transit services are cost-effectively provided to meet the short-term mobility needs of a community.
- **Response:** Arrival of the police/security personnel at a location from which an alarm signal has been received. It can also refer to the length of time it takes the police/security personnel to respond to an alarm.

Small- and medium-sized transit systems should consider that assaults against an operator may take place. For the most part, the assault or perhaps harassment will be of lesser severity. *TCRP Synthesis 93: Practices to Protect Bus Operators from Passenger Assault* (Nakanishi and Fleming 2012) defines assault broadly as “overt physical and verbal acts of aggression by a passenger that interfere with the mission of a bus operator—to complete his or her scheduled run safely—and that adversely affect the safety of the operator and customers.” In the survey of transit agencies conducted in conjunction with *TCRP Synthesis 93*, 61 responses were received in which assault was further characterized (Table 5.2).

*TCRP Synthesis 93* provided insight into the types of assault that create the largest problem for transit agencies (Table 5.3). (Note also the commentary below that warns that minor assaults such as spitting are sometimes predecessor events to aggravated felony assault).

When asked which operator assault type(s) is or has recently been problematic for the responding agency, the assault type considered to be most problematic for agencies was verbal threats, intimidation, or harassment, as indicated in Table 3. This result mirrors those of workplace violence studies that indi-

**Table 5.2. Assault definitions.**

Definition	%
Aggravated assaults involving weapons	100
Simple assaults (e.g., kicking, punching)	100
Sexual assault	95
Spitting	84
Verbal threats/intimidation/harassment involving weapons	74
Projectiles thrown inside the bus (including liquids)	72
Verbal threats/intimidation/harassment without weapons	62
Projectiles thrown at the bus	48
Total Responses	61

**Table 5.3. Problematic assault types.**

Problematic Assault Type	%
Verbal threats/intimidation/harassment	81
Assaults involving spitting	60
Assaults involving projectiles thrown at the bus	38
Assaults involving projectiles thrown inside the bus (including liquids)	26
Assaults while vehicle is in motion	9
Assaults due to operator race/gender/size	5
Simple assault	3
Assaults involving weapons	2
Total Responses	58

cate that verbal attacks are the most common form of workplace violence. The next most problematic assault type was spitting. Although seemingly minor, being spat upon can be temporarily traumatic to the victim. Also, because aggravated assaults that result in physical injuries can be preceded by minor assaults, even minor incidents need to be reported and closely monitored. Note that 100% of large agencies reported that they consider spitting to be problematic, whereas 70% of midsize and 26% of smaller agencies reported it as problematic.

## Revenue Security

Assuring that passengers pay their fare for riding on the bus, trolley, or train has been a chronic problem for transit agencies worldwide since the inception of pay-for-service ground transportation systems. In the United States, the necessary openness and accessibility of transit system design has spawned varied approaches by agencies to protect revenue. Bridging the countermeasures spectrum from turnstiles and hardened steel exit points of a system like the New York Subway, to the proof-of-payment honor systems of First Transit or the San Diego Transit system, fare evasion or avoidance strategies range from being timeworn and tested to technologically innovative and even experimental. Failure to pay fare is a crime, generally called “fraud” in most jurisdictions. And criminals are becoming just as sophisticated and innovative in finding ways to defeat fare collection systems as transit agencies are in trying to defend them.

Fare evasion and fare theft are reported as major security problems at many transit systems. Fare evasion, as defined in the NTD is “the unlawful use of transit facilities by riding without paying the applicable fare.” Some of the terms used by transit agencies to specifically describe fare evasion include, misuse of tickets, fare evasion, and counterfeiting and forgery of fare media. As stated in *Transit Security: A Description of Problems and Countermeasures* (Mauri et al. 1997), there are many forms of fare evasion and fare theft. Table 5.4 contains examples of the types of fare evasion tactics.

## Transit Equipment and Property Protection

Protecting against losses associated with the property and infrastructure of transit systems is largely a matter of controlling theft and vandalism. These 2 primary areas of security-related concerns demand attention at most agencies on an ongoing basis. Theft can take the form of both internal pilferages by employees or through externally caused losses by individuals who target valuable materials used by public transit agencies.

### Internal Theft

Although sometimes employees are literally caught in the act of stealing from their employers, typically employee theft is often first detected through findings associated with shrinkage

**Table 5.4. Forms of fare evasion and fare theft.**

<p><b>Fare Payment Avoidance</b>—Payment procedures typically require passage through some barrier, either physical or human. The fare evader searches for opportunities to avoid or surmount this barrier. On a bus, with the operator monitoring the payment of fares, fare evaders use avoidance techniques such as entering the vehicle through the rear door or boarding with a large group hoping to avoid detection.</p>	<p><b>Shortchanging</b>—"Shorting the box" is a common method of fare evasion. In this case, the passenger deposits a collection of coins into the fare box that amounts to something less than the full fare. If the driver is unable or unwilling to verify the amount deposited, the passenger rides at a discount. There is little risk for the fare evader. If challenged, the shortchanger simply pretends to have erred and deposits the balance of the fare.</p>
<p><b>Refusal to Pay</b>—The fare evader refuses to pay the fare. In many circumstances, the operator, intimidated by the situation, will allow the fare evasion to occur rather than cause a confrontation or risk an assault.</p>	<p><b>Misuse of Fare Media</b>—Mass transit systems allow a variety of fare media to be used for fare payment. In addition to cash, fare media include tokens, tickets, transfers, and passes. Deliberate misuse or falsification of fare media is a common form of fare evasion.</p>
<p><b>Discounted Fares</b>—Transit systems often sell passes at a substantial discount to youths, students, the elderly, and the disabled. Unauthorized persons attempt to use these passes to gain entrance to the system at a reduced rate.</p>	<p><b>"Two Ticket Scam"</b>—In transit systems that determine fare rates based upon trip length, regular users can carry a set of fare tickets from various points throughout the system to "shorten" the ride and reduce the fare.</p>
<p><b>Tampering with Automated Fare Collection (AFC) Machines</b>—AFC ticket vending machines have not proven to be tamperproof.</p>	<p><b>Alteration of Magnetic Fare Cards</b>—Transit users with access to the proper equipment can and do alter the value of their magnetic fare cards. Magnetic fare tickets can also be easily demagnetized. The transit system will usually refund the remaining value of the ticket in this situation on the assumption that the demagnetization was accidental.</p>
<p><b>Swipe-sellers</b>—as the hustlers are called, commonly jam the bill slot in metro card machines to force riders to buy a "swipe" to get past the turnstile. They charge anywhere from \$1 to \$2. The fare is \$2.50. They exploit flaws in discarded cards that allow someone to get through after repeatedly swiping it, or they charge people to go through a service gate.</p>	<p><b>"Strip split"</b>—someone buys a fare card, cuts out the magnetic strip and splits it lengthwise up to 4 times. Then the pieces are glued to a regular demagnetized fare card and turned in. The crook adds a nickel or so to the fare card clone, and out pops a new genuine fare card worth the full amount. The new cards are then sold on the black market.</p>
<p>People who receive a transit subsidy and don't end up using it all can illegally sell their surplus subsidy on the black market.</p>	<p>Fare card <b>"sleight of hand."</b>—The thief usually helps the tourist through a turnstile or cage and then swipes their card for them, and hands back a worthless card in exchange.</p>
<p>For transit systems using the <b>proof-of-payment</b> or <b>"honor system"</b> evaders just ride without paying and hope they don't get caught, or they can make a break for it when they see a fare checker coming.</p>	<p><b>Fare media counterfeiting</b>—includes currency, passes, tickets, transfers, and tokens. The counterfeiting of transit passes ranges in sophistication from simple photocopying to careful reprinting. Monthly or yearly passes often inspire careful and expensive counterfeiting efforts.</p>

uncovered through the transit agency's audit or inventory program that identifies shortages or missing materials from warehouses, depots, or other maintenance facilities. However, just because shrinkage is identified, it does not always follow that larceny of property is detected or even investigated. Depending on the effectiveness of inventory control systems, stealing from the transit agency may occur unchecked if appropriate safeguards or security measures are not in place to prevent or deter them. Unfortunately, in many instances, action is only taken when the incidents become widespread or the loss becomes intolerable.

Generally the intent of pilferage is to obtain items or property with high resale value. Spare parts at bus or paratransit systems, including radiators, transmissions, engines, voltage regulators, fuel injectors, alternators, and starters, represent high-value automotive materials that can be sold for a profit to receivers of stolen goods. Similarly, although not as costly, consumable auto parts such as oil, tires, spark plugs, anti-freeze, paint, batteries, and even fuel can also “go missing” on a frequent basis. These types of theft or losses are often written off as normal use of materials making them virtually undetectable. Hand and power tools, air compressors, generators, or other types of repair equipment represent a third type of transit system property that may end up stolen and result in costly replacement.

Preventing internal fraud, sometimes called “white collar crime” is also a matter for consideration by transit agencies. While information about the occurrence of this type of security risk is often closely held, there are numerous instances of agency employees illegally converting goods purchased with company credit cards or purchase orders to either personal use or for resale.

## External Theft

While the random hijacking or joyride instance of bus vehicle theft continues to occur infrequently, the much more serious crime of grand theft of one or more buses from an agency’s fleet represents a high-value loss that can significantly impact the ability of the company to provide transportation services. Grand theft takes place when it is the intent of the taker to permanently deprive the owner of the use of the vehicle. The conveyance may be re-marked or painted, sold for scrap and parts, or otherwise disposed of. Agency’s that deploy school buses as a part of their fleet may experience a higher occurrence rate of grand theft of these types of vehicles.

But by far, the most prolific and costly occurrence of larceny from bus and rail transit systems alike is the stealing of metals, including copper, mercury, brass, or iron from vehicles, facilities, or rights-of-way. In particular copper, once overlooked by thieves as having little value, has skyrocketed as a preferred resale metal because of a surge in price on international markets. Nine years ago, copper futures traded at 80 cents a pound on the Chicago Mercantile Exchange. By 2006, they were at 4 dollars a pound. They are now trading at about 3 dollars a pound, lower than 7 years ago but still 375% higher than 2003. On its website, the FBI says copper theft is “threatening U.S. critical infrastructure by targeting electrical substations, cellular towers, telephone land lines, railroads, water wells, construction sites, and vacant homes for lucrative profits” (FBI 2008). According to a 2011 U.S. Department of Energy report, the theft of copper in the United States has exceeded 1 billion dollars.

Transit agencies offering light rail or commuter rail services are more likely targets of copper thieves because of the large amount of unprotected or minimally protected infrastructure that contain the metal. Copper is the metal of choice and is present in right-of-way transit signal systems, overhead contact wires, electrical relay switches, power and transmission lines, and telecommunications links ([www.copper.org](http://www.copper.org)). In 2012, 1 transit agency reported that approximately 4.2 miles and 70,000 pounds of copper wire had been stolen from within its hollow elevated guideway. The theft was valued at well over \$200,000 (Shaner 2012).

Large amounts of copper are also present in transportation vehicles. A typical, diesel-electric railroad locomotive uses about 11,000 pounds of copper. More than 16,000 pounds (8 tons) of copper is used in the latest and most-powerful locomotives manufactured by General Electric Company and General Motors Corporation. Electrically powered subway cars, trolleys, and buses use from 625 pounds to 9,200 pounds of copper each, for a weighted average of 2,300 pounds apiece. Copper is an essential component in the motors, wiring, radiators, connectors, brakes, and bearings used in cars and trucks. The average car contains 1.5 kilometers (0.9 mile) of copper wire, and



the total amount of copper ranges from 20 kilograms (44 pounds) in small cars to 45 kilograms (99 pounds) in luxury and hybrid vehicles ([www.copper.org](http://www.copper.org)).

Transit facilities are also subject to metal theft because copper has been, and continues to be, a main component used in building construction for electrical wiring, plumbing, heating and cooling systems, refrigeration units, and telecommunications links. In particular, unstaffed, unattended, or even abandoned buildings or structures are a likely target for metal thieves who commit break-ins seeking to strip out copper for sales to scrap dealers.

Metal theft can have significant secondary impacts on the operation of a public transit system. In California, the state legislature made findings in this regard in the passage of *Assembly Bill No. 1971—An Act to Amend Section 496a of, and to Add Section 594.05 to, the Penal Code, Relating to Theft (California Assembly 2012)*.

SECTION 1. The Legislature finds and declares all of the following:

- (a) The theft of nonferrous materials, such as copper, copper alloys, stainless steel, and aluminum, but excluding beverage containers, is a serious problem in many parts of California.
- (b) The theft of these metals is having a significant negative effect on many public agencies throughout the state, including public transit providers.
- (c) Frequently, the cost of repairing or replacing the infrastructure, component, or item from which the metal has been removed greatly exceeds the value of the metal itself.
- (d) This criminal activity is costing public transit systems millions of dollars annually.
- (e) These crimes can greatly affect the efficiency of transit providers, causing significant vehicle speed reductions, service disruptions, and delays.
- (f) The theft of nonferrous materials from public transit systems also poses a significant threat to public safety.
- (g) The theft of these metals may result in the loss of power to critical elements of the transit system and to related communications, lighting, and other portions of the system.
- (h) Stolen cable can create dangerous conditions as stray electrical current is conducted through other metals, creating heat in adjacent metals, and damaging the integrity of the system in the area of theft.
- (i) In addition to the possible dangers posed to employees and the transit-riding public, thieves engaged in these crimes are exposed to serious injury or death through possible electrocution.

## Vandalism and Graffiti

Headlines across the United States continue to confirm that the vandalism of transit vehicles, bus shelters and bus depots is a perpetual problem that is extremely difficult to resolve or overcome. Even with recent advances in construction materials (graffiti resistant) (anti-etch materials) losses remain in the millions of dollars with multiple events of vandalism known to occur on systems. These events can sometimes take the form of crime sprees with dozens of vehicles in a depot damaged or subjected to graffiti, or an entire neighborhood's transit bus shelters being damaged or destroyed during a single overnight period. Often times vandalism is perpetrated by juveniles acting in concert. In particular graffiti can take this form.

The NTD collects information about arrests associated with the vandalism of transit properties categorizing incidents based on location of occurrence. The breakdown includes vandalism of (1) transit vehicles; (2) transit stations; (3) non-revenue facilities; and (4) roadway, right-of-way and parking facilities. The NTD defines vandalism as the willful or malicious destruction or defacement of transit property or vehicles. According to the NTD, it includes “a broad range of injury to property, from deliberate, extensive destruction of property at one extreme to mischievous, less extensive damage at the other extreme.” Property damage resulting from these offenses as well as the number of arrests is reported.

Acts of vandalism can include:

- Damage to trash receptacles at bus or rail terminals.
- Inking, spray paint, or markers.
- Scratching, etching, or scribing windows.
- “Artwork” and tagging.
- Smashing windows on buses or shelters.
- Cutting, severing signal communications lines.
- Damage to fare gates.
- Disabling fare machines.
- Shooting of BBs, pellets, or other projectiles at vehicles.
- Destruction of turnstiles.
- Cuts, slashes, or tears in vinyl or other seat coverings.
- Burns from cigarettes, matches, or lighters.
- Splashing caustic chemicals on bus shelters.
- Damaging restroom facilities.
- Deflating, cutting valve stems or slashing tires.
- Spraying fire extinguishers.
- Missiling, throwing hard objects at vehicles.
- Track switch tampering.

The annual costs of vandalism in the United States remains an elusive number based on a lack of aggregate information or statistics. However graffiti cleanup costs alone are significant. A report on the subject published in 2002 by researchers at the U.S. Department of Justice stated, “there are huge public costs associated with graffiti: an estimated \$12 billion a year is spent cleaning up graffiti in the United States. Graffiti contributes to lost revenue associated with reduced ridership on transit systems, reduced retail sales and declines in property value. In addition, graffiti generates the perception of blight and heightens fear of gang activity” (Lamm Weisel Guide No. 9). In 2006, a survey from a variety of cities across the U.S. suggests that graffiti cleanup alone costs taxpayers about \$1–3 per person each year. For smaller communities the amount dedicated to graffiti cleanup annually may be less than \$1 per person.

All graffiti is not alike, even though the consequences are. The information Table 5.5 was adapted from the National Council to Prevent Delinquency (NCPD). ([www.anti-graffiti.org](http://www.anti-graffiti.org))

**Table 5.5. Graffiti description.**

Graffiti Description	Perpetrator	Rate of Occurrence
A “tag” is the graffiti vandal’s moniker applied quickly and repetitively.	Non-Gang	80%
A “throw-up” is a more elaborate tag, usually done in 2 or more colors. Vandals often use balloon letters, which are filled in or left as outlines.	Non-Gang	5%
“Pieces,” short for “masterpieces,” are large, detailed drawings. They are colorful, can include cartoon-like characters, and may take hours or more to complete.	Non-Gang	5%
Conventional or generic graffiti includes random markings, initials, declarations of love, social commentary, profanity, and other non-threatening messages. Generic graffiti has no particular style.	Non-Gang	*
Ideological or hate graffiti is any racial, religious, or cultural slur.	Non-Gang	*
Gang graffiti is used to mark gang territory, list members, offer drugs or contraband for sale, or send warnings to rivals. It may include letters, symbols, or numbers known only by gangs and law enforcement.	Gang	10%

\*Breakdown unknown.

### Spotlight on Graffiti

**San Diego, CA** – Metropolitan Transit System (MTS) undercover security operations arrested 5 juveniles in the past 2 weeks who are responsible for 277 individual tags covering 3,580 square feet and damage estimated at more than \$25,000. According to Paul Jablonski, Chief Executive Officer of MTS, “Each year we have close to \$1 million in costs to repair vandalism on our bus and trolley vehicles as well as to our property along our rail lines.” (Press Release March 6, 2012 MTS Website [www.sdmts.com](http://www.sdmts.com))

**New York, NY** – Members of MTA New York City Transit’s Eagle Team joined with members of New York’s Finest to erase a graffiti vandal who had trespassed into a Bronx subway yard shortly after midnight on Monday and spray painted a pair of subway cars as they sat waiting for the morning rush period. Painted vandalism costs the MTA approximately \$1 million a year to remove. This is money that could be far better spent elsewhere, and don’t forget, graffiti removal keeps trains out of service while they are being cleaned. Additionally, in order to reach the trains, which are often “hit” in lay-up areas, these vandals put themselves at great risk of serious injury or even death. (Press Release June 27, 2014 MTA Website [www.mta.info](http://www.mta.info))

**Ann Arbor, MI** – The Ann Arbor Community Center is without the use of its bus for transporting children in its summer day camp on field trips after a vandal or vandals covered one side of it with graffiti. The Rev. Yolanda Whiten, president and CEO of the Ann Arbor Community Center, said the bus was parked for the long weekend the evening of July 3, but on the morning of July 7, she noticed black, white and some red paint scrawled across one side of the vehicle. The community center had to cancel part of a field trip that day because Whiten and other camp officials did not want the children on the graffiti-covered bus. Whiten estimated that it will cost several thousand dollars to get the paint removed, as volunteers worked scrubbing the paint on the bus and were not able to remove it. (July 10, 2014 [www.mlive.com](http://www.mlive.com))

**Gary, IN** – Northern Indiana Commuter Transportation District police are asking for the public’s help in identifying 2 suspects who allegedly fired a handgun at glass partitions at the Gary Metro station Monday. At 2 p.m. Monday, security cameras captured images of 2 men wearing winter clothing firing a handgun at glass partitions on the train platform. Another window inside the Adam Benjamin Metro Center was damaged by gunfire as well. Police believe a BB or pellet gun was used in the shootings, which led to \$2,000 in damages. (February 21, 2014 [www.nwitimes.com](http://www.nwitimes.com))

**San Francisco, CA** – Thousands of baseball fans took to the streets of San Francisco to celebrate the Giants’ World Series victory, with revelers gathering on corners, in parks and at watering holes — and some turning rowdy. Some violence and vandalism was reported, with revelers setting a public transit bus on fire, flipping over a vehicle and breaking the windows of several businesses and vehicles. (October 29, 2012 Associated Press)

**Eagan, MN** – Passengers who board Minnesota Valley Transit Authority buses at the Eagan Transit Station may be wondering when the restrooms will reopen. “Hopefully soon,” said spokeswoman Robin Selvig. The restrooms have been locked for a couple of weeks due to vandalism and property damage inside the station at Pilot Knob Road and Yankee Doodle Road. Selvig said somebody had been putting rocks down the toilet, which led to plumbing problems, and that a homeless person may have been using them for shelter. (August 6, 2014 [www.startribune.com](http://www.startribune.com))

## Fraud Prevention

Transit fraud schemes can include (1) bid rigging, (2) price fixing, (3) goods and materials substitution, (4) bribery and kickbacks, (5) false claims, and (6) labor and materials overbilling. Employee participation in such cases is rarely reported. Fraud can result in significant revenue loss, higher costs for goods or services, opportunity costs, overruns, project delays through shortages, shoddy materials or workmanship, funding shortfalls, and loss of goodwill or public trust.

Bid rigging occurs when contractors act in collusion to increase profit. There is a misrepresentation that bidders are in competition with one another when, in fact, they have predetermined who will win the bid and at what is often a highly inflated price. Price fixing consists of competitors acting in unison to set the prices at which their goods or services are sold. Bribery is the act of giving money or gift giving that alters the behavior of the recipient, where the gift is of a dishonest nature. Bribery is defined by *Black's Law Dictionary* as the "offering, giving, receiving, or soliciting of any item of value to influence the actions of an official or other person in charge of a public or legal duty." A kickback is money, goods or services paid "under the table" by a contractor or subcontractor for referral of business for a contract. False claims are the intentional use of inaccurate records or statements to obtain unearned payments for goods or services rendered. And, finally, overbilling fraud consists of contractors charging for work not performed, or submitting inflated invoices for a greater amount of work than what was actually performed. Contractors can also commit overbilling by charging off inventory usage of goods or materials not used on a job or falsifying the amount of materials actually used.

## Homeland Security Issues

The following information describes the major homeland security-/homeland defense-related threats facing public transit systems:

*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 some paints are a serious health threat and may cause death. Smoke can reduce visibility, obscuring exit pathways and making escape more difficult for victims. Fires may be intentional or accidental, and 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*—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 while the fireball may ignite other building materials leading to a larger fire. Explosives can cause the destruction of assets within a facility, structural damage to the facility itself, and injuries or fatalities. Explosions may start a fire, which may inflict additional damage and cause additional injuries and fatalities. The type and amount of explosive material used and location of the explosion will determine the overall impact of the explosives.

*WMDs*—WMDs are nuclear, radiological, chemical, and/or biological weapons capable of inflicting mass casualties. Radioactive materials and other contaminants in different forms such as powders, liquids, gases, and dirty bombs that are intended to harm large numbers of people are also examples of WMDs. Potential hazards resulting from WMDs include fatalities, negative health effects, and permanent or temporary contamination of a facility. Because many WMD

materials have little discernible characteristics, symptoms are the first sign of an attack. In addition, some chemical and biological agents will not produce symptoms for hours or days after the attack has occurred.

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

*Tampering*—Tampering refers to interfering with the property of another person or organization with the intent to cause inconvenience or harm. Malicious tampering can facilitate the accomplishment of the other threat events such as tampering with subway track causing derailment. Transit infrastructure may be damaged by a truck, boat, or airplane carrying explosives to induce structural damage and fatalities and injuries to its users. Tampering with electrical systems can cause power loss wreaking havoc on transit operations, especially subway/rail operations, which rely on electrical power.

*Power Loss*—Loss of or disturbances to electrical power, locally or regionally, can significantly disrupt transit service and operations by diminished or suspended operations control and signal systems, computer-aided dispatch, and radio systems. Loss of power may be caused by an intentional or unintentional event aimed at the transit system or nearby targets. Power losses can affect not just the transit operations but also those in the surrounding 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 also be an attractive weapon or vehicle for carrying out terrorist operations, due to its familiar and innocuous nature.

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

(Source: Adapted from Rabkin et al. 2004.)

# Police and Security Staffing

## Security Forces

Decisions about the deployment of security forces can be difficult for transit agencies that are experiencing security-related problems at either their stations, on board conveyances, or along their routes. The reason is that adding personnel for any purpose is often the most costly operating expenditure that the agency will face. It is therefore prudent for small- and medium-sized transit agencies to exercise caution in determining security personnel requirements.

Not surprisingly, relatively few small- or medium-sized transit agencies feel the need to maintain a dedicated agency police or security force. Less than 13% of small agencies and 17% of medium-sized agencies surveyed indicated that personnel assigned specifically to perform security work were included in the operating budget. This decision not to deploy dedicated security is consistent with the crime and disorder-related findings of this research project that disclose a minimal levels security-related risk for small- and medium-sized agencies.

Typically small agencies depend exclusively upon local law enforcement random patrol for security support. Only one agency out of 62 reported hiring an off-duty police officer part-time to work on property. Forty percent (40%) of medium-sized agencies utilize either local police on dedicated patrol; a mixture of local police and contracted security; or off-duty, part-time police personnel. See Table 6.1.

Expenditures for overall security parallel the statistics with roughly half of both small- and medium-sized agencies reporting that they do not have a budget for security. Agencies that do budget for security generally spend less than \$25,000 on an annual basis. See Figure 6.1.

As mentioned previously and as graphically portrayed in the Security Countermeasures Cost Scale below, Figure 6.2, the costs associated with deploying personnel can be the most expensive security countermeasure a transit agency can undertake, but clearly, depending on the threats and unresolved vulnerabilities facing the organization, security personnel are often the most critical and significant resource available to reduce security-related risk. Unlike any other security countermeasure or technology, personnel provide the one vital capability for which there is no substitution—the ability to comprehend and apply reason. Security personnel bring the capacity to perceive the true nature of a threat and to recognize ongoing aggressor tactics. When adequately armed or reinforced, they can repel or overcome the use of deadly force by responding with equal or greater force to neutralize the threat or activity. This factor alone is predominate in both the homeland security and public safety context. Absent a response force, aggressors or criminals would quickly disregard other security countermeasures as irrelevant.

Determining the necessity for security personnel or the extent to which forces should be deployed is dependent upon the nature of the threats facing the agency, primarily based on issues such as size, population served, and operating locale. Statistics support a view that transit

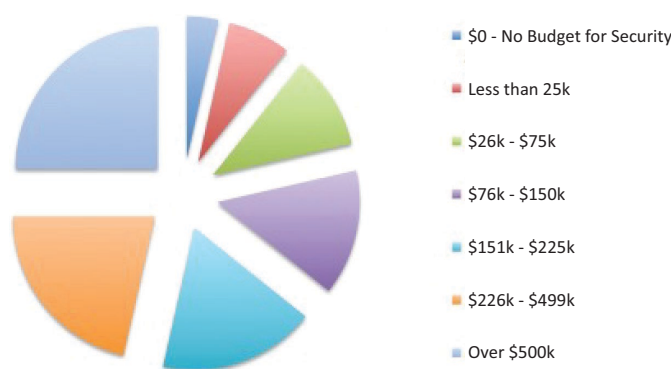
**Table 6.1. Security personnel.**

SECURITY PERSONNEL	SMALL	MEDIUM
Local Police Random Patrol	95%	77%
Contracted Security and Dedicated Local Police Patrol	1%	30%
Off-Duty Police Part-Time	>1%	9%

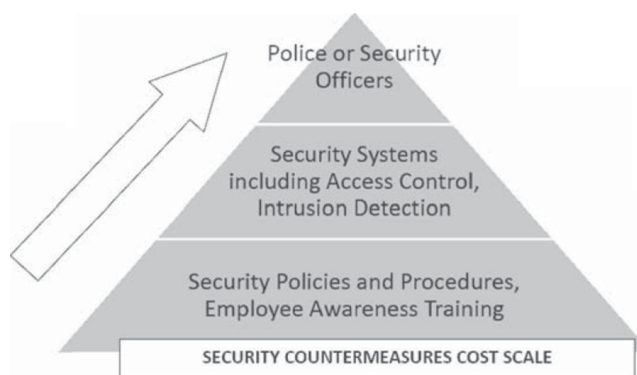
systems operating in high density population areas are likely at higher risk of crime or disorder than more rural systems. For example, FBI crime statistics recorded for calendar year 2009 disclosed that of the 806,843 total aggravated assaults committed, 701,454 (86.9%) occurred in metropolitan areas; 57,750 (7.2%) occurred in cities outside metropolitan areas; and 47,639 (5.9%) occurred in nonmetropolitan counties. Rates of aggravated assault were greatest in the South (44.5%). The Northeast (14.2%), Midwest (18.9%), and Western (22.5%) regions of the United States all have lower aggravated assault rates.

Other external factors also impact on security personnel decisions such as the availability of public safety response personnel in the operating area, what users or customers expect to see in terms of security, or whether other organizations in the industry use security personnel. Internal factors such as the agency’s history of deploying security forces or whether the organizational culture is tolerant of security restrictions will also have bearing.

As depicted in Figure 6.3, small- and medium-sized agency decision makers have an initial—spend or don’t spend—hurdle to clear in thinking about security personnel deployment. When



**Figure 6.1. Police and security staff annual budget.**



**Figure 6.2. Security countermeasures cost scale (Frazier et al. 2009).**

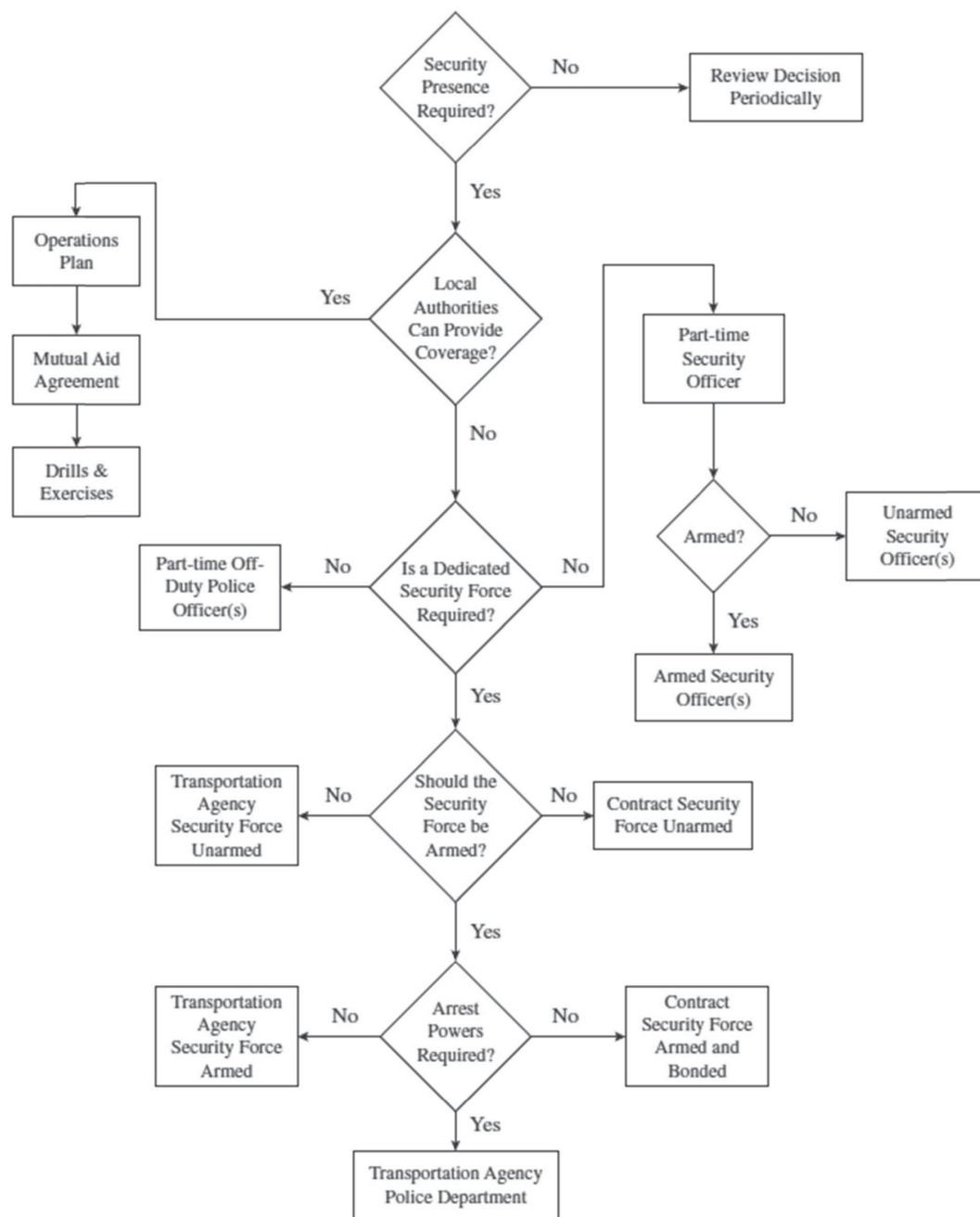


Figure 6.3. Transportation security force planning flowchart (Frazier et al. 2009).

the risks associated with crime or disorder rates are low or minimal, it is perfectly rational for a transit agency to decide that deploying a dedicated security force is not a cost-effective utilization of limited resources. In such circumstances, the agency should also be cognizant that isolated high-profile security events or incidents of major or serious crime may occur. If and when such events or incidents occur, the affected agency should be prepared to evaluate the impact of the occurrence on prior decisions and balance the security risk, including possible passenger or employee perceptions of a lack of security that may result. Note that spending operating dollars on security labor can be an easy decision for the agency to make at the outset, but a much harder decision to amend or withdraw. Those agencies that have previously deployed a security force can attest to the difficulties associated with eliminating a security presence even when that



presence is no longer warranted. *For this reason, any agency that has not yet made an investment in sustaining a security force will ideally use great care in ensuring that the rationale for security personnel staffing is objective and consistent with both an established threat profile and other organizational needs and requirements.* In the event that the agency determines that a security force is not required, a periodic review of this decision should be made in conjunction with ensuing risk assessments performed. The agency should also work toward achieving a written plan of security operations that documents the public safety service level and response contemplated.

For those small- and medium-sized transit agencies whose security risks suggest that a dedicated force may be warranted, the key question to be answered is whether a security presence, beyond what is available from the locale's public safety community, is necessary to protect the system and its users. Answering this question will require significant interaction with local law enforcement authorities to establish the level of protection and response to security incidents that can be expected. The transit agency should be prepared to discuss its operating characteristics, routes, staffing and other pertinent information with law enforcement representatives to assist in determining threats, vulnerabilities, and potential loss-related impacts of security events occurring on the system.

Figure 6.3 also describes relevant decision points for a transit agency that has objectively determined that dedicated security forces are required to protect its passengers, assets, and critical infrastructure. The diagram shows that there are a number of planning options that should be analyzed, starting with an assessment of what type of security personnel and equipment should be deployed.

The tradeoffs associated with these options have significant bearing on the transit agency's overall security posture. At one end of the available choices is the deployment of unarmed, part-time security officers, with no arrest authority. At the other end is the fielding of a full-time, armed police department with powers of arrest. Where the agency falls on this decision line will impact on the capabilities of not just the security labor force but also the performance and effectiveness of all other integrated system security countermeasures.

For those small- and medium-sized agencies that determine that a police presence is required, there are a number of representative approaches for deployment that should be considered. *TCRP Web Document 15 (Project F-6): Contractor's Final Report: Guidelines for the Effective Use of Uniformed Transit Police and Security Personnel* (Interactive Elements, Incorporated 1997) provides excellent examples of police deployment programs at some of the larger transit agencies in the United States. In some of the cases contracted, police were deployed. In others, a dedicated transit agency police force provided the response to the problem. The principal findings of the study were field-tested recommendations and guidelines for police and security management of parking lots, station quality-of-life concerns, and on-board, order-maintenance difficulties. Table 6.2 contains a synopsis of the programs. Although the information is somewhat dated the activities referenced remain consistent with transit policing problems and issues today. In fact many of the programs, or similar approaches to those listed continue to be utilized.

Irrespective of what underlying qualitative factors drive the decision about fielding security personnel, the best way to accurately make staffing *level* determinations is through the use of quantitative analysis. The *FTA's Security Manpower Planning Model (SMPM)* (Blake and Uccardi 2008) is a tool available to small- and medium-sized transit agencies to assist in making this determination. SMPM is an easy to use "what if" spreadsheet workbook available online at the FTA's website. It supports the entry of scenario-based data depicting police or security officer coverage levels. Inputs regarding the potential contracted use of security agency or part-time police personnel can also be entered along with fields for budget data that can be entered to establish summary costs that track

**Table 6.2. Police deployment programs at larger transit agencies.**

Agency Name, Program Area and Approach	Commentary
<b>MARTA Police Department (Atlanta)</b> <b>Security Challenges: A Focus on Park-N-Rides</b>	The Metropolitan Atlanta Rapid Transit Authority (MARTA) implemented bike patrols as a way to enhance visibility of officers at Lindbergh Station, a heavy rail station that is also a bus transfer point with 1,167 parking spaces in its open lot and 306 spaces in its parking deck. The station was the scene of a large number of thefts of and from autos. The strategy of assigning 2 uniformed officers on bike patrol resulted in a drop of 58.3 percent in Part I crimes during the test period.
<b>LIRR Police Department (New York)</b> <b>Auto Crime Unit: A Response to Parking Lot Crime</b>	The Long Island Rail Road (now MTA NY), developed a team of plainclothes officers to respond to escalating problems of auto theft. This apprehension-oriented unit of police officers made use of surveillance teams and borrowed vehicles to preclude easy recognition, but also used such problem-oriented techniques as commuter education and a Combat Auto Theft program to confront thefts.
<b>MetroLink (Los Angeles)</b> <b>Local Police Response to Park-N-Ride Crime</b>	MetroLink, the Los Angeles metropolitan area's commuter rail system, is policed by the Los Angeles County Sheriff's Department. Patrolling parking lots, though, is the responsibility of individual, local police departments. However, responding to a small amount of crime that was alarming to residents, the Claremont Police Department assigned a non-sworn, uniformed officer with a marked patrol car to a fixed post in the lot adjoining the historic rail station. Crime dropped to zero.
<b>San Diego Trolley System (San Diego)</b> <b>Comparing Security Perceptions and Storefront Patrol</b>	Faced with concerns by citizens that an extension of the San Diego Trolley to Santee would result in increased crime and disorder in their town, city managers contracted with the San Diego Sheriff's Department to staff a storefront substation. They also incorporated numerous Crime Prevention Through Environmental Design (CPTED) elements into the station. The resulting absence of crime and disorder was in contrast to the El Cajon Station, an older facility that suffered visible blight and that received no special attention at the time of its opening. The problems of recapturing the quality-of-life of a location were contrasted with steps to prevent disorder before it begins.
<b>NYPD (New York)</b> <b>Uniformed Officers Board Buses</b>	Uniformed New York City police officers rode or boarded buses in 2 boroughs to test the effects of this tactic on transit crime. A comparison of the 3-month test periods with the 2 previous years showed a drop in both criminal and non-criminal reported incidents. Although uniformed police officers are a rare sight on New York City buses, this test of police officer visibility attracted neither patron nor media comment.
<b>Houston Metro Police (Houston)</b> <b>Riding the Bus: Community Policing for Transit</b>	Houston's Metro Police assigned an officer to ride 2 bus lines sharing the same transfer point for 3 hours each week day. Crime and disorderly behavior was reduced substantially, but, more important, the officer's interactions with operators, patrons, teenagers, school officials, and business people along the routes are classic examples of the philosophy of community policing. This case study presents a specific methodology for incorporating proactive patrol into the transit environment.

to the selected scenario(s). The SMPM is a Microsoft Excel file that was developed using Excel 2003. All display and program menu items in this manual were written based on the behavior of the model under this version. The model is working and can be accessed at [http://www.fta.dot.gov/TSO/12527\\_13860.html](http://www.fta.dot.gov/TSO/12527_13860.html) as of July 2014. See Figure 6.4.

The SMPM Instruction Manual, also available on the FTA website, states that

The SMPM is a flexible decision support tool created to enable transit security planners the ability to assess impacts of strategic decisions on resources and staffing. Based on the data inputted, the model identifies staffing levels and budgeting. The SMPM is flexible in the sense that it can be used by any transit agency with existing or planned security resources, regardless of operating mode(s) or size. Further, the

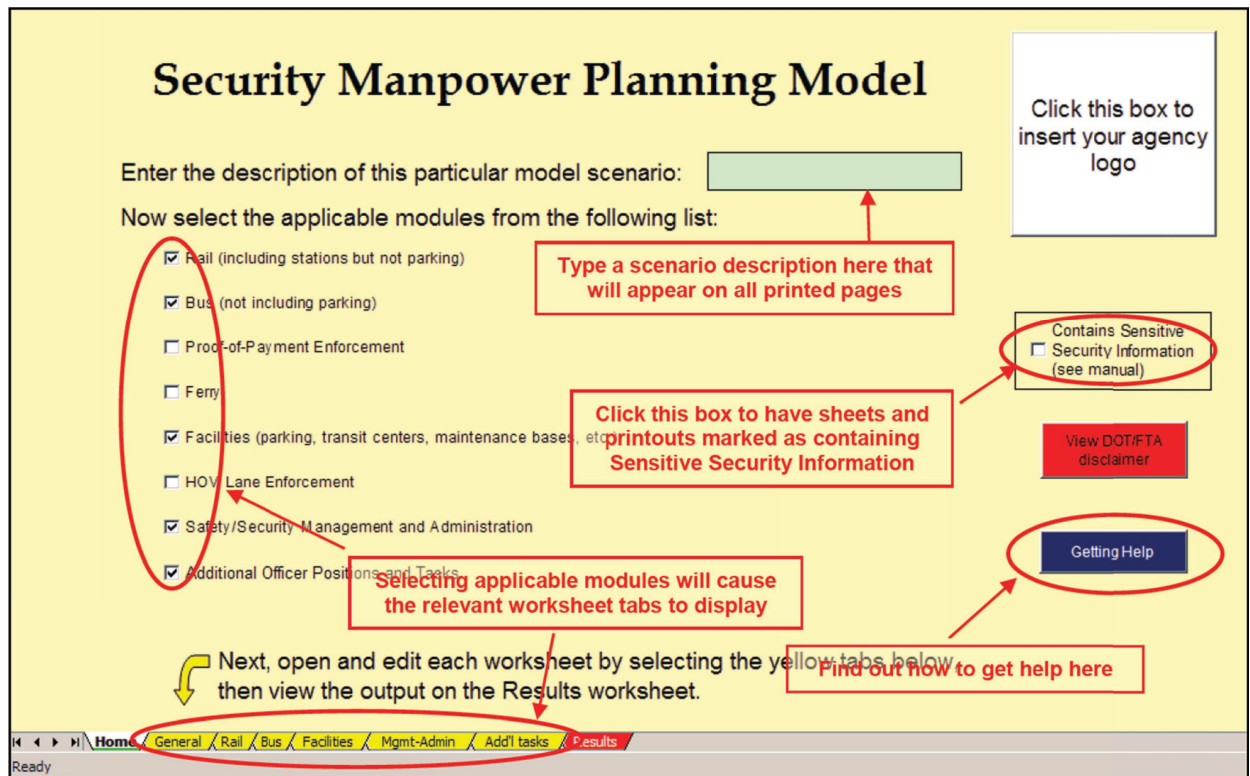


Figure 6.4. SMPM home screen.

model can assist security planners in assessing impacts of various scenarios on resource and deployment strategies including:

Changes in revenue service operations (e.g., adding a new rail line, re-structuring existing routes, or special event service planning).

Changes in ridership patterns, crime/incident rates and threat information.

Changes in security personnel configurations (e.g., alternative mixes of internal/external security resources).

Changes in how security forces are deployed.

Adjustments to security coverage levels.

Implementation of proof-of-payment fare enforcement or other related security duties.

Quantification of required security staffing levels may also be accomplished through the use of 1 or both of 2 alternative sets of data that should be available to the transit agency: (1) crime incident-based information, including both calls for service and self-initiated incident responses, and/or (2) security breach and scenario-driven information.

- **Crime and Disorder Incident-Based Information**—The first type of quantification requires close coordination with local law enforcement in the acquisition of crime and incident information. The law enforcement agency must have the ability to isolate transit agency calls for service and crime reports from those of the general jurisdictional area. This method, which is based on the capture and recording of actual security events is highly preferred as the means to correctly establish security personnel staffing levels, and perhaps more importantly, the true and accurate determination of the transit agency's security profile and risk.
- **Security Breach Information**—As mentioned previously, it is fortunate that from the quality of service perspective, most small- and medium-sized transit agencies experience a low level of

serious criminal incidents. Known as “Part 1 Crimes” in conformance with FBI UCR characterization criteria, crimes such as homicide, rape, robbery, aggravated assault, and arson occur so infrequently that the rate is often statistically insignificant from a crimes analysis standpoint. When the situation exists where quantifying serious crime data is inadequate to assist in establishing needed security staffing levels, the transit agency may be required to maintain its own records about the occurrence of lesser crimes and security incidents, including events such as public intoxication, trespass, fare evasion, vandalism, petit larceny, vagrancy, gang activity, disorderly conduct, or other security breaches on the system. In some instances, this may require the centralization of claims-related data, employee notifications, communications or dispatch center records, unusual occurrence reports, customer complaint information, labor union grievance submissions, or supervisor activity reports. Activity and occurrences can then be broken down by location, time of day, day of week, and other criteria. The information is then measured against acceptable standards as established by agency leadership at a level where risk is maintained within tolerable limits.

By extending this concept of data collection productivity quantification to those security-related issues that are most important to the agency, security planners can reasonably approximate how large the security force should be. It is worth repeating that other qualitative factors such as prior existing assignments of security or police to a given location will also have an impact on staffing decisions, but these subjective criteria should be recognized as an inefficient, albeit sometimes necessary method of allocating security forces. By assimilating threat assessment information into the productivity-driven quantification method discussed above, security planners can merge risk data with security operations data to minimize security vulnerabilities while at the same time obtaining a reasonable approximation of security force workflow.



## CHAPTER 7

# Security Countermeasures

In contrast to the much more extensive and costly security-related requirements necessary to protect large-sized transit agencies, the scope and extent of countermeasures warranted for small- and medium-sized agencies is correspondingly smaller. Basically the difference lies in the reduced infrastructure and critical asset footprint and operating characteristics of small- and medium-sized agencies. Because the vast majority of these agencies are limited to “rubber tire” vehicles and conveyances, the need to protect infrastructure components or systems such as communications and signal systems, electric power and transmission systems is lessened. Similarly buildings, maintenance depots, and other large capacity facilities required to support light rail or commuter rail surface transportation systems are not required to operate smaller “bus-only” systems, so the list of assets in need of protection is much lower. And finally, protecting dedicated rights-of-way, including critical infrastructure such as tunnels or subways, overhead or elevated structures, tracks, or wayside assets structures is typically not required at small- or medium-sized systems.

Lesser populations associated with the operating environment of small- and medium-sized agencies also contributes to the reduced need for security countermeasures. As previously discussed homeland security concerns, crime rates and the occurrence of security issues at smaller agencies are directly proportional to the size, scope, and location of the agency’s service area and the population served.

In summary, with a few exceptions, the small- and medium-sized transit agencies profiled in this study operate over the road with buses, trolleys, vans, or cars that require a level of security commensurate with the protection of (1) vehicles in transit on highways, rural and suburban city, borough, or township streets or other roadways; (2) infrastructure such as unstaffed bus shelters or bus stops, vehicle storage depots, bus stations, and maintenance facilities necessary to support these conveyances; (3) employees who operate the conveyances; (4) minimal administrative and management staff; and (4) the passengers who use the agency’s transportation services.

Under such circumstances, the security response associated with the protection of people, e.g., crimes against person, is mainly on-board-vehicle-focused with secondary concerns for transit system users who are along the roadside at shelters or bus stops awaiting the arrival of a transit vehicle. But even under this latter category, security is more so the responsibility of local authorities who have jurisdiction over what happens on the specific route. Property protection requirements are more expansive with security concerns related to both the interior and exterior of vehicles in transit, as well as in storage depots, bus shelters along transit routes, bus stations, administrative facilities, material and equipment storage areas, and more recently, fare collection machines located in publicly accessible venues.

## Protecting People On Board

Survey results for small- or medium-sized agencies indicate that the occurrence of crime, in particular violent crime, on board transit buses is an infrequent occurrence. Of the 172 total respondents, just under 85% reported no criminal activity whatsoever had occurred in the previous year period. However 1 homicide, 10 incidents of robbery, and 17 incidents of aggravated assault were reported, along with 2 sexual assaults (see Figure 7.1).

### Spotlight on On-Board Vehicle Security

(Charlotte Area Transit System, <http://charmeck.org/city/charlotte/cats/Bus/ridingcats/Pages/Code%20of%20Conduct.aspx>)

#### Riders Code of Conduct

*The following has been adapted from Charlotte Code Sec. 15-272 and 15-273. Any violation of these articles may be enforced by the issuance of a civil penalty in the amount of \$50 or by arrest.*

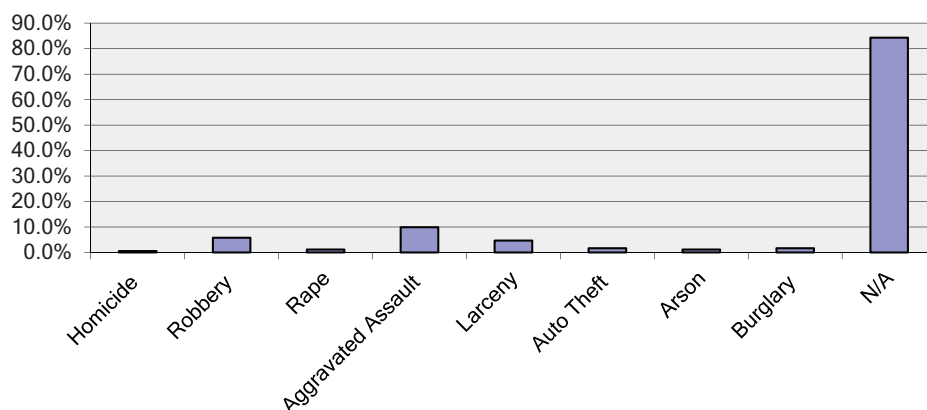
#### ACTS PROHIBITED

It is unlawful for any person to commit the following acts on a CATS or LYNX vehicle:

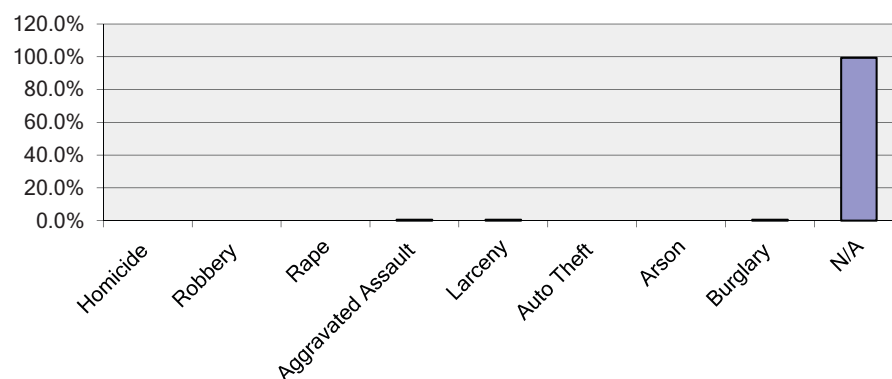
- Smoke or carry any lighted tobacco product or expel the residue of any other tobacco product including chewing tobacco
- Consume any alcoholic beverage or possess an open container of any alcoholic beverage
- Engage in disruptive, disturbing behavior including: loud conversation, profanity or rude insults, or operating any electronic device used for sound without an earphone(s)
- Take any animal onto a vehicle unless its purpose is to assist a person with a disability or in training activities
- Carry, possess or have within immediate access any dangerous weapon
- Possess or transport any flammable liquid, combustible material or other dangerous substance such as gasoline, kerosene or propane
- Litter
- Vandalize the vehicle or station platform by writing, marking, scribbling, defacing or causing damage to the vehicle or platform facilities in any manner
- Beg by forcing yourself upon another person
- Excrete any bodily fluid or spit upon or at another person on the vehicle or station platform
- Possess, use or sell any controlled substance
- Lying down on seats, benches or tables at stations and bus stops
- Standing, sitting or lying within 2 feet of the edge of the rail station platforms except for boarding and exiting the light rail vehicle
- Skating or skateboarding on station platforms
- Trespassing upon any area not open to the public and posted as such

Only 3 total crime incidents occurring on board trains were reported, which included 1 aggravated assault (see Figure 7.2).

## 54 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems



**Figure 7.1.** Criminal incidence—Part 1 crimes—location of incidents—bus.



**Figure 7.2.** Criminal incidence—Part 1 crimes—location of incidents—train.

## On-Board Vehicle Countermeasures

In contemplating the appropriate level of security needed to protect vehicle operators and passengers from violent offenses occurring on board a conveyance, small- and medium-sized agencies should first take into account the purpose and benefits of the various types of security countermeasures that are available. Security can be designed to prevent, deter, detect, mitigate, respond to, or recover from an incident. In the on-board vehicle context prevention, deterrence and response should take precedence from a planning standpoint with mitigation, detection, and recovery considered as close seconds. Definitions are provided in Table 7.1.

### Prevention

Unfortunately there are very few security measures available to prevent violence from occurring on board a transit vehicle. Buses are not reserved. They are public open access vehicles available for use by an unrestricted general population. Buses are populated by anonymous riders who present nothing more than a fare media or card to get on board. Typically, individuals who represent security risks are not pre-identified or barred from riding because their propensity to violence is generally unknown. There is virtually no screening for weapons or dangerous implements prior to boarding. Riders are placed in close proximity to one other, strangers, friends

**Table 7.1. Level of security.**

Purpose	Definition	Source
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act.	DHS National Infrastructure Protection Plan NIPP (DHS 2013)
Deterrence	An activity, procedure, or physical barrier that reduces the likelihood of an incident, attack, or criminal activity.	Transit Agency Security and Emergency Management Protective Measures (FTA 2006)
Detection	The identification and validation of potential threat or attack that is communicated to an appropriate authority that can act.	Transit Agency Security and Emergency Management Protective measures (FTA 2006)
Mitigation	The application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.	DHS Risk Lexicon (DHS 2008)
Response	Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.	DHS National Infrastructure Protection Plan NIPP (DHS 2013)
Recovery	The development, coordination, and execution of plans for impacted areas and operations.	Transit Agency Security and Emergency Management Protective measures (FTA 2006)

and associates alike with on and off access readily available in case a hasty retreat is required. In summary, the openness of public transit systems makes them virtually unprotectable using modern security technology.

In the absence of technology, the remaining option for preventing violence on board a conveyance is the deployment of security forces. Although this response is more so one of deterrence, it is technically possible to prevent an incident from occurring if security personnel are physically present and able to stop an ongoing attack or criminal assault.

## Deterrence

There are security countermeasures available to deter criminals or other would-be attackers from committing violence on board transit vehicles. As mentioned above, security forces can serve as a significant deterrent to violent crime. Security-related technologies can also greatly reduce both the perceived window of opportunity of an individual and the potential impact of his/her actions. See Table 7.2.

## Response

With respect to on-board violence from a security standpoint, the highest priority action that should be undertaken by small- and medium-sized transit agencies is to establish a robust capability and multi-layered capacity to respond immediately to the occurrence of either a threat of violence or a violent incident. The infrequent rate of occurrence, coupled with an inability to prevent all acts of violence leaves transit agencies in the conundrum of either deterring violent incidents or responding to them effectively. Deterrence as indicated in the table above is largely a matter of how the criminal or offender interprets the risk of apprehension or personal loss.



**Table 7.2. Security countermeasures.**

Countermeasure	Ease of Use	Deterrent Value	Cost
Police or Security Staffing On Board Conveyance	Easy	High—Security personnel bring the capacity to perceive the true nature of a threat and to recognize ongoing aggressor tactics. When adequately armed or reinforced, they can repel or overcome the use of deadly force by responding with equal or greater force to neutralize the threat or activity.	Very High
Visible Surveillance Systems	Medium	High—Readily evident CCTV creates a concern for offenders that they would be providing evidence that will lead to their apprehension. “Caught on camera” can have a tremendous deterrent impact.	High
Screening	Hard	High—Pre-boarding inspections can eliminate or reduce the use of dangerous weapons or other implements.	Very High
Physical Barriers—Compartment Barriers or Shielding	Medium	High—Driver/operators can be protected from assault.	High
Barring Systems	Difficult	High—Technology that identifies known aggressors who are then refused access to vehicles. Low-tech option would include providing operators with photos of offenders.	Low to Medium
Public Address System and Signage	Easy	Medium—Educating passengers and the public on safe actions to take; advising would-be criminals of the presence of security. Signs and warnings prohibiting guns, knives, scissors, etc. should be posted at the entry of the bus.	Low

However, in many cases, the offender is not making a rational decision in the first place when they commit a violent act. Offenders can be mentally disabled, emotionally wrought, under the influence of alcohol or drugs, or simply pathological, in which case security measures aimed at deterrence can have minimal if any impact.

Accomplishing this objective of immediate and effective response can be both demanding and costly. Indeed, the transit agency may need to weigh its tolerance for the infrequent occurrence of violent crime on board a conveyance against the daily effort and costs required to maintain a robust response capability and capacity. As shown in the survey, for the majority (85%) of small- and medium-sized agencies, this decision is based on circumstances in which their agencies are completely devoid of any criminal activity.

There are numerous types of countermeasures that can support the maintenance of an effective response program for on-board incidents. Many of these measures are low cost and/or low effort, consisting of policy responses, awareness and training, security planning, or coordination with local authorities. Because of the importance of the issue, it is suggested that all transit agencies, regardless of a lack of incidents or crime, engage at a minimum in these threshold security response activities. For those agencies that are experiencing periodic violence on board transit vehicles, additional efforts as listed should be undertaken. (It should also be noted that detection, mitigation, and recovery types of security actions are included in the response category). See Table 7.3.

**Table 7.3. Response and cost.**

Response Activities	Ease of Use	Response Value	Cost
Intelligence Information Sharing Cooperation	Medium	High—Working as a team with local planners, law enforcement and first responders. Requires the designation of a primary point of contact and dedication of significant time to maintain effective liaison.	Dollars—Low Time—High
Training, Drills Immediate Actions	Hard	High—Practicing with first responders on how to respond to and mitigate on-board vehicle violent incidents.	Dollars—High Time—High
Alarms, Panic Buttons with Police or Security Force Response	Medium	High—On-board vehicle emergency event notification technology coupled with immediate response by security forces. Vehicles with silent communication/emergency capability.	Dollars—Low Time—Very High
Surveillance with Immediate Police or Security Force Response	Hard	High—Real-time watching for suspicious activity on board vehicles remotely coupled with rapid response to incidents can create an observable omnipresent impact.	Dollars—High Time—Very High
Shadowing Vehicles	Hard	High—High visibility security patrols or bus field supervision provide immediate response capability.	Dollars—Medium Time—Medium
Remote Sensors with Police or Security Force Response	Hard	High—Sensor/pager systems can be installed to detect dangerous substances, such as radioactive or biohazardous material, and alert the operator or dispatch when the vehicle has been contaminated.	Dollars—High Time—Very High
Driver Operator Security Awareness Training	Easy	High—Train employees to monitor and observe people, events, activities, and items and take careful note of irregular or suspicious behavior.	Dollars—Low Time—Low
Driver Operator Security Training	Medium	High—Customer service, conflict mitigation, self-defense or assault prevention training. Training should be provided to all drivers concerning management of hostile passengers.	Dollars—Low Time—Low
Vehicle Locators Systems (AVLs)	Medium	High—Buses should have vehicle location systems (cell/satellite locators) to know a bus' actual location at any time from dispatch or some other centralized location.	Dollars—Medium Time—Low
Communication Protocol for Violent Incidents	Easy	High—Make sure all people involved in the communication process are trained and prepared for deployment of the process if and when necessary.	Dollars—Low Time—Low
Electronic Distress Signs	Easy	High—Emergency “Call Police” signs observable from the exterior of the vehicle.	Dollars—Low Time—Low
Personal Protective Equipment	Medium	Medium—Operator issued defensive weapons such as pepper spray. Requires policy and procedure promulgation as well as defensive tactics training.	Dollars—Medium Time—Medium
Real-Time Audio	Medium	Medium—Streaming audio.	Dollars—Medium Time—Medium
Violent Incident Emergency Response Plan	Easy	Medium—Hold-ups, hijacking, shootings, homicides, hostage situations, assaults and severe passenger disturbances on the bus.	Dollars—Low Time—Low

*(continued on next page)*

**Table 7.3. (Continued).**

Response Activities	Ease of Use	Response Value	Cost
Surveillance without Police or Security Force Response	Hard	Low—Event recording of incidents.	Dollars—High Time—Medium
Fire Suppression Equipment	Easy	Low—Mitigating or controlling the impact of an event in progress.	Dollars—Low Time—Low

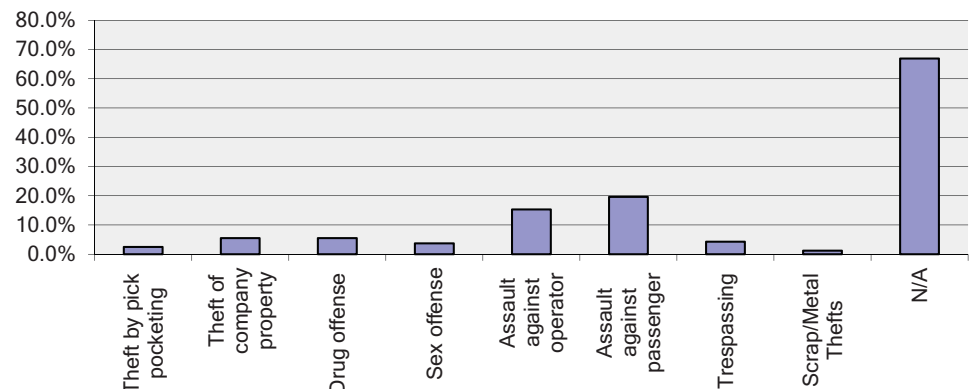
**Other On-Board Vehicle Incidents**

As disclosed in the survey, incidents of simple assault against a driver or passenger occur much more frequently than violent or aggravated assaults. 15.3% of agencies reported assaults against operators while 19.6% indicated they had experienced assaults against passengers. (See Figure 7.3.)

**Spotlight on Operator Assaults**

Public Awareness Campaigns, such as Septa’s Red Kite Training Program for Conflict Management, developed from a post-war community healing approach into a training model used internationally. The program uses trauma-informed crisis management as a means to de-escalate violence with those who have experienced it. Program tenets include a belief that teaching public-service workers the effects of trauma and how to de-escalate those who have experienced it is the key to community safety.

This training program is designed to help employees to be more aware and to show more understanding for individuals (the customers), by allowing them to understand self-importance, to show respect and to see the human factor, allowing them to focus on de-escalating potential problems before they happen. Operators participate in their training while learning they have choices in every interaction and how they can create a shift that can disarm a potentially difficult situation.



**Figure 7.3. Criminal incidence—other crimes—location of incidents—bus.**

Included in this category of on-board vehicle incidents would be incidents of nonviolent offensive touching or verbal assault. Black's Law Dictionary states, "an assault can be committed without actually touching, or striking or doing bodily harm, to the person of another." The dictionary defines assault as "any willful attempt or threat to inflict injury upon the person of another, when coupled with an apparent present ability so to do, and any intentional display of force such as would give the victim reason to fear or expect immediate bodily harm." Assault is sometimes confused with the crime of "battery" which is basically the use of illegal force—intentional and wrongful physical contact with a person without his or her consent that entails some injury or offensive touching—against another.

Of course countermeasures for lesser degree assaults occurring on board vehicles would be the same as for more violent events. But one type of simple assault that deserves particular attention by all transit agencies is spitting on vehicle operators. *TCRP Synthesis 93: Practices to Protect Bus Operators from Passenger Assault* (Nakanishi 2011) disclosed that concerns about incidents of spitting were second only to verbal threats or intimidation. 100% of large agencies, 70% of medium agencies, and 26% of small agencies considered spitting on operators to be problematic. A Metro Transit Authority of NY statistical report summed up the gist of the issue: "Of all the assaults that prompted a bus operator to take paid leave in 2009, a third of them, 51, 'involved a driver being spat upon.' . . . No weapon was involved in these episodes. 'Strictly spitting,' said Charles Seaton, a New York City Transit spokesman. And the encounters, while distressing, appeared to take a surprisingly severe toll: the 51 drivers who went on paid leave after a spitting incident took, on average, 64 days off work—the equivalent of 3 months with pay. One driver, who was not identified by the authority, spent 191 days on paid leave." (www.ndtv.com Michael M. Grynbaum, NYT News Service | Updated: May 25, 2010)

DNA swab "spit kits" are a recent countermeasure designed to combat the growing problem of spitting. Deployed first in England and now in Boston and soon to be in New York, DNA kits include swabs, a rinse, and a sealed container to store an assailant's saliva sample for purposes of later prosecution. At present the kits cost \$200.00 each.

The FBI maintains a national DNA database known as CODIS. CODIS is the acronym for the "Combined DNA Index System" and is the generic term used to describe the FBI's program of support for criminal justice DNA databases as well as the software used to run these databases. The CODIS system contains DNA profiles contributed by federal, state, and local participating forensic laboratories. As of June 2014, the National DNA Index (NDIS) contained over 11,015,147 offender profiles, 1,922,415 arrestee profiles, and 565,159 forensic profiles. CODIS's primary metric, the "Investigation Aided," tracks the number of criminal investigations where CODIS has added value to the investigative process. As of June 2014, CODIS has produced over 250,809 hits assisting in more than 239,317 investigations. (www.fbi.gov)

## Protecting People at Bus Stops

In a study of the 10 most dangerous bus stops in Los Angeles (Loukaitou-Sideris et al. 2001) the following summary was observed, "Bus stops are common settings for transit crime. They provide cover for criminals who can hang out waiting for victims without arousing suspicion. Bus stops are populated by anonymous riders, who represent easy targets. In their vicinity many bus stops had facilities, bars, liquor stores, ATMs typically known as crime generators."

Crime or violence at a bus stop is usually a matter for investigation and resolution by local authorities. Normally a small- or medium-sized agency would not be directly impacted by an event occurring at one of these locations. However, concern about the perception of passengers that an agency's bus stops are unsafe could adversely impact ridership. Prevalent crimes include

typically either those involving public nuisance or public offense (drinking in public, drug violations, lewd or disorderly conduct), or crimes against persons (petty thefts such as pickpocket or jewelry snatching, robbery, assault, or rape).

Anecdotally, it would not be unusual for a transit agency to be familiar with those locations along their bus routes where crime occurs. These locations, known as “hot spots,” usually possess certain environmental characteristics that create both opportunity for crime and concealment or routes of escape to preclude apprehension. To the extent practical transit agencies should consider bus stop or shelter placement and security taking the following factors into consideration. The environmental factors and the source for the empirical data are provided in Table 7.4.

In 2010 the American Public Transportation Association (APTA) published Recommended Practice (RP) SS-SIS-RP-008-10, *Bus Stop Design and Placement, Security Considerations* (APTA 2010). The RP recommends that a transit agency perform a security risk assessment of all bus

**Table 7.4. Environmental factors/sources.**

Environmental Factor	Source
Offenders want to avoid the risk of being seen while committing a crime. The possibility of surveillance by shop owners, managers, employees, guards, or caretakers has been found to have a strong effect in reducing crime.	Brantingham and Brantingham (1993)
Specific commercial uses are more likely to generate crime than others, especially if there is a high concentration of them in a limited area. The presence of a great number of liquor stores, bars, and taverns can have a negative effect on neighborhood crime.	Block and Block (1995)
Physical incivilities (trash, graffiti, abandoned buildings, disrepair, unkempt lots) and social incivilities (rowdy behavior, drug dealing, public drunkenness, prostitution, panhandling, and loitering) result in higher crime and resident fear. The relationship of physical incivilities to crime is expressed in the "broken window" thesis, popularized by Wilson and Kelling (1982). A broken window left unrepaired implies that social control is weak in an area. Potential offenders are more likely to act if they believe that no one is in control.	Skogan (1990) and Wilson and Kelling (1982)
Areas with vacant lots or buildings, public parks, and schools often attract youth and gang-related crime.	Perkins et al. (1992)
Crime rates are higher at intersections with alleys, midblock passages, multi-family housing, and undesirable establishments such as liquor stores and check cashing establishments, vacant buildings, and graffiti and litter. The proximity of undesirable establishments, particularly liquor stores, had a major negative impact on crime. The existence of graffiti and litter also aggravated crime incidence.	Loukaitou-Sideris et al. (2001)

stops in its system. The assessment should facilitate the use of CPTED, taking into account the need for natural surveillance, clear lines of sight, lighting, landscaping, natural access control, use and ownership, signage, physical barriers, selection of materials, CCTV utilization, communications systems, and passenger amenities such as weather protection and seating. The RP also suggests that the placement of stops and/or shelters should be based on the following criteria: (1) pedestrian traffic and demographic information, (2) passenger volume, (3) traffic volume and circulation, and (4) crime rate in area of the bus stop.

## Protecting Transit Properties

As mentioned previously the critical assets of small- and medium-sized agencies generally include vehicles, storage depots, bus shelters along transit routes, bus stations, administrative facilities, material and equipment storage areas, and more recently, fare collection machines located in publicly accessible venues.

### Spotlight on Fare Collection and Fare Evasion

There are many ways to pay a transit fare—Cash/Tokens/Tickets/Transfers/Daily Passes/Monthly Passes/Magnetic Swipe Cards/"Tap" Proximity Readers/Contactless "Open" Fare Payments, etc.

New technologies and ways of thinking are changing the way that fares are collected on transit systems. Electronic payment systems for mass transit agencies offer many benefits including ease of use, convenience for riders, security improvements, and reduced costs. Although methods for collecting cash fares remain a necessity for transit, there are ever increasing opportunities to allow passengers to use other forms of payment, including smart cards issued by the agency, debit or credit cards, or even smart phones to pay for their tickets.

Collecting fares is handled at many agencies through proof-of-payment "honor" systems that use revenue collection officers to check compliance. These systems are supported by vandal resistant ticket machines that are made available to riders at station stops or depots. Often, the machines are covered by remote surveillance cameras that send images to central stations.

In 2012, MBTA in Boston became the first transit agency to permit passengers to use smart phones to pay for tickets. Rather than spend large sums to outfit transit stops with new and improved ticket machines, the agency found a way to allow hand-held devices owned by system users to facilitate collection of revenue. Smart card-only fare boxes on vehicles are also being rolled out at different systems in the U.S. Cashless fare boxes are reliable, easily configurable, capable of processing all types of electronic fare media, and can interface with other devices or systems, including passenger count verification systems.

Non-electronic drop boxes placed on vehicles continue to allow for the secure acceptance of coins and bills while allowing the operator to visually count the amount received. Cash is later removed from the boxes at a secure location. Cash validating fare boxes reject invalid coins, tokens, and bills without visual inspection.

Support equipment for today's fare systems can include data systems, validation technology, counterfeit detection readers, vaulting systems, ticket vending machines, ticket office machines, and web-based acceptance configuration software.

A 2013 problem statement submitted to the TCRP titled *Transit Fare Evasion: Measurement, Prevention, Economics, and Societal Factors* postulates "while there is growing industry experience and statistics on this topic, resources are often obscure and considered an adjunct to research in law enforcement, security, fare collection, sociology, or financial audits. Information is not easily accessible or widely disseminated." The problem statement recommends "synthesis to provide comprehensive, issue-centric guidance for practitioners on how evasion can be measured, monitored, and minimized under an assortment of different fare policies, fare collection methodologies, and operations." The project proposes "to identify relationships between fare evasion rates and contributing factors, including inspection/ticket collection rates, penalty/on-board surcharge amounts, probability of getting cited or arrested, but also demographic factors (age, income, etc.), geography, and transportation fares." The proposal also seeks to "discuss experience with different countermeasures, surveillance, and prevention strategies."

## Vehicles and Conveyances

Protecting vehicles consists of securing rolling stock while in transit and at rest. While there are infrequent occasions when larceny of a bus is reported, the main issue of security concern is vandalism.

TRB's Transit Cooperative Research Program (TCRP) *Research Results Digest 9: Responding to Vandalism of Transit Bus and Rail Vehicle Passenger Windows* (TCRP 1996) chronicled the increase in breakage and smashing of bus windows that was becoming endemic in the late 90s rising by as much as 11% each year. In New York City alone, the MTA New York City Transit reported that properly maintaining vandal-etched bus and rail windows was costing the city \$60–70 million annually. The research digest identified a 3-part strategy for how to reduce the rate of incidence: (1) the development of repair techniques for the current system; (2) material solutions to the problem, i.e., materials or material systems that provide resistance to vandalism; and (3) prevention. Existing transparent window materials in use include safety glass, coated acrylic, and coated polycarbonate. Prevention includes police/security, maintenance, and operator involvement, as well as transit authority policies, punishment, legislation, surveillance, and other technologies. (See Tables 7.5 and 7.6.)

From a security standpoint preventing, deterring, or reducing incidents of vandalism to rolling stock must take into account the nature of the criminal, including those with a proclivity to engage in the acts of window smashing or shattering, destruction of other vehicle surfaces, or graffiti. Unfortunately in many, if not most instances, these types of acts are committed by juvenile offenders.

Protecting against juvenile crime for transit vehicles at rest can be accomplished by the imposition of a security inspection process and perimeter protection measures such as fencing, access control, and surveillance or intrusion detection technology. The National Transit Institute (NTI) published an excellent, *Employee Guide to System Safety and Security*, which contains

**Table 7.5. Repair approaches.**

Repair Approaches	Ease of Use	Cost
Easily procured replacements and easy maintenance, especially quick change-out of windows.	Easy	Low
Flat windows are widely available, and can be changed relatively easily between window material systems.	Easy	Low
Fixed windows are the most attractive from a maintenance standpoint.	Easy	Low
Refurbishment of acrylic windows removed from service, ground, polished, and recoated at a refurbishment/repair facility.	Medium	Low
Transom windows have been chosen as a compromise by many agencies for although they are more complex than fixed windows, they are less prone to failure than sliding windows.	Medium	Medium
Window systems that allow very fast change-out (5 min or less is desirable). To achieve quick change-out, these window systems may require items such as dry seals on the outboard side of the window and a clamped interior frame, which is removed easily after removal of a number of specialty head (e.g., Torx) quarter-turn fasteners.	Medium	Medium
Curved window panes, while aesthetically pleasing, have a number of inherent disadvantages including limited availability.	Hard	High
"Zero tolerance/no vehicle in service with graffiti" standard.	Hard	High
Sliding windows.	Hard	High

**Table 7.6. Material solutions.**

Material Solutions	Ease of Use	Cost
Sacrificial ply system, which is an inexpensive piece of plastic held to the window's interior side with two-sided tape, or is held in place by the window frame itself. These plies can be replaced quickly after being vandalized.	Easy	Low
Peel-ply protective film placed over the interior of the window. When this peel-ply is damaged, it is stripped off and replaced. Peel-ply products are also inexpensive, but do not change-out as quickly as the sacrificial ply products.	Easy	Low
Acrylic can be refurbished (ground, polished, and recoated) but it does not provide the impact protection of laminated safety glass or polycarbonate (acrylic fractures into large jagged pieces when broken). Acrylic is subject to hazing and crazing, it burns, and it requires a protective coating.	Medium	Medium
Polycarbonate provides superior impact resistance but its softness is susceptible to abrasion and scratching, as well as environmental and chemical attack, and it must have a protective coating.	Medium	Medium
Anti-spall films have been developed specifically to combat "smash and grab" robberies, car-jacking, and hurricanes. They are applied to the interior surface of glass windows to prevent glass spall (flying glass) when the window is damaged. In some cases, the relatively soft anti-spall film is further protection from carving and etching by a sacrificial acrylic ply.	Medium	Medium
Glass provides superior service life and is impervious to chemical attack, aging, and environment. Moreover, glass is the most difficult material to scratch. But its drawbacks are that it is heavy, cannot be refurbished easily, and has higher liability because of flying glass when a window breaks.	Medium	High
Polyurethane coatings and liners have been developed that increase the durability of plastic transparencies. Polyurethane liners have self-healing properties (gouges and imprints and abrasion damage disappear with time and/or with the application of heat).	Medium	High
Acrylic side window clad with a very thin (0.030 in.) chemically tempered glass ply. This glass does not shatter on impact and only retains damage at the impact site. The interlayer adhesive system prevents the glass from spalling.	Hard	High



**Table 7.7. Inspection points.**

Floors	Restrooms	Engine compartments
Below seats	Luggage compartments	Exhaust system
Operator's area	Lights	Fuel tanks
Steps	Wheel wells	Frame and underbody

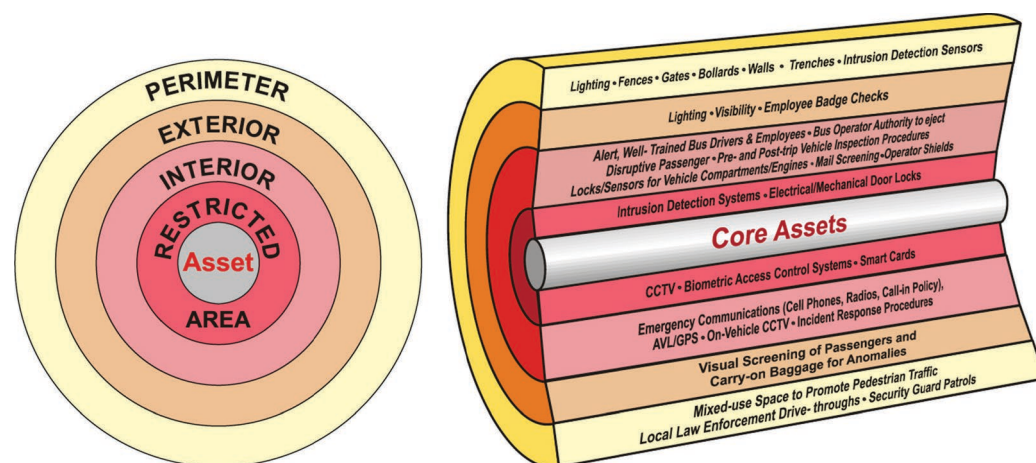
information about how to inspect vehicles for security breaches. The guide recommends that operators perform sweeps during “pre- and post-trip inspections, layovers or when your bus has been unattended.” (See Table 7.7.) Inspection points include:

Small- and medium-sized agencies should ensure at a minimum that trespassers cannot enter bus depots, garages, or other end-of-line bus storage facilities, maintenance and repair yards or other fleet layover locations. Chapter 2 of *NCHRP Report 525, Volume 14: Security 101: A Physical Security Primer for Transportation Agencies* (Frazier et al. 2009), provides in-depth discussion of perimeter security countermeasures that can be utilized to protect buses in storage. The key concept discussed in the text is one of “layers of security,” which consists of the combined usage of supportive security measures such as CCTV, lighting, fencing, and alarm systems to form a virtually impenetrable security zone. (See Figure 7.4.)

### Spotlight on Juvenile Vandalism

One of the difficulties associated with managing incidents of juvenile vandalism is the often random nature of the crime. To the transit agency, it may seem that the damage caused by vandals was the result of irrational unplanned acts committed without a motive. Known as “malicious mischief,” this characteristic of randomness makes defending against incidents much more difficult because the timing, targeting, and occurrence of the vandalism cannot be easily predicted. Under such circumstances protective plans to secure critical assets and properties is the only solution. Transit agencies must identify what assets need protection and then establish a minimum acceptable security posture to defend against vandalism related losses.

It is also worthwhile to note that sometimes although random in nature, juvenile vandalism can also be purposeful. For example, there have been occasions where juvenile offenders have entered school bus storage facilities and either deflated the tires on an entire fleet of school buses or slashed tires. The outcome of the vandalism was cancellation of school. Juvenile crime against property, in particular graffiti, can also be committed for the purpose of gaining notoriety. Graffiti vandals are known to display their “identification” or paint over or deface the signature mark of another rival. As discussed in *TCRP Research Results Digest 9* (TCRP 1996) the most successful method found to deter graffiti, etching, scribing and other “moniker” markings or paintings is through taking a “zero tolerance” approach. As it relates to rolling stock, zero tolerance means “no vehicle in service with graffiti.” By use of an integrated team of drivers, maintenance personnel, and security staff the agency combats the graffiti vandal’s desire for notoriety by immediately eradicating the graffiti. *TCRP Research Results Digest 9* recommends a structured proactive approach that includes “anti-graffiti education, immediate reporting of problems, immediate response to problems, routine and random uniformed and undercover patrols, video surveillance, rewards and



**Figure 7.4.** *Layers of security* (FTA Security Design Considerations, Rabkin et al. 2004).

bounties, truancy sweeps, documentation of incidents, interagency sharing of tag documentation and tagger files, prosecution of all vandals (treatment of vandalism as a crime), punishment, including arrest and detainment as well as vandal and parental monetary fines and responsibility for damages, and immediate cleanup/repair of vandalism/damage (within 24 hours or less)."

Of course not all vandalism is committed by juveniles. Infrequently, an angry or overzealous mob can band together at the same place and time to wreak destruction upon transit property. Similarly, there are incidents of targeted vandalism against fare boxes on board vehicles, disabling of fare collection machines, or damaging access control turnstiles so that they do not function. (In such cases, the likely motivation is either fare evasion or theft of revenues.)

## Other Transit Property

As shown in the survey results below small- and medium-sized transit agencies own or operate minimal real property. Generally, the physical infrastructure of such agencies includes (1) one administrative building owned or leased; (2) one maintenance facility, rail yard or bus garage; and (3) less than 2 passengers terminals, owned or leased. (See Figure 7.5.)

## Buildings and Other Facilities

As has been suggested throughout this text, small- and medium-sized transit agencies must specifically address the uniqueness in their operating environment when making security improvements. Buildings such as administrative offices, stations, warehouses, car shops, maintenance facilities, plants and industrial areas, dispatch centers, and fuel depots all have the potential to demand specialized individual security countermeasures or solution sets. This is even more true when environmental and operational factors such as location of the asset, area crime rates, and hours of operation are taken into account. Of course the major influence on how building security is handled is based on functional purpose. For example, there is a significant difference between how public and nonpublic building security should be managed.

Critical Assets: Key Infrastructures Please insert the number of each type of asset.						
Answer Options	1	2 - 6	7-12	Other	Rating Average	Response Count
Administrative Buildings/Facilities	141	17	0	9	1.26	167
Maintenance Facilities (Rail Yard and Bus Garage)	119	10	0	16	1.40	145
Passenger Terminals/Stations	57	17	5	24	1.96	103
Intermodal Centers	39	4	1	28	2.25	72
<i>answered question</i>						175
<i>skipped question</i>						5

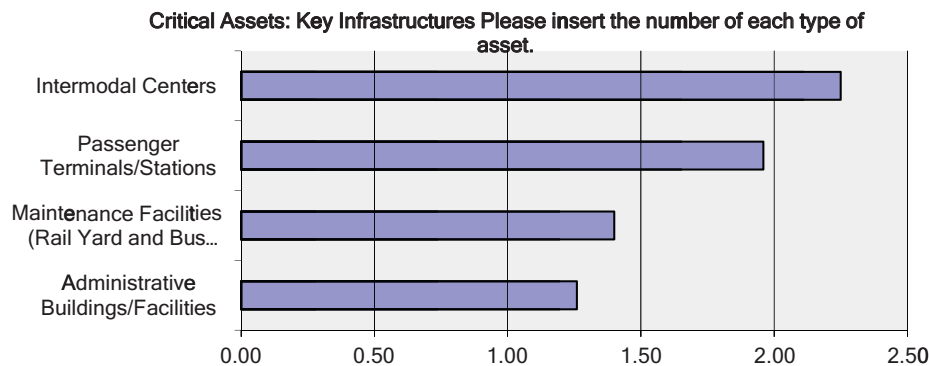


Figure 7.5. Critical assets: key infrastructures.

For nonpublic spaces, access control, perimeter security, intrusion detection systems, and other similar types of technology can be deployed to protect facilities from external losses. However, in transit buildings that are open to the public, during hours of operation, security personnel or possibly surveillance systems are the primary means of providing protection.

### Administrative Offices

The federal government has spent substantial time and money to establish comprehensive building security standardization requirements and criteria to protect federal office space. The work began in earnest on April 20, 1995, 1 day after the bombing of the Alfred P. Murrah Building in Oklahoma City, when the president directed the Department of Justice (DOJ) to assess the vulnerability of federal office buildings in the United States, particularly to acts of terrorism and other forms of violence. Within 2 months, DOJ completed the study and published its report, “*Vulnerability Assessment of Federal Facilities*,” (DOJ 1995) containing “minimum security standards” intended for use in all federally occupied facilities. The standards were based on DOJ security level criteria that basically considered occupancy, volume of public content, building size, and agency mission. See Table 7.8.

The standards addressed 4 general areas of security and supplied a total of 52 minimum compliance requirements for countermeasures in:

- Perimeter Security—Parking, Lighting, Physical Barriers.
- Entry Security—Receiving/Shipping, Access Control, Entrances/Exits.
- Interior Security—Employee/Visitor ID, Utilities, Occupant Emergency Plans.
- Security Planning—Intelligence Sharing, Training, Admin Procedures.

Summarizing the available standards and other building security guidelines suggests that the following potential areas of vulnerability should be reviewed for possible implementation of security countermeasures:

- |                              |                                  |
|------------------------------|----------------------------------|
| Pedestrian Entranceways      | Vehicular Access and Circulation |
| Parking Garages              | Public Toilets and Service Areas |
| Refuge Collection Sites      | Loading Docks                    |
| Shipping and Receiving Areas | Stairwells                       |

**Table 7.8. Security level and criteria** (adapted from U.S. Department of Justice 1995).

SECURITY LEVEL	CRITERIA
Level I	10 Federal employees 2,500 sq ft Low volume of public contact
Level II	11 to 150 Federal employees 2,500 sq ft – 80,000 sq ft Moderate volume of public contact Routine operations similar to private sector and/or facility shared with private sector
Level III	151-450 Federal employees 80,000 – 150,000 sq ft Moderate/high volume of public contact Contains agency mix such as: Law enforcement ops Court functions Government records
Level IV	More than 450 Federal employees Multi-story facility More than 150,000 sq ft High volume of public contact High-risk law enforcement intelligence agencies District courts
Level V	Level IV profile and agency/mission critical to national security

Source: Adapted from DOJ 1995.

Public Corridors	Equipment and Maintenance Spaces
Mailrooms	Lobbies and Waiting Areas
Roofs	Water Supply
Air Intakes	Fuel Storage Areas
Utility Feeds	Elevators
General Office Space	Dining Facilities
Retail Areas	Computer Rooms

In addition, the following systems or sub-systems should be considered for protective measures:

Mechanical	Engineering
Electrical	Ventilation
Fire Protection	Communications
Emergency Power	Structural
Lighting	Entry Control
Physical Security	Electronic Security
Information Technology	Command and Control

For most small- or medium-sized transit systems a “Level 1” (10 employees, 2,500 sq ft, and low volume of public contact) or infrequently “Level 2” (11 to 150 Federal employees, 2,500 sq ft–80,000 sq ft, moderate volume of public contact, routine operations similar to private sector and/or facility shared with private sector) security posture would be sufficient. Table 7.9 depicts the minimum and desirable standards for Level 1 and Level 2 security for federally occupied facilities.

However, note that there are often issues associated with ownership for security in leased spaces. If the transit agency is occupying leased space, security responsibility may lie with the

**Table 7.9. Standards for Level 1 and Level 2 security** (adapted from DOJ 1995).

<b>Perimeter Security</b>	<b>Level 1</b>	<b>Level 2</b>
<b>Parking</b>	○	○
Control of Facility Parking	○	○
Control of Adjacent Parking	○	○
Avoid Leases where Parking Cannot be Controlled	○	○
Leases Should Provide Security Control for Adjacent Parking	○	○
Post Signs and Arrange for Towing Unauthorized Vehicles	●	●
ID System and Procedures for Authorized Parking (If Applicable)	○	○
Adequate Lighting for Parking Areas	○	○
<b>Closed Circuit Television (CCTV) Monitoring</b>		
CCTV Surveillance Cameras with Time Lapse Video Recording	○	●
Post Signs Advising of 24 Hour Surveillance	○	●
<b>Lighting</b>		
Lighting with Emergency Power Backup	●	●
<b>Entry Security</b>	<b>Level 1</b>	<b>Level 2</b>
<b>Receiving and Shipping</b>		
Review Shipping and Receiving Procedures (Current)	●	●
Implement Shipping and Receiving Procedures (Modified)	○	○
<b>Access Control</b>		
Evaluate Facility for Security Guard Requirements	○	○
Security Guard Patrol	○	○
Intrusion Detection System with Central Monitoring Capability	○	○
Upgrade to Current Life Safety Standards (Fire Detection, Fire Suppression Systems, Etc.)	●	●
<b>Entrances/Exits</b>		
X-Ray & Magnetometer at Public Entrances	N/A	○
Require X-Ray Screening of All Mail/Packages	N/A	○
Peep Holes	○	○
Intercom	○	○
Entry Control w/CCTV and Door Strikes	○	○
High-Security Locks	●	●
<b>Interior Security</b>	<b>Level 1</b>	<b>Level 2</b>
<b>Employee/Visitor Identification</b>		
Agency Photo ID for All Personnel Displayed at All Times	N/A	○
Visitor Control/Screening System	○	●
Visitor ID Accountability System	N/A	○
Establish ID Issuing Authority	○	○
<b>Utilities</b>		
Prevent Unauthorized Access to Utility Areas	○	○
Provide Emergency Power to Critical Systems (Alarm Systems, Radio Communications, Computer Facilities, Etc.)	●	●
<b>Occupant Emergency Plans</b>		
Examine Occupant Emergency Plans (OEPs) and Contingency Procedures Based on Threats	●	●
OEPs in Place, Updated Annually, Periodic Testing Exercise	●	●
Assign & Train OEP Officials (Assignment Based on Largest Tenant in Facility)	●	●
Annual Tenant Training	●	●
<b>Daycare Centers</b>		
Evaluate Whether to Locate Daycare Facilities in Buildings with High-Threat Activities	N/A	●
Compare Feasibility of Locating Daycare in Facility's Outside Locations	N/A	●

Table 7.9. (Continued).

Security Planning	Level 1	Level 2
<b>Intelligence Sharing</b>		
Establish Law Enforcement Agency/Security Liaisons	●	●
Review/Establish Procedure for Intelligence Receipt/Dissemination	●	●
Establish Uniform Security/Threat Nomenclature	●	●
<b>Training</b>		
Conduct Annual Security Awareness Training	●	●
Establish Standardized Unarmed Guard Qualifications/Training Requirements	●	●
Establish Standardized Armed Guard Qualifications/Training Requirements	●	●
<b>Tenant Assignment</b>		
Co-Locate Agencies with Similar Security Needs	○	○
Do Not Co-Locate High-/Low-Risk Agencies	○	○
<b>Administrative Procedures</b>		
Establish Flexible Work Schedule in High-Threat/High-Risk Areas to Minimize Employee Vulnerability to Criminal Activity	○	○
Arrange for Employee Parking In/Near Building After Normal Work Hours	○	○
Conduct Background Security Checks and/or Establish Security Control Procedures for Service Contract Personnel	●	●
<b>Construction/Renovation</b>		
Install Mylar Film on All Exterior Windows (Shatter Protection)	○	○
Review Current Projects for Blast Standards	●	●
Review/Establish Uniform Standards for Construction	●	●
Review/Establish New Design Standard for Blast Resistance	○	○
Establish Street Set-Back for New Construction	○	○
<b>Key</b>		
● Minimum Standard ○ Desirable		

building's owner. In such circumstances, the transit agency should participate in decisions regarding the appropriate levels of security and also engage in contractual negotiations as needed to ensure that agency personnel and properties are adequately protected.

### Transit Stations

The text *Policing Transportation Facilities* (DeGeneste and Sullivan 1994), was one of the first transit crime-specific studies to chronicle the types of crime and order issues specifically related to transit. Chapter 1 of the text, "Moving the Masses," described transportation facilities as a vital link in the economic and social life of communities. Drug trafficking, terrorism, cargo theft, smuggling, organized crime, fear of crime, and the risk of hazardous cargo release were all identified as threats to public safety and order. Chapter 8 of the text, "Public Bus/Rail Terminal Crime," dealt directly with the security issues associated with operating a public surface transportation facility. Crimes identified include theft, pickpocketing, fraud, prostitution, drug use and sales, passenger assaults, and robberies. Although focused more so toward larger intermodal facilities, the text also included references to the types of quasi-criminal disorder issues that often plague terminals regardless of size. Problems such as loitering, panhandling, runaways, truants, and homeless populations were identified as exacerbating criminal activity occurring at terminals. These lesser offenses and conditions were also recognized as contributing to the public's perception of disorder or fear that is sometimes associated with a transit station.

The survey results shown below confirm that 20 years later these types of quasi-crime, offenses or disorder continue to have the highest and most adverse security impact on small- and medium-sized agencies (see Figure 7.6). While any occurrence of assault or robbery would instantly command the highest level of concern at such facilities, on a daily basis it is the disorder of a terminal that causes small- and medium-sized agencies the most problem in terms of operations and public perception. Similarly, homeland security concerns regarding bomb threats or explosions, chemical or biological agents, or the use of WMDs are not at the forefront of security issues confronting small- and medium-sized agencies. Although one occurrence of a homeland security event would immediately change both this condition and perspective, for purposes of deciding upon the appropriate security posture for a small- or medium-sized terminal or station, it is the prevention or deterrence of disorder and low-level crime that should be given the greatest consideration. Fortunately, as borne out by the survey, less than 2% (3 out of 164

<b>Criminal Incidents - Quality-of-Life—Location of Incidents—Station</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Disorderly Persons	36.2%	63
Homeless/Vagrancy	33.3%	58
Drunkness/Liquor Law Violations	30.5%	53
Smoking/Eating/Littering	27.6%	48
Loud Music	11.5%	20
Graffiti/Vandalism	31.6%	55
N/A	52.9%	92
<b><i>answered question</i></b>		<b>174</b>
<b><i>skipped question</i></b>		<b>6</b>

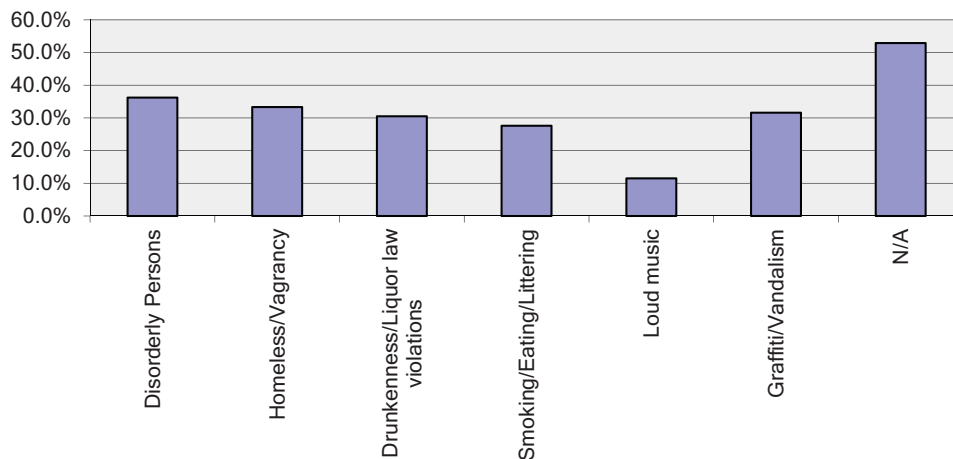


Figure 7.6. Criminal incidents—quality of life—location of incidents—station.

respondents), reported experiencing a bomb threat or other homeland security-related threat against transit properties in the previous year.

### Spotlight on Homeless Programs

Homelessness is not a crime, but with large numbers of the homeless population finding shelter and sleeping in transportation facilities across the country, it is a problem—a problem that’s been around for decades, analyzed, written about, and confronted in many ways, but with little success. Transit facilities are frequently used by those seeking shelter. Many of these individuals suffer from serious health concerns, such as alcoholism, drug addiction, or mental illness and their presence can compromise the transportation facilities’ ability to provide safe and efficient service to the public. The availability of social services offering shelter and food has not resolved the problem, as the homeless continue to resist using these services out of fear, shame, and as some think, pride, leaving the transportation facility to find a solution to dealing with this indigent population by working to bring them to the services they need or force them out into the street. To answer the problem, programs have been developed such as “Wheels to Work.” A Sacramento, CA-based program, “Wheels to Work” offers the homeless transportation, employment search services, health resources, and training about how to use public transit. Similarly, in their effort to move the population from their facilities into services that can provide the help they need, San Luis Obispo Transit partnered with other organizations to build a new homeless shelter, an effort that has taken years and encountered resistance in the community, but one that is nearing completion. Also in California, BART, the Bay Area Rapid Transit System, has put in place Crisis Intervention Training for police and community service people. BART created a new position to manage the homeless issue, not a police position but a “Crisis Intervention Training Coordinator and Community Outreach Liaison” position.

The core security issue that planners must decide upon in establishing a protective environment for the occupants, passengers, employees, retail, and premises of a transit station is whether an “enforcement-only” level of security is appropriate. If the occurrence of crime and/or disorder is rare or infrequent, the best approach may be to establish collaboration with local authorities and first responders who have enforcement responsibility for the facility. However, where incidents of either crime or disorder are prevalent, the transit agency should consider the deployment of proactive security forces or, as an alternative, real-time live-action CCTV surveillance systems. Answering this question will require significant interaction with local law enforcement authorities to establish the level of protection and response to security incidents that can be expected. Agencies should consider the following questions:

- Is there a need for a part-time or full-time security presence?
- Should the security force be proprietary or contracted?
- Should the security force be armed?
- Does the security force need arrest powers?

Because of the costs associated with personnel, where other types of countermeasures will suffice, such as training existing personnel to perform security functions, placement of alarm systems, using access controls, or deploying surveillance cameras, serious consideration should be



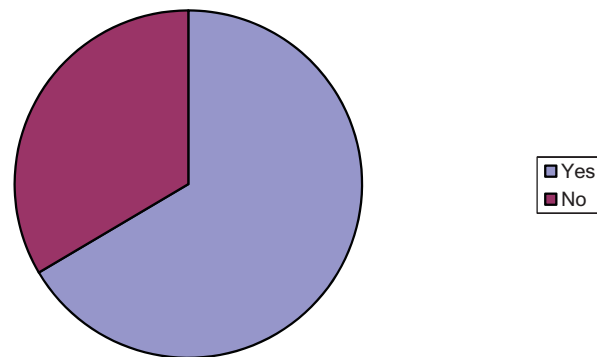
**Table 7.10. Security personnel.**

SECURITY PERSONNEL	SMALL	MEDIUM
Local Police Random Patrol	95%	77%
Contracted Security and Dedicated Local Police Patrol	1%	30%
Off-Duty Police Part-Time	>1%	9%

given for opting for one of these types of solutions. As mentioned in Chapter 6, typically small- and medium-sized agencies depend exclusively upon local law enforcement random patrol for security support. See Table 7.10.

Surveillance system deployments can also be somewhat costly, particularly those systems that have the capability of real-time live-action monitoring. However, there is a significant increase in the use of surveillance systems underway in transit, indeed in all transportation. From a transit standpoint, CCTV systems are currently being deployed in stations, on board conveyances—buses, light rail and commuter trains, on trolleys, ferries, and even on paratransit vehicles. The positive aspects of such systems extend beyond support of security efforts. (See Figure 7.7.)

APTA SS-SIS-RP-002-08, Final Version 8/26/08, *Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities* (APTA 2008) provides criteria for CCTV camera coverage and fields of view at transit passenger facilities. The RP states, “CCTV cameras are placed in such a manner as to observe and monitor certain locations to aid in



Security Countermeasures CCTV: Is Video Surveillance Used on Your Property?		
Answer Options	Response Percent	Response Count
Yes	66.5%	109
No	33.5%	55
<b>answered question</b>		<b>164</b>
<b>skipped question</b>		<b>16</b>

**Figure 7.7. Security countermeasures CCTV: Is video surveillance used on your property?**

**Table 7.11. Location monitoring.**

Entrances/exits	The CCTV cameras should be placed to view pedestrian and vehicular entrances and exits. There may be multiple entrances and exits that may require camera view at each location. Consideration should be given to bidirectional flow.
Ticket sales, ticket vending machines and turnstiles, gates, station-agent kiosks, booths	The cameras should provide a recognizable image of the person(s) involved in the transaction/interaction.
Elevator	Each elevator cab should have a camera mounted in the cab, with the intent to obtain full coverage and field of view of the cab interior and entrance to monitor passenger activity.
Platforms and platform edges	Cameras should provide coverage and field of view of the entire length and width of the platform and platform edge to monitor passenger activity.
Pedestrian passageways/concourses	Cameras should provide coverage and field of view of the entrances, exits, and the entire length of the passageway, including stairways, ramps, elevator lobbies, and escalators to monitor passenger activity.
Access locations to nonpublic areas (ancillary areas)	Cameras should provide coverage and field of view to monitor nonpublic entrances/exits, including temporary revenue vehicle storage areas.
Restricted area entrances	Cameras should provide coverage and field of view to monitor and identify entrances and access points to restricted rights-of-way (e.g., tunnel portals from station areas or elevated structures).
Concession areas	Cameras should provide coverage and field of view to monitor concession areas.
Other locations to be considered	Cameras should provide coverage of other locations identified as warranting security monitoring through the systemwide and asset-specific security risk assessments.
Other CCTV resources	Coverage and field of view from other existing and planned camera networks such as state (e.g., department of transportation), local (e.g., city or county transportation departments), joint-use facility security systems, local private businesses and media also should be considered.

maintaining safe and secure transit environments for people, operations and critical infrastructure.” Table 7.11 details the recommended monitoring locations.

A second RP from the recommended practice program, APTA IT-CCTV-RP-001-11 published June 2011, *Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems* (APTA 2011) provides definitive information about the types of cameras, recording systems, transmission systems and trainlines that are relevant to transit placement of surveillance systems. It is recommended that transit agency personnel who are considering the utilization of CCTV surveillance systems consult the APTA RP for additional guidance. There are essentially 2 types of surveillance systems available today, those that are basic in design and those that are supported by smart technology. The tradeoff between the 2 is that basic systems that are required to perform real-time monitoring specifications require multiple monitoring screens and stations and additional personnel, while smart systems can be designed and taught to detect events, isolate coverage, and notify personnel of security-related issues. Smart systems can also cause an increase in transmission costs.



## CHAPTER 8

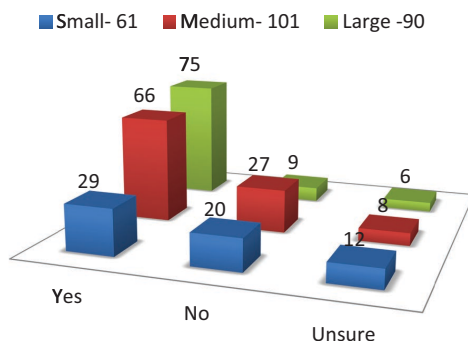
## Security Plan Implementation and Management

The design of a security protocol should occur only after the performance of a risk assessment and the development of a comprehensive security plan. Until these first steps are completed, insufficient data will be available to make good decisions about security strategies. In a perfect world, strategy is data driven. In business, it is a commonly accepted practice, e.g., “what cannot be measured cannot be managed.” However, the security industry has been slow to adopt the use of measurable factors in the reduction of risk. Fortunately, in the past decade or so, more and more transit systems have begun the process of managing security by formally adopting policies, processes, and procedures in which risk is evaluated. The survey of small- and medium-sized transit agencies confirmed that just under half of small and two-thirds of medium-sized agencies have previously conducted risk assessments and developed security plans. (See Figure 8.1.)

Although the benefits of security planning cannot be overstated, the method by which assessments and plans are drawn can range from being marginally documented and ineffective to being well thought out and conceived. Post 9-11 and the homeland defense, homeland security impetus, literally hundreds of risk assessment and security planning methodologies were developed by government, practitioners, researchers, and the security industry. Some of these methodologies, such as the *RAMCAP Framework: Risk Analysis and Management for Critical Asset Protection* (ASME 2005) were broad based in approach, suggesting that risk assessment and planning could be performed in accordance with some type of universally applicable standards. Others were highly specific and developed specifically for a particular industry, or operational or functional area.

On the government side, the surface transportation industry risk management methodologies and practices were created by the DOJ, Office of Domestic Preparedness, DHS, TSA, and the FTA. Typically, the methodologies were tied to the acquisition of grant funding by transportation agencies that were (and still are) required to perform assessments and conduct security planning in order to access federal funding. Practitioners and researchers including AASHTO, APTA, and the Transportation Research Board’s Transit and National Highway Cooperative Research Programs (TCRP and NCHRP) contributed additional methods and private security industry businesses such as Science Applications International Corporation, ICF International Corporation, and ALION Science and Technology Corporation still further augmented the field of transportation risk management (see Table 8.1).

In June of 2008, the General Accounting Office (GAO) released its report entitled *DHS Risk-Based Grant Methodology Is Reasonable, But Current Version’s Measure of Vulnerability is Limited* (GAO 2008). The report provided a graphic representation of a risk management framework divided into 5 phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks;



**Figure 8.1. Number of agencies with a security plan.**

**Table 8.1. Agencies, methodology, and citations.**

Agency	Methodology	Citation
DOJ, Office of Domestic Preparedness	Transportation Risk Assessment Methodology (TRAM)	Not Available
DHS	National Infrastructure Protection Plan, Transportation Sector Specific Plans, Mass Transit Modal Annex	<a href="http://www.dhs.gov/sites/default/files/publications/NIPP%202013">http://www.dhs.gov/sites/default/files/publications/NIPP%202013</a>
TSA	TSA/FTA Security and Emergency Management Action Items for Transit Agencies (2006)	<a href="http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf">www.tsa.gov/assets/pdf/mass_transit_action_items.pdf</a>
TSA	Baseline Assessment and Security Enhancement (BASE) Program	Security Sensitive Information Designation, contact TSA for assistance
FTA	The Public Transportation System Security and Emergency Preparedness Planning Guide (Balog et al. 2003)	<a href="http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=53">http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=53</a>
FTA	49 CFR Part 659 State Safety Oversight— System Safety and System Security Plans	<a href="http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=642">http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=642</a>

(continued on next page)

**Table 8.1. (Continued).**

Agency	Methodology	Citation
FTA	Transit Agency Security and Emergency Management Protective Measures	<a href="http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=439">http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=439</a>
TCRP	<i>TCRP Report 86/NCHRP Report 525: Surface Transportation Security Volume 8 – Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies</i> (Boyd et al. 2005)	<a href="http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v8.pdf">http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v8.pdf</a>
TCRP	<i>TCRP Report 86, Volume 10: Hazard and Security Plan Workshop: Instructor Guide</i> (AECOM Consult, Inc. et al. 2006)	<a href="http://www.tcrponline.org/PDFDocuments/TCRP_RPT_86v10.pdf">www.tcrponline.org/PDFDocuments/TCRP_RPT_86v10.pdf</a>
NCHRP	<i>NCHRP Report 525: Surface Transportation Security, Volume 15, Costing Asset Protection: An All Hazards Guide for Transportation Agencies (CAPTA)</i> (Science Applications International Corporation and PB Consult 2009)	<a href="http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v15.pdf">http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v15.pdf</a>
American Public Transportation Association	Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP), APTA SS-SRM-RP-001-09 RP: SEPP (2008)	<a href="http://www.aptastandards.com/LinkClick.aspx?link=http%3a%2f%2fwww.aptastandards.com%2fPortals%2f0%2fSecurity_pdfs%2fAPTA_SS_SRM_RP_001_09%2520SEPP.doc&amp;tabid=329&amp;mid=1683&amp;language=en-US">http://www.aptastandards.com/LinkClick.aspx?link=http%3a%2f%2fwww.aptastandards.com%2fPortals%2f0%2fSecurity_pdfs%2fAPTA_SS_SRM_RP_001_09%2520SEPP.doc&amp;tabid=329&amp;mid=1683&amp;language=en-US</a>



**Figure 8.2. Conceptual risk management framework (GAO 2008).**

(4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and the results achieved. Most above-listed methods follow this conceptual framework (see Figure 8.2.).

Of particular note, widespread use of the TSA's BASE assessment protocols is occurring in transit regardless of agency size. The BASE review was developed by the Surface Transportation Security Inspection Program (STSIP) and the Transportation Security Network Management (TSNM) office of the TSA in order to support the agency's strategic goals of increasing domain awareness, enhancing prevention and protection capabilities, and furthering response preparedness efforts of transit systems nationwide. It is designed to do the following:

- Baseline a transit agency's internal security processes, procedures, and policies against TSA and FTA developed security recommendations.
- Enhance a transit agency's overall security environment through development of corrective action recommendations to remediate any security program weaknesses identified during the review.
- Identify programs and protocols that might be "Smart Practice" models for other systems.
- Increase TSA's insight into universal security issues, concerns, and trends occurring nationally in order to inform future policy decisions and to target resources accordingly.

BASE reviews are supported directly by TSA through an inspection program that includes field collection of data by TSA (surface) Inspectors. The collected data is reviewed and evaluated against TSA/FTA Security and Emergency Management Action Items (SEMAI) (see Table 8.2).

BASE utilizes a checklist format that consists of approximately 200 line items. Each line item is assigned a score based on the evaluation. Once all scores are entered into the BASE checklist for each line item, a percentage is calculated for each of the sections. On completion of the field

**Table 8.2. TSA/FTA SEMAI for transit agencies.**

ITEM	ACTION
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 Security and Emergency Management Plan(s) with local and regional agencies.
5	Establish and maintain a Security and Emergency Training Program.
6	Establish plans and protocols to respond to the DHS National Terrorism Alert System (NTAS) threat levels.
7	Implement and reinforce a Public Security and Emergency Awareness program.
8	Conduct tabletop and functional drills.
9	Establish and use a risk management process to assess and manage threats, vulnerabilities, and consequences.
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).
12	Control access to security-critical facilities with ID badges for all visitors, employees, and contractors.
13	Conduct physical security inspections.
14	Conduct background investigations of employees and contractors.
15	Control access to documents of security-critical systems and facilities.
16	Develop a process for handling and access to sensitive security information (SSI).
17	Audit program.

review, a copy of the completed checklist is provided to and reviewed with the assessed transit agency. Additionally, a copy is also provided to TSA Headquarters for analysis.

In addition to high usage of BASE review methods, a very large number of transit agencies utilize and maintain security plans in accordance with FTA's *The Public Transportation System Security and Emergency Preparedness Planning Guide* (SSEPP) (Balog et al. 2003). The guide contains the statement of purpose (Figure 8.3):

**COMMIT** to a program that enables the public transportation system to:  
 ⇒ **PREVENT** incidents within its control and responsibility, effectively protect critical assets;  
 ⇒ **RESPOND** decisively to events that cannot be prevented, mitigate loss, and protect employees, passengers, and emergency responders;  
 ⇒ **SUPPORT** response to events that impact local communities, integrating equipment and capabilities seamlessly into the total effort; and  
 ⇒ **RECOVER** from major events, taking full advantage of available resources and programs.

**Figure 8.3. SSEPP statement of purpose.**

The SSEPP describes security planning as “more of a process than a product.” This approach coincides with a vision of a security plan being a dynamic living document that is continually under review and subject to change. The key aspect of importance that should be reinforced in developing the security plan is the need for flexibility. Alternatives and options should be incorporated into the plan to make it flexible and capable of responding to various situations or unexpected events.

APTA RP SS-SRM-RP-001-09, *Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)* (APTA 2008), provides further guidance to transit agencies that have never completed a plan or that seek to update an existing plan. The RP “describes the process by which a SEPP may be developed, implemented and evaluated.” A template for transit agencies to develop a customized SEPP is provided in Annex D.

### Spotlight on Document Security

*A note about Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit Agencies (49 CFR, Parts 15 and 1520).*

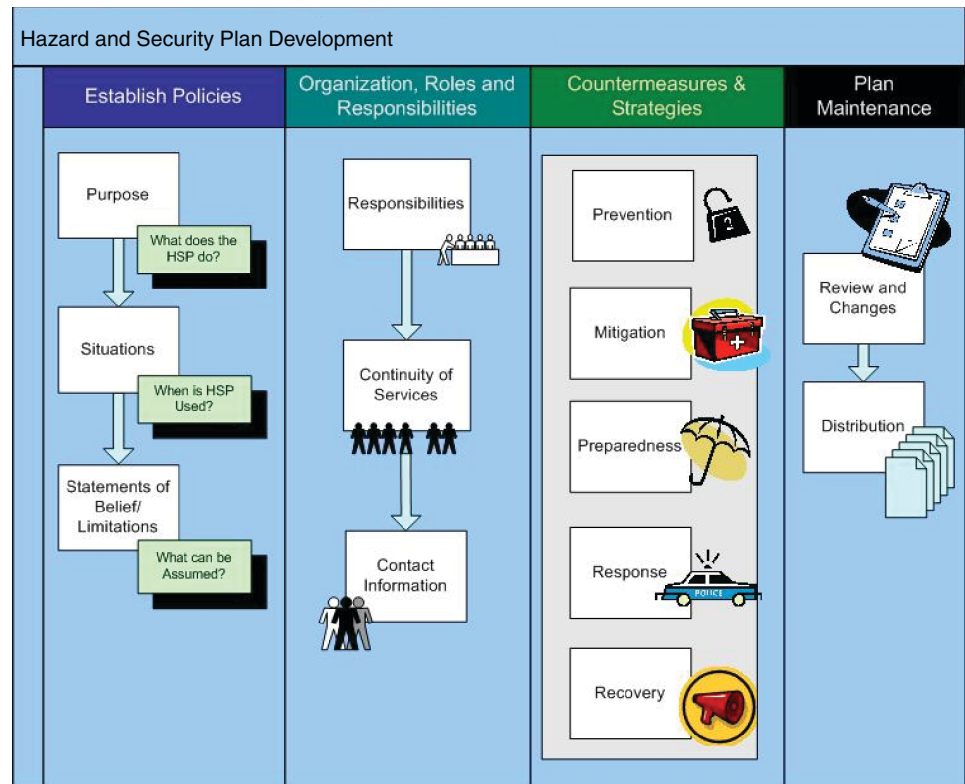
“Sensitive security information (SSI) is information about security, operations, facilities or other assets or capital projects whose disclosure would be detrimental to the security of transit employees or customers. Essential transit agency security program planning must include the designation, markings and control of SSI. By law, transit agencies are required to categorize and protect SSI. Protecting SSI means restricting its distribution and controlling access to it. By law, SSI is not subject to disclosure under the Freedom of Information Act (FOIA) or state “sunshine laws.” It is also not available under discovery in civil litigation, and it is not required to be part of the record in a federal rulemaking. Transit agencies should use this guidance as a resource in planning and developing policies and procedures for identifying, marking and handling SSI in order to control access to it. To the extent practical, agencies should integrate the designation, marking and handling of SSI into their existing security program procedures.” See APTA SS-SIS-RP-011-13, *Security Planning for Public Transit* (APTA 2013) for further information.

Irrespective of what risk assessment process and security planning framework is utilized, the major issue regarding effectiveness is how well the program is implemented. *TCRP Report 86: Volume 10, Hazard and Security Plan Workshop* (AECOM Consult, Inc. et al. 2006) provides an excellent overview of the transportation security planning and implementation process. The document also presents a template for Hazard and Security Plan (HSP) development. The template is designed to help transportation programs and transit agencies implement what it describes as the 4 core planning development functions: (1) establish priorities, (2) organization roles and responsibilities, (3) countermeasures and strategies, and (4) plan maintenance. (See Figure 8.4.)

### Establish Priorities

As indicated above, the starting point for plan development is to identify what the document is intended to do. Although the plan needs to be sufficiently flexible to cover a broad range of security incidents, the best way to ensure plan effectiveness is to use a prioritized scenario-based list of critical event types to drive plan activity. This list should consist of events considered routine





**Figure 8.4. HSP development (AECOM Consult, Inc. et al. 2006).**

and most likely to occur as well as those that may occur less frequently but with far reaching consequences. The HSP identifies the objectives of this phase of security planning as to:

- Create a written statement of purpose covering routine and emergency situations.
- Define the situations that the HSP will cover.
- Look at assumptions about the situations surrounding the use of the plan.
- Discuss how an organization plan fits into the overall community security and emergency plan.

### **Organization, Roles, and Responsibilities**

This phase of planning consists of determining key personnel and their security roles and responsibilities. Incident-based priority security tasks should be listed and assigned to a specific individual known as the primary or principal. Secondary responsibility should be placed in other individuals whose ability to perform will not be compromised by the loss of the primary. Interdependencies of functions should be delineated between departments and coordinating points established to facilitate liaison in areas of overlapping responsibility. Planners should ensure that this section of the plan provides clear and concise direction to assigned personnel regarding their primary and secondary duties. The goal is to achieve the stated objectives and security requirements of the plan under all potential operating conditions or scenarios. The HSP identifies the objectives of this phase of the security plan as to:

- Develop an organizational structure, with a clearly defined chain of command and designated roles and responsibilities, containing:
  - Responsibilities,
  - Continuity of services, including:
    - Designating lines of succession and delegating authority for the successors,

- Developing procedures for the relocation of essential departments,
  - Developing procedures to deploy essential personnel, equipment, and supplies, and
  - Establishing procedures for backup and recovery of computer and paper records, and
- Contact information.

## Countermeasures and Strategies

Consistent with emergency management principles, the risk and vulnerabilities reduction measures and strategies associated with transportation sector security planning should follow the 5 stages of protection activity: prevention, mitigation, preparedness, response, and recovery. Security planners should select countermeasures, keeping in mind the concepts of system security, layered or overlapping security, and system integration. The HSP identifies the objectives of this phase of the security plan as:

### Part A: Prevention

- Examine activities to reduce the likelihood that incidents will occur.
- Establish safe and secure procedures for passengers, vehicles, drivers and facilities.

### Part B: Mitigation

- Examine activities to reduce asset loss or human consequences (such as injuries or fatalities) of an incident.
- Establish safe and secure procedures for passengers, vehicles, drivers, and facilities.

### Part C: Preparedness

- Examine preparedness activities to anticipate and minimize the impacts of security-related incident and equip employees to better manage these incidents.
- Establish emergency policies and procedures for passengers, employees, and management to follow in case of emergencies.
- Keep training, drills, and contact lists up to date.
- Establish and maintain mutual aid agreement with fire departments, emergency medical services, and emergency management services.

### Part D: Response

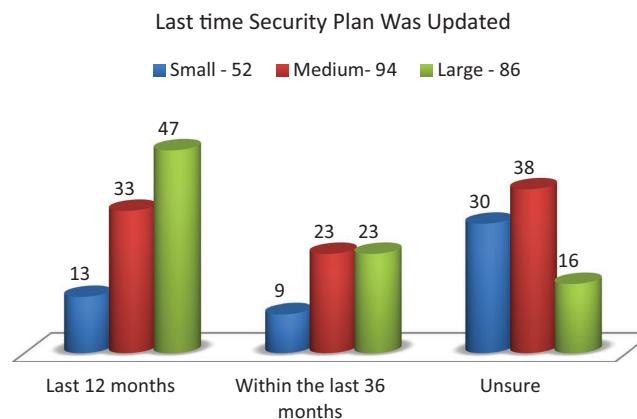
- Examine activities used to react to security-related incidents and hazards and help protect passengers, employees, the community, and property.
- Establish what information is to be collected by which employee.
- Ensure that policies and procedures established in the mitigation and preparedness portions of the HSP are followed.

### Part E: Recovery

- Examine policies to assist in recovering from incidents that have occurred so service can resume as quickly as possible.
- Establish a review of policies, documents, plans, and vehicles.
- Evaluate response and oversee recovery and restoration of personnel, service, vehicles, and facilities.

## Plan Maintenance

In this final phase of planning, substantial emphasis should be placed on assuring that security plans remain current and responsive to the dynamic changes that can occur in the transportation operating environment. Equal emphasis should be placed on the creation of a process that will support plan consistency with the future needs of the agency. Optimally plans will be scalable



**Figure 8.5. Security plan updating.**

and upgradable on a flexible timeline that has sufficient sensitivity to external security factors to allow for as-needed adjustments.

As stated above, a large percentage of small- and medium-sized agencies report having completed security plans. But, survey results disclosed that far fewer agencies were successfully updating and maintaining their plans and procedures (see Figure 8.5).

The HSP recommends programmatic scheduled plan review periodically—at least every 6 months to a year. The document also provides guidelines for how this review should be conducted:

- Identify areas to update.
- Determine completeness.
- Reassess roles and responsibilities.
- Review factual information (especially names and phone numbers included in the plan).
- Reevaluate employee knowledge and awareness (training assessments, for example).
- Revise programs and procedures included in the HSP.

The HSP also suggests that the occurrence of certain events may require planners to accelerate the scheduled conduct of a review. These include:

- The addition of new members inside the organization and outside the organization who have specific roles outlined in the HSP (e.g., a new general manager or a new local fire chief).
- New operations or processes that affect the HSP (e.g., a new bus line).
- New or renovated sites or changes in layout (e.g., a new bus garage or office building).
- Changes with outside agencies, new suppliers, vendors, etc. (e.g., a new memorandum of understanding, or MOU, signed with the local sheriff's department).

In some respects, the HSP Approach was well ahead of its time in 2006 when the planning process was presented. As opposed to a strict focus on security, which was notably the major focus of risk assessment and plan development at the time, *TCRP Report 86: Public Transportation Security, Volume 10, Hazard and Security Plan Workshop: Instructor Guide* (AECOM Consult., Inc. 2006) expanded its reach to address all manner of incidents, including natural catastrophes, earthquakes, floods, weather-related problems, and accidentally caused disasters, along with security concerns. Notwithstanding the purpose of this current research that is squarely focused upon security at small- and medium-sized agencies, there is a current evolution of thinking that a broader-based “All Hazards” and “Resilient” planning approach is preferable to processes based solely upon security risk.

# Conclusions

## Key Points Summary

### Risk Factors

1. In the public transit environment, the protection and security of people are the foremost concerns. This includes the passengers who use the system, the employees who deliver the transportation services, and a third set of indirect participants who interface with transit systems such as station vendors, other building tenants or occupants, delivery persons, or those with homes or businesses in proximity to transit facilities or infrastructure.
2. In addition to human assets, public transit agencies have an extensive range of property or infrastructure-related assets as well as intrinsic or intangible assets such as goodwill. Transit vehicles—buses, trolleys, trains—are the most recognizable of transit’s infrastructure; however, there are also stations owned or operated by transit agencies, and stops or shelters, office buildings, maintenance facilities, parking lots, information systems, communications huts, and other types of property used to support services.
3. Public transit agencies should be prepared to respond to the following 3 types of security risks.
  - a. Homeland Defense/Homeland Security—The Risk of Terrorist Attack
    - i. From a worldwide perspective, transportation assets moving by air, land, or sea have long been a primary target of focused attacks by hijackers, pirates, anarchists, or terrorists. Specific to public transit, terrorist attacks have been launched directly against intercity and over-the-road buses, subways, elevated trains, passenger trains, trolleys, ferries, and other types of conveyances.
  - b. Felony or Misdemeanor Crime—The Risk of Crime and Criminal Activity
    - i. The nation’s mass transit systems and the people who use these systems are susceptible to the occurrence of felony (major) and misdemeanor crime, including both crimes against persons and crimes against property.
  - c. Minor Offenses and Disorder
    - i. Quasi-crime, offenses, or disorder continue can have the highest and most adverse security impact on transit agencies. Problems include loitering, panhandling, runaways, truant, and homeless populations, which can exacerbate criminal activity.

### Small- and Medium-Sized Agencies Security Risk Profile

1. Research determined that there are significant differences between the security risks, needs, and issues facing smaller agencies when compared to those of large metropolitan transit systems. Fortunately the findings are that police and security problems at small- and medium-sized systems occur with much less frequency or magnitude of severity. A survey of

- large, medium, and small transit agencies disclosed that the smaller the system, the less probable it is for the agency to experience significant levels of crime or disorder.
2. Similarly, homeland security—or terrorism-related threats rarely occur on smaller systems. However, serious crime, including violent crime, does occur infrequently on smaller systems. And there is also a potential for major security events or crisis to occur.
  3. In contrast to the much more extensive and costly security-related requirements necessary to protect large-sized transit agencies, the scope and extent of countermeasures warranted for small- and medium-sized agencies is correspondingly smaller. Basically the difference lies in the reduced infrastructure and critical asset footprint and operating characteristics of small- and medium-sized agencies.
  4. With a few exceptions, the small- and medium-sized transit agencies profiled in this study operate over the road with buses, trolleys, vans, or cars that require a level of security commensurate with the protection of: (1) vehicles in transit on highways, rural and suburban city, borough, or township streets, or other roadways; (2) infrastructure such as unstaffed bus shelters or bus stops, vehicle storage depots, bus stations, and maintenance facilities necessary to support these conveyances; (3) employees who operate the conveyances; (4) minimal administrative and management staff; and (5) the passengers who use the agency's transportation services.
  5. Irrespective of the size of the agency, in general terms, transit security problems fall into a small group of categories: (1) passenger security, (2) employee security, (3) revenue security, (4) transit equipment and property protection, (5) fraud, and (6) homeland security security-related threats and vulnerabilities.
  6. The highest consequence security issue that small- and medium-sized transit agencies must confront on a daily basis is the potential for employees to be assaulted while performing their duties. Although lesser crimes or violations may occur more frequently, by and large the most significant criminal threat outside of homicide that the transit agency will face is as an aggravated assault committed against an employee.

### **Homeland Security**

1. Major homeland security/homeland defense threats include:
  - a. Arson
  - b. Explosives
  - c. WMDs or Mass Effect
  - d. Violent Confrontations/Hostage Situations
  - e. Malicious Tampering
  - f. Transit Vehicle as a Weapon
  - g. Network Failure/Cyber Attack

### **Crime and Disorder**

1. Transit systems must remain open and accessible to thousands of daily customers, sometimes 24 hours a day and 7 days a week, and comingled among these law-abiding fare-paying passengers is a criminal element whose goal is to commit crimes by taking advantage of targets of opportunity.
2. Crimes against person include homicide, aggravated and simple assault, robbery, rape, sex offenses, and harassment. Each transit system experiences its own unique blend of these types of crimes in terms of frequency and severity.
3. Both small- and medium-sized transit agencies should rarely see any form of homicide on their systems. However, even these systems may not be immune to isolated incidents where

murder is caused by conflict between primary or non-primary family, friends, or acquaintances. Similarly, strangers in pursuit of gain or some other rational or irrational motivation may commit murder either concurrent with the commission of a felony, or as a result of mental deficiency.

4. Assault crimes are charged based on “degrees” of consequence or through determination of weapon types whether used or possessed. Simple assault or harassment may occur based solely on a nonviolent offensive touching, for example, spitting on another individual, while aggravated assault would be charged in circumstances where a weapon is brandished in commission of a felony or an individual is severely beaten with lasting injuries. Along this violent or perceived violent continuum, victims who suffer injury are categorized and offenders are charged with either a felony or misdemeanor offense. Small- and medium-sized transit agencies can expect to have some form of assault on passengers occur periodically, but usually along the lesser side of the continuum.
5. Both small- and medium-sized transit agencies must be prepared to contend with the commission of robberies against their passengers, although incidents of violent attacks remain infrequent.
6. Rape and other felony-related sex offenses rarely occur on transit systems. Victimization occurs when passengers become targets of opportunity. For example, during late night hours at an unoccupied, sparsely attended or closed station, or in a transit-operated parking lot, a perpetrator may take advantage of the seclusion to prey upon an unescorted passenger.
7. Assuring that passengers pay their fare for riding on the bus, trolley, or train has been a chronic problem for transit agencies worldwide since the inception of pay-for-service ground transportation systems. Fare evasion and fare theft are reported as major security problems at many transit systems.
8. Protecting against losses associated with the property and infrastructure of transit systems is largely a matter of controlling theft and vandalism.
9. By far the most prolific and costly occurrence of larceny from bus and rail transit systems alike is the stealing of metals including copper, mercury, brass, or iron from vehicles, facilities, or rights-of-way. In particular, copper, once overlooked by thieves as having little value has skyrocketed as a preferred resale metal because of a surge in price on international markets. Transit agencies offering light rail or commuter rail services are more likely targets of copper thieves because of the large amount of unprotected or minimally protected infrastructure that contain the metal.
10. Headlines across the United States continue to confirm that the vandalism of transit vehicles, bus shelters, and bus depots is a perpetual problem that is extremely difficult to resolve or overcome. Even with recent advances in construction materials (graffiti resistant) (anti-etch materials) losses remain in the millions of dollars with multiple events of vandalism known to occur on systems.
11. Crime or violence at a bus stop is usually a matter for investigation and resolution by local authorities. Normally a small- or medium-sized agency would not be directly impacted by an event occurring at one of these locations. However, concern about the perception of passengers that an agency’s bus stops are unsafe could adversely impact ridership.

## Workplace Violence

1. Like transit passengers, transit employees, especially bus drivers, are potential victims of transit crime. When crimes against person involving employees occur during working hours, the events are properly categorized as workplace violence incidents.

2. The continuing major trend toward cashless fare collection systems and the placement of automated ticket dispensing machines in transportation is further removing the opportunity for criminals to obtain cash through dangerous confrontations like hold-ups or robberies.
3. Risk factors associated with operator assaults:
  - a. Interacting directly with the public
  - b. Working alone or in isolated areas
  - c. Having a mobile workplace
  - d. Working late night or early morning hours
  - e. Working in high-crime areas
  - f. Providing services to people who may be experiencing frustration (for example, with fare increases or service reductions)
  - g. Having a workplace where access is uncontrolled
  - h. Handling money or fares
    - i. Having enforcement responsibilities
    - j. Having inadequate escape routes

### Security Countermeasures

1. The design of a security protocol should occur only after the performance of a risk assessment and the development of a comprehensive security plan. Until these first steps are completed insufficient data will be available to make good decisions about security strategies.
2. Consistent with emergency management principles the risk and vulnerabilities reduction measures and strategies associated with transportation sector security planning should follow the 5 stages of protection activity; prevention, mitigation, preparedness, response and recovery. Security planners should select countermeasures keeping in mind the concepts of system security, layered or overlapping security and system integration.
3. Not surprisingly, relatively few small- or medium-sized transit agencies feel the need to maintain a dedicated agency police or security force. Less than 13% of small agencies and 17% of medium-sized agencies surveyed indicated that personnel assigned specifically to perform security work were included in the operating budget. This decision not to deploy dedicated security is consistent with the crime and disorder-related findings of this research project that disclose a minimal levels security-related risk for small- and medium-sized agencies.
4. Because of the costs associated with personnel, where other types of countermeasures will suffice—such as training existing personnel to perform security functions, placement of alarm systems, using access controls or deploying surveillance cameras—serious consideration should be given for opting for one of these types of solutions.
5. For those small- and medium-sized transit agencies whose security risks suggest that a dedicated force may be warranted the key question to be answered is whether a security presence, beyond what is available from the locale's public safety community, is necessary to protect the system and its users.
6. Unfortunately there are very few security measures available to *prevent* violence from occurring on board a transit vehicle. Buses are not reserved. They are public open access vehicles available for use by an unrestricted general population. Buses are populated by anonymous riders who present nothing more than a fare media or card to get on board. Typically individuals who represent security risks are not pre-identified or barred from riding because their propensity to violence is generally unknown.
7. There are numerous types of countermeasures that can support the maintenance of an effective *deterrence and response* program for on board incidents. Many of these measures are lost cost and/or low effort, consisting of policy responses, awareness and training, security planning, or coordination with local authorities.

8. Protecting vehicles consists of securing rolling stock while in transit and at rest. While there are infrequent occasions when larceny of a bus is reported, the main issue of security concern is vandalism.
9. From a security standpoint preventing, deterring, or reducing incidents of vandalism to rolling stock must take into account the nature of the criminal act including those with a proclivity to engage in the acts of window smashing or shattering, destruction of other vehicle surfaces, or graffiti. Unfortunately in many if not most instances these types of acts are committed by juvenile offenders.
10. Buildings such as administrative offices, stations, warehouses, car shops, maintenance facilities, plants and industrial areas, dispatch centers and fuel depots all have the potential to demand specialized individual security countermeasures or solution sets. This is even more true when environmental and operational factors such as location of the asset, area crime rates, and hours of operation are taken into account.
11. For nonpublic spaces access control, perimeter security, intrusion detection systems and other similar types of technology can be deployed to help protect facilities from external losses. However, in transit buildings that are open to the public, during hours of operation security personnel or possibly surveillance systems are the primary means of providing protection.
12. The core security issue that planners must decide upon in establishing a protective environment for the occupants, passengers, employees, retail and premises of a transit station is whether an “enforcement-only” level of security is appropriate. If the occurrence of crime and/or disorder is rare or infrequent the best approach may be to establish collaboration with local authorities and first responders who have enforcement responsibility for the facility.
13. Where incidents of either crime or disorder are prevalent the transit agency should consider the deployment of proactive security forces or as an alternative real-time live-action CCTV surveillance systems. From a transit standpoint CCTV systems are currently being deployed in stations, on-board conveyances—buses, light rail and commuter trains, on trolleys, ferries and even on paratransit vehicles. The positive aspects of such systems extend beyond support of security efforts.
14. There are essentially 2 types of surveillance systems available today, those that are basic in design and those that are supported by smart technology. The tradeoff between the 2 is that basic systems that are required to perform to real-time monitoring specifications require multiple monitoring screens and stations and additional personnel, while smart systems can be designed and taught to detect events, isolate coverage and notify personnel of security-related issues.



## References

- AECOM Consult, Inc., Maier Consulting, Inc., and Peter Schauer Associates. 2006. *TCRP Report 86, Public Transportation Security, Volume 10, Hazard and Security Plan Workshop, Instructor Guide*. Transportation Research Board of the National Academies. Washington, D.C. Accessed May 6, 2015 at <http://www.nap.edu/catalog/13695/tcrp-report-86-volume-10-hazard-and-security-plan-workshop>.
- Amalgamated Transit Union (ATU). 2012. Fact sheet: Preventing Violence against Bus Operators. Accessed May 6, 2015 at <http://www.atu.org/atu-pdfs/conventiondocs/convention-docs/ATU-Violence-Fact-Sheet.pdf>.
- American Public Transportation Association (APTA). 2008, revised 2012. *Recommended Practice RP APTA SS-SRM-RP-001-09, Rev. 1. Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)*. Accessed May 6, 2015 at <http://www.apta.com/resources/standards/Documents/APTA-SS-SRM-RP-001-09.pdf>.
- American Public Transportation Association (APTA). 2008. Recommended Practice APTA SS-SIS-RP-002-08. *Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities*. Accessed May 6, 2015 at [http://transit-safety.volpe.dot.gov/security/securityinitiatives/actionitems/Item2008/13/CCTV\\_Passenger\\_Final\\_8-13.pdf](http://transit-safety.volpe.dot.gov/security/securityinitiatives/actionitems/Item2008/13/CCTV_Passenger_Final_8-13.pdf).
- American Public Transportation Association (APTA). 2010. Recommended Practice SS-SIS-RP-008-10, Bus Stop Design and Placement, Security Considerations. Accessed May 6, 2015 at <http://www.apta.com/resources/standards/Documents/APTA-SS-SIS-RP-008-10.pdf>.
- American Public Transportation Association (APTA). 2011. Recommended Practice APTA IT-CCTV-RP-001-11. *Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems*. Accessed May 6, 2015 at <http://www.apta.com/resources/standards/Documents/APTA-IT-CCTV-RP-001-11.pdf>.
- American Public Transportation Association (APTA). 2013. *Recommended Practice APTA SS-SIS-RP-011-13. Security Planning for Public Transit*. Accessed May 6, 2015 at <http://www.apta.com/resources/standards/Documents/APTA-SS-SIS-RP-011-13.pdf>.
- ASME Innovative Technologies Institute. 2005. *RAMCAP Framework: Risk Analysis and Management for Critical Asset Protection*. Accessed May 6, 2015 at <http://files.asme.org/ASMEITI/RAMCAP/12604.pdf>.
- Balog, J. N., Boyd, A., and Caton, J. E. 2003. *The Public Transportation System Security and Emergency Preparedness Planning Guide*. Federal Transit Administration. Accessed May 6, 2015 at <http://www.fta.dot.gov/documents/PlanningGuide.pdf>.
- Black's Law Dictionary. Accessed May 6, 2015 at <http://thelawdictionary.org>.
- Blake, R., Uccardi, M. *Security Manpower Planning Model Instruction Manual*. 2008. Springfield, Virginia. National Technical Information Service/NTIS. Accessed May 6, 2015 at [http://www.fta.dot.gov/TSO/12527\\_13860.html](http://www.fta.dot.gov/TSO/12527_13860.html).
- Block, R. L., and C. R. Block. 1995. Space, Place, and Crime: Hot Spot Areas and Hot Places of Liquor-Related Crime, in J. Eck and D. Weisburd (eds.) *Crime and Place*, Monsey, NY: Willow Tree Press.
- Boyd A., Caton, J., Singleton, A., Bromley, P., and Yorks, C. 2005. *TCRP Report 86/NCHRP Report 525: Surface Transportation Security, Volume 8, Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies*. Transportation Research Board of the National Academies, Washington, D.C.
- Brantingham P. L., and P. J. Brantingham. 1993. Nodes, Paths, and Edges: Considerations on the Complexity of Crime and Physical Environment, *Journal of Environmental Psychology*, Vol. 13, pp. 3–28.
- Bureau of Labor Statistics Census of Fatal Occupational Injuries. 2012. TABLE A-1, Fatal Occupational Injuries by Industry and Event or Exposure, All United States. Accessed May 6, 2015 at <http://www.bls.gov/iif/oshwc/foi/cftb0268.pdf>.

- California Assembly Bill No. 1971—An Act to Amend Section 496a of, and to Add Section 594.05 to, the Penal Code, Relating to Theft (Filed July 10, 2012). Accessed May 6, 2015 at [http://www.leginfo.ca.gov/pub/11-12/bill/asm/ab\\_1951-2000/ab\\_1971\\_bill\\_20120710\\_chaptered.pdf](http://www.leginfo.ca.gov/pub/11-12/bill/asm/ab_1951-2000/ab_1971_bill_20120710_chaptered.pdf).
- Charlotte Area Transit System (CATS) Riders Code of Conduct (adapted from Charlotte Code Sec. 15-272 and 15-273). Accessed May 6, 2015 at <http://charmck.org/city/charlotte/cats/Bus/ridingcats/Pages/Code%20of%20Conduct.aspx>.
- Countermeasures Assessment & Security Experts, LLC. Forthcoming. TCRP Project F-21, “Tools and Strategies for Eliminating Assaults Against Transit Operators.” Transportation Research Board of the National Academies. Washington, D.C. Accessed May 6, 2015 at <http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=3544>.
- DeGeneste, H. I., and Sullivan, J. P. 1994. *Policing Transportation Facilities*. Accessed May 6, 2015 at <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=151198>.
- Department of Justice, Office of Domestic Preparedness. 2010. Transportation Risk Assessment Methodology (TRAM). Citation Not Available—see description of the Terrorism Risk Assessment and Management Toolkit on page 36 of Review of the Department of Homeland Security’s Approach to Risk Analysis (2010). Accessed May 6, 2015 at <http://www.nap.edu/catalog/12972/review-of-the-department-of-homeland-securitys-approach-to-risk-analysis>.
- DHS. 2008. *Risk Steering Committee: DHS Risk Lexicon, September 2008*. [dhs.gov/xlibrary/assets/dhs\\_risk\\_lexicon.pdf](http://dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf).
- DHS. 2013. *National Infrastructure Protection Plan*. U.S. Department of Homeland Security (DHS). Accessed May 6, 2015 at <http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf>.
- FBI. 2012. *Crime in the United States 2012*. USA. Accessed May 6, 2015 at <http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012>.
- FBI. 2012. *Hate Crime Statistics 2012*. Federal Bureau of Investigation. Accessed May 6, 2015 at <http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2012>.
- FBI. 2012. *Law Enforcement Officers Killed and Assaulted*. Federal Bureau of Investigation. Accessed May 6, 2015 at <http://www.fbi.gov/about-us/cjis/ucr/leoka/2012>.
- FBI. 2012. *National Incident-Based Reporting System 2012*. Federal Bureau of Investigation. Accessed May 6, 2015 at <http://www.fbi.gov/about-us/cjis/ucr/nibrs/2012>.
- FBI. Combined DNA Index System (CODIS). Accessed May 6, 2015 at <http://www.fbi.gov/about-us/lab/biometric-analysis/codis>.
- FBI. *Precious Metal: Copper Theft Threatens U.S. Infrastructure*. December 3, 2008. USA. Federal Bureau of Investigation. Accessed May 6, 2015 at [http://www.fbi.gov/news/stories/2008/december/copper\\_120308](http://www.fbi.gov/news/stories/2008/december/copper_120308).
- Frazier, E. R. Sr.; Nakanishi, Y. J.; Lorimer, M. A. 2009. *NCHRP Report 525, Volume 14: Security 101: A Physical Security Primer for Transportation Agencies*. Transportation Research Board of the National Academies, Washington, D.C. Accessed May 6, 2015 at <http://www.trb.org/Publications/Blurbs/162394.aspx>.
- FTA. 2006. *Transit Agency Security and Emergency Management Protective Measures*. Washington, D.C. <http://www.fta.dot.gov/TSO/EmergencyManagement.html>.
- GAO. 2008. *DHS Risk-Based Grant Methodology Is Reasonable, But Current Version’s Measure of Vulnerability is Limited*. U.S. Government Accountability Office (GAO). Accessed May 6, 2015 at <http://www.gao.gov/products/GAO-08-852>.
- Interactive Elements, Incorporated. 1997. *TCRP Web Document 15: Guidelines for the Effective Use of Uniformed Transit Police and Security Personnel*. TRB, National Research Council, Washington, D.C. Accessed May 6, 2015 at [http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp\\_webdoc\\_15-a.pdf](http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_webdoc_15-a.pdf).
- Lamm Weisel, D. 2002. *Problem-Oriented Guides for Police Series, Guide No. 9: Graffiti*. Community Oriented Policing Services, U.S. Department of Justice. [popcenter.org/problems/PDFs/Graffiti.pdf](http://popcenter.org/problems/PDFs/Graffiti.pdf).
- Loukaitou-Sideris A, Liggett R, Iseki H, Thurlow W. 2001, Measuring the effects of built environment on bus stop crime. *Environment and Planning B: Planning and Design* 28(2) 255–280. Accessed May 6, 2015 at <http://www.uctc.net/papers/419.pdf>.
- Mauri, R. A., Cooney, N. A., Prowe, G. J. 1984/Reprint 1997. *Transit Security: A Description of Problems and Countermeasures*. U.S. Department of Transportation. Accessed May 6, 2015 at [http://www.fta.dot.gov/documents/TS\\_Problem\\_Coutnermeasures.pdf](http://www.fta.dot.gov/documents/TS_Problem_Coutnermeasures.pdf).
- Nakanishi, Y. 2009. *TCRP Synthesis 80: Transit Security Update*. 2009. Transportation Research Board of the National Academies, Washington, D.C. Accessed May 6, 2015 at <http://www.trb.org/main/blurbs/160791.aspx>.
- Nakanishi, Y. J., Fleming, W. C., 2011. *TCRP Synthesis 93: Practices to Protect Bus Operators from Passenger Assault*. Transportation Research Board of the National Academies, Washington, D.C. Accessed May 6, 2015 at <http://www.nap.edu/catalog/14609/tcrp-synthesis-93-practices-to-protect-bus-operators-from-passenger>.

- National Council to Prevent Delinquency (NCPD) (now the Graffiti Resource Council (GRC). Accessed May 6, 2015 at <http://www.anti-graffiti.org>.
- National Crime Victimization Survey (NCVS). 2013. U.S. Department of Justice, Bureau of Justice Statistics. Accessed May 6, 2015 at <http://www.bjs.gov/index.cfm?ty=dcdetail&iid=245>.
- National Transit Database. Federal Transit Administration. Accessed May 6, 2015 at <http://www.ntdprogram.gov/ntdprogram/>.
- NTI. *Employee Guide to System Safety and Security*. National Transit Institute (NTI). Accessed May 6, 2015 at [http://www.ntionline.com/products/index.php?product\\_type=3](http://www.ntionline.com/products/index.php?product_type=3).
- Pearlstein, A.; Wachs, M. 1982. Crime in Public Transit Systems: An Environmental Design Perspective. *Transportation*. September 1982, Volume 11, Issue 3, pp. 277–297. Kluwer Academic Publishers. Accessed May 6, 2015 at <http://link.springer.com/article/10.1007%2FBF00172653#>.
- Perkins, D., J. Meeks, and R. Taylor (1992). The Physical Environment of Street Blocks and Resident Perceptions of Crime and Disorder: Implications for Theory and Measurement, *Journal of Environmental Criminology*, Vol. 12, pp. 21–34.
- Rabkin, M., Brodesky, R., Ford, F., Haines, M., Karp, J., Lovejoy, K., Regan, T., Sharpe, L., and Zirker, M. 2004. *Transit Security Design Considerations*. Federal Transit Administration. Accessed May 6, 2015 at <http://www.fta.dot.gov/documents/ftasesc.pdf>.
- Rugala, E. A., Isaacs, A. R., editors. *Workplace Violence: Issues in Response*. 2002. Federal Bureau of Investigation. National Center for the Analysis of Violent Crime. Accessed May 6, 2015 at <http://www.fbi.gov/stats-services/publications/workplace-violence>.
- Science Applications International Corporation, and PB Consult. 2009. *NCHRP Report 525, Surface Transportation Security, Volume 15, Costing Asset Protection: An All Hazards Guide for Transportation Agencies (CAPTA)*. Transportation Research Board of the National Academies, Washington, D.C.
- Shaner, Z. May 11, 2012. BREAKING: 4.2 Miles of Copper Wire Stolen from LINK. Seattle Transit Blog. Accessed May 6, 2015 at <http://seattletransitblog.com/2012/05/11/breaking-4-2-miles-of-copper-wire-stolen-from-link/>.
- Skogan, W. G. (1990). *Disorder and Decline: Crime and the Spiral of Decay in American Neighborhoods*, New York: MacMillan.
- TCRP. 1996. *Transit Cooperative Research Program Research Results Digest 9: Responding to Vandalism of Transit Bus and Rail Vehicle Passenger Windows*. 1996. Washington, D.C. Transportation Research Board, National Research Council. Accessed May 6, 2015 at <http://www.trb.org/Publications/Blurbs/153749.aspx>.
- TRB Public Transportation Marketing and Fare Policy Research Needs Statements. 2013. Transit Fare Evasion: Measurement, Prevention, Economics, and Societal Factors. Transportation Research Board of the National Academies. Washington, D.C. Accessed May 6, 2015 at <http://rns.trb.org/dproject.asp?n=33883>.
- TSA/FTA. Security and Emergency Management Action Items for Transit Agencies. Federal Transit Administration. Accessed May 6, 2015 at <http://transit-safety.volpe.dot.gov/security/securityinitiatives/ActionItems/default.asp>.
- U.S. Department of Justice. *Vulnerability Assessment of Federal Facilities*. 1995. Accessed May 6, 2015 at <https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf>.
- Wilson, J. Q., and Kelling, G. L. 1982. “Broken Windows: The Police and Neighborhood Safety,” *Atlantic Monthly*, 249(3), 29–38.



## APPENDIX A

# Agencies Participating in the F-18 Study of Agency Size— Large, Medium, Small

## **Large-Sized Transit Agencies (serving a population over 200,000)**

Access Services  
 Antelope Valley Transit Authority  
 Area Transportation Authority of North Central Pennsylvania  
 Arlington Transit  
 Ben Franklin Transit  
 Brockton Area Transit Authority  
 Cape Fear Public Transportation Authority  
 Capital Area Transportation Authority  
 Capital Metro  
 Capital Area Transit System  
 Central Contra Costa Transit Authority  
 Charleston Area Regional Transportation Authority  
 Charlotte Area Transit  
 City & County of Honolulu Department of Transportation Services  
 City of Modesto  
 City of Redondo Beach—Beach Cities Transit  
 City of Riverside, Special Transit  
 City of Santa Clarita Transit  
 City of Scottsdale  
 City of Visalia—Visalia Transit  
 Concord Kannapolis Area Transit  
 CTTransit  
 CTUIR Public Transit  
 Des Moines Area Regional Transit Authority  
 Eastern Contra Costa Transit Authority  
 Foothill Transit  
 Fort Wayne Citilink  
 Fresno Area Express  
 Gaston County Access  
 Georgia Regional Transportation Authority  
 Golden Empire Transit District  
 Golden Gate Bridge Highway & Transportation District  
 Greater Attleboro Taunton Regional Transit Authority  
 Greater Cleveland Regional Transit Authority  
 Greater Dayton RTA

## 92 Policing and Security Practices for Small- and Medium-Sized Public Transit Systems

Greater New Haven Transit District  
Guilford County Transportation and Mobility Services  
Gwinnett County Transit  
Hillsborough Area Regional Transit  
Indianapolis Public Transportation Corporation (INDYGO)  
Interurban Transit Partnership  
Knox County CAC Transit  
Knoxville Area Transit  
Lane Transit District  
Lawrence County Port Authority  
Lee County Transit  
Luzerne County Transportation Authority  
Madison County Transit  
Marin Transit  
Metro Transit Oklahoma City  
Metro Transit  
Metropolitan Transit (MN)  
Metropolitan Tulsa Transit Authority  
Milwaukee County Transit System  
Mountain Metropolitan Transit  
Municipality of Anchorage  
Nashville Metropolitan Transit Authority  
NCSU Wolfline  
Niagara Frontier Transportation Authority  
North County Transit District  
Norwalk Transit System  
Omaha Metro Transit  
Omnitrans  
Pace Suburban Bus  
Palm Tran  
Phoenix Public Transit Department  
Pinellas Suncoast Transit Authority  
Potomac & Rappahannock Transportation Commission  
Rhode Island Public Transit Authority  
Ride Connection  
Rock Island County Metropolitan Mass Transit District  
S.F. Bay Area Rapid Transit  
San Diego Metropolitan Transit System  
San Joaquin Regional Rail Commission  
San Joaquin RTD  
San Juan  
Santa Clara Valley Transportation Authority  
Santa Rosa Citybus  
Seattle Center Monorail  
SMART  
SORTA  
South Florida Regional Transportation Authority  
Space Coast Area Transit  
Spokane Transit  
StarTran  
Suffolk Transit

Sun Metro  
 Taps Public Transit  
 Transit Authority of Lexington, KY (LEXTRAN)  
 Transit Authority of Northern Kentucky  
 Transit Authority of River City  
 Triangle Transit  
 TriMet  
 Utah Transit Authority  
 Valley Metro  
 Valley Regional Transit  
 Valley Transit  
 Via Mobility Services  
 Victor Valley Transit Authority  
 Vista  
 Westmoreland County Transit Authority  
 Winston-Salem Transit Authority

### **Medium-Sized Transit Agencies (serving a population between 50,000 and 200,000)**

Albany Transit System  
 Athens Transit  
 Arrowhead Transit  
 Bay Metro Transit  
 Belle Urban—Racine, WI  
 Birmingham-Jefferson County Transit Authority  
 Broome County Transit  
 C-TRAN  
 Cache Valley Transit District  
 Casper Area Transportation Coalition  
 CCTA  
 Charles County Maryland  
 Charlotte County Transit  
 Cities Area Transit  
 City of Anderson Transit System  
 City of Asheville's—Asheville Redefines Transit Art  
 City of Corona Transit Service  
 City of Harrisonburg Dept of Public Transportation  
 City of Lompoc  
 City of Loveland Transit  
 City of Mesquite  
 City of Tempe (AZ)  
 City of Washington, PA  
 City/County Transportation  
 Citylink  
 Cleveland Area Rapid Transit/University of Oklahoma  
 Clinton Area Transit System  
 Coast Transit Authority  
 Collin County Area Regional Transit (CCART)  
 Columbia Transit  
 Community Action of Southern Kentucky

Cooperative Alliance for Seacoast Transportation  
Davenport Citibus  
Decatur Public Transit System  
Duluth Transit Authority  
East Alabama Regional Planning and Development Commission  
EAU Claire Transit  
Everett Transit  
Fayetteville Area System of Transit  
Fond Du Lac Area Transit  
Go BG Transit  
Great Glens Falls Transit  
Greeley Evans Transit  
Jackson Area Transportation Authority  
Jacksonville Transit  
Jacksonville Transit, Jacksonville North Carolina  
Johnson County Seats  
Jonesboro Economical Transportation System (JETS)  
Jump Around Carson  
Kitsap Transit  
La Crosse Municipal Transit Utility  
Lake County BCC  
Lake Transit Authority  
Lawrence Transit  
Lebanon Transit  
Lee-Russell  
Link Transit  
Livermore Amador Valley Transit Authority  
Livingston Essential Transportation Service (LETS)  
Long Beach Public Transit  
Macatawa Area Express  
Manchester Transit Authority  
Mason City Public Transit  
Mecosta Osceola Transit Authority  
Metro Ride  
Metropolitan Transit Authority of Black Hawk County  
Milford Transit District  
Murfreesboro Public Transit  
Muskegon Area Transit  
Okaloosa County Transit  
Oshkosh Transit System  
Petaluma Transit  
Pierce Transit  
Porter County Aging and Community Services  
Porterville Transit  
Richland County Transit Board  
Rio Metro Regional Transit District  
Salem-Keizer Transit  
San Luis Obispo Regional Transit Authority  
San Luis Obispo Transit  
Sandoval County  
SCUSA Transportation

Sioux Area Metro  
 St. Johns County COA  
 St. Joseph Transit  
 St. Johns County Council on Aging  
 Star Transit  
 Straits Regional Ride  
 The Jule  
 Topeka Metropolitan Transit Authority  
 Town of Cary, NC, Cary Transit (C-TRAN)  
 Transportation Lincoln County (TLC)  
 Tri-County Council for The Lower Eastern Shore of Maryland  
 Union City Transit  
 Unitrans  
 University of Georgia Transit  
 Valley Transit District  
 Voluntary Action Center  
 Washington County  
 Waukesha Metro Transit  
 Wausau Area Transit System  
 Western Contra Costa Transit Authority  
 WHATCOM Transportation Authority  
 Wichita Falls Transit  
 Wildcat Transportation  
 Wiregrass Transit Authority  
 Yuba-Sutter Transit Authority  
 Yuma County Intergovernmental Public Transportation Authority

### **Small-Sized Transit Agencies (serving a population less than 50,000)**

Access Johnson County Public Transit  
 Access Scioto County Public Transit  
 Anson County Transportation System  
 Area IV Agency on Aging & Cap  
 Benzie Transportation Authority  
 Bethel Transit System  
 Butler Transit Authority  
 Caldwell Parish Public Transit  
 Capital Transit  
 Carbon County Senior Services  
 City of Las Cruces—Roadrunner Transit  
 City of Lompoc  
 City of Neligh Dial-A-Ride  
 City of Niles Dial-a-Ride  
 City of Paso Robles  
 Clare County Transit  
 Clare County Transit Corporation  
 Clovis Area Transit System  
 Columbia County Rider Transportation  
 Community Action Committee of Pike County  
 Community Connection of Baker County



Community Connector  
County of Kauai Transportation Agency  
Culver Citybus  
Delmarva Community Services, Inc.  
Downeast Transportation, Inc.  
Dunklin County Transit Service, Inc.  
Galveston Island Transit  
Hancock Co. Transportation  
Hobbs Express—City of Hobbs  
Hub City Transit/City of Hattiesburg  
Huntington Area Transportation  
Jefftran  
Kaser Bus Service  
Klickitat County Senior Services  
Laguna Beach Transit  
Lewiston-Auburn Transit Committee  
Lincoln County Transportation  
Lorain County Transit  
Lyon County Area Transit  
Marshalltown Municipal Transit  
Monroe Bus Corp.  
Municipality of Hatillo  
NEICAC Transit  
Ogallala Public Transit  
Ozaukee County Transit Services  
Pine Bluff Transit  
Pueblo of Laguna Shaa'srk'a Transit  
R.E.A.L., Inc.  
Sanilac Transportation Corporation  
Senior Center Resources and Public Transit, Inc.  
Senior Friendship Center  
Shiawassee Area Transportation Agency  
Spartanburg Area Regional Transit Agency  
Spring Valley Jitney  
Standing Rock Public Transit  
Swain Public Transit  
Talbot County Transit  
Ten Sleep Senior Center  
Town of Oro Valley  
Twin Cities Area Transportation Authority  
Twin Cities Area Transportation Authority Pratt County Council on Aging  
Valparaiso  
Virginia Regional Transit  
Washington County  
Watsonwan County DBA TMT (Take Me There)  
Wilson Transit System

*Abbreviations and acronyms used without definitions in TRB publications:*

A4A	Airlines for America
AAAAE	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	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
HMCRRP	Hazardous Materials Cooperative Research Program
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
MAP-21	Moving Ahead for Progress in the 21st Century Act (2012)
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
PHMSA	Pipeline and Hazardous Materials Safety Administration
RITA	Research and Innovative Technology Administration
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

**TRANSPORTATION RESEARCH BOARD**  
500 Fifth Street, NW  
Washington, DC 20001

**ADDRESS SERVICE REQUESTED**

## THE NATIONAL ACADEMIES™

*Advisers to the Nation on Science, Engineering, and Medicine*

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.

[www.national-academies.org](http://www.national-academies.org)

ISBN 978-0-309-30881-6



9 780309 308816