

## Security 101: A Physical Security Primer for Transportation Agencies

### DETAILS

---

212 pages | | PAPERBACK

ISBN 978-0-309-43561-1 | DOI 10.17226/22998

### AUTHORS

---

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.

**NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM**

---

---

**NCHRP REPORT 525**

---

---

***Surface Transportation Security***  
***Volume 14***  
**Security 101: A Physical Security Primer**  
**for Transportation Agencies**

**Ernest R. Frazier, Sr.**

**Yuko J. Nakanishi**

**Mary Ann Lorimer**

COUNTERMEASURES ASSESSMENT AND SECURITY EXPERTS, LLC  
Camden, NJ

*Subject Areas*

Planning and Administration • Operations and Safety • Aviation • Public Transit  
Rail • Freight Transportation • Marine Transportation • Security

---

Research sponsored by the American Association of State Highway and Transportation Officials  
in cooperation with the Federal Highway Administration

---

**TRANSPORTATION RESEARCH BOARD**

WASHINGTON, D.C.

2009

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

## **NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM**

Systematic, well-designed research provides the most effective approach to the solution of many problems facing highway administrators and engineers. Often, highway problems are of local interest and can best be studied by highway departments individually or in cooperation with their state universities and others. However, the accelerating growth of highway transportation develops increasingly complex problems of wide interest to highway authorities. These problems are best studied through a coordinated program of cooperative research.

In recognition of these needs, the highway administrators of the American Association of State Highway and Transportation Officials initiated in 1962 an objective national highway research program employing modern scientific techniques. This program is supported on a continuing basis by funds from participating member states of the Association and it receives the full cooperation and support of the Federal Highway Administration, United States Department of Transportation.

The Transportation Research Board of the National Academies was requested by the Association to administer the research program because of the Board's recognized objectivity and understanding of modern research practices. The Board is uniquely suited for this purpose as it maintains an extensive committee structure from which authorities on any highway transportation subject may be drawn; it possesses avenues of communications and cooperation with federal, state and local governmental agencies, universities, and industry; its relationship to the National Research Council is an insurance of objectivity; it maintains a full-time research correlation staff of specialists in highway transportation matters to bring the findings of research directly to those who are in a position to use them.

The program is developed on the basis of research needs identified by chief administrators of the highway and transportation departments and by committees of AASHTO. Each year, specific areas of research needs to be included in the program are proposed to the National Research Council and the Board by the American Association of State Highway and Transportation Officials. Research projects to fulfill these needs are defined by the Board, and qualified research agencies are selected from those that have submitted proposals. Administration and surveillance of research contracts are the responsibilities of the National Research Council and the Transportation Research Board.

The needs for highway research are many, and the National Cooperative Highway Research Program can make significant contributions to the solution of highway transportation problems of mutual concern to many responsible groups. The program, however, is intended to complement rather than to substitute for or duplicate other highway research programs.

## **NCHRP REPORT 525: VOLUME 14**

Project 20-59 (28)  
ISSN 0077-5614  
ISBN: 978-0-309-11793-7  
Library of Congress Control Number 2006902911

© 2009 Transportation Research Board

### **COPYRIGHT PERMISSION**

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

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

### **NOTICE**

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

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

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

The Transportation Research Board of the National Academies, the National Research Council, the Federal Highway Administration, the American Association of State Highway and Transportation Officials, and the individual states participating in the National Cooperative Highway Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

*Published reports of the*

### **NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM**

*are available from:*

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

*and can be ordered through the Internet at:*

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

Printed in the United States of America

# THE NATIONAL ACADEMIES

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

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

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

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

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

The **Transportation Research Board** is one of six major divisions of the National Research Council. 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 NCHRP REPORT 525, VOLUME 14**

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

## **NCHRP PROJECT 20-59 PANEL** **Field of Special Projects—Area of Security**

**David S. Ekern**, *Virginia DOT, Richmond, VA (Chair)*  
**Dave Cardenas**, *Los Angeles World Airports, Los Angeles, CA*  
**John M. Contestabile**, *Johns Hopkins Univ./Applied Physics Lab, Laurel, MD*  
**Ernest R. “Ron” Frazier**, *Countermeasures Assessment and Security Experts, LLC, Camden, NJ*  
**Vicki Glenn**, *VHB, Inc., Vienna, VA*  
**Barbara Ivanov**, *Washington State DOT, Olympia, WA*  
**Michael Miles**, *California DOT, Sacramento, CA*  
**Sonia Pitt**, *Excalibur Associates, Inc., Alexandria, VA*  
**Mary Lou Ralls**, *Ralls Newman, LLC, Austin, TX*  
**Gina C. Wesley**, *University of Louisville, Louisville, KY*  
**Jeffrey L. Western**, *Western Management and Consulting, LLC, Madison, WI*  
**Richard Winston**, *Evanston, IL*  
**Ernesto L. Acosta**, *TSA Liaison*  
**Steven L. Ernst**, *FHWA Liaison*  
**Richard Gerhart**, *FTA Liaison*  
**Anthony B. Tisdale**, *FTA Liaison*  
**Rick Barnaby**, *FHWA Liaison*  
**William Brownlow**, *AASHTO Liaison*  
**Mark S. Bush**, *AASHTO Liaison*  
**Philip J. Caruso**, *Institute of Transportation Engineers Liaison*  
**Xavier Delache**, *Ministere des Transports de l'Equipment du Tourisme et de la Mer Liaison*  
**Nicholas Farber**, *National Conference of State Legislatures Liaison*  
**Marvin Fell**, *US Department of Homeland Security Liaison*  
**David Hahn**, *APTA Liaison*  
**Greg Hull**, *APTA Liaison*  
**Robert D. Jaffin**, *American Public University Liaison*  
**Anthony R. Kane**, *AASHTO Liaison*  
**Peter LaPorte**, *District of Columbia Emergency Management Agency Liaison*  
**Erhart M. “Mark” Olson**, *Washington Metropolitan Area Transit Authority Liaison*  
**Vincent P. Pearce**, *US DOT Liaison*



# FOREWORD

By **S. A. Parker**

Staff Officer

Transportation Research Board

*Security 101: A Physical Security Primer for Transportation Agencies* provides transportation managers and employees with an introductory-level reference document to enhance their working knowledge of security concepts, guidelines, definitions, and standards. This is a document for use primarily by those who are neither security professionals nor well versed in security language. There are many types of security: personal, cyber, document, information, operations, personnel, infrastructure, etc. This document focuses on physical security, the part of security concerned with measures and concepts designed to (1) safeguard personnel; (2) prevent unauthorized access to equipment, installations, materiel, and documents; and (3) safeguard equipment, installations, materiel, and documents against espionage, sabotage, damage, and theft.

Physical security is integral to an all-hazards approach to preparedness. As such, this report covers the major components of an effective security program at the conceptual level, including risk management and risk assessment, plans and strategies, physical security countermeasures, security personnel and other personnel, infrastructure protection, and homeland security. This primer can be used as an introduction to the extensive literature and additional sources of information identified in the appendixes; however, readers are reminded that plans need to be tested through exercises to ensure adequacy and to reinforce roles and responsibilities.

This volume of *NCHRP Report 525* was prepared under NCHRP Project 20-59(28) by Countermeasures Assessment and Security Experts, LLC, of Camden, New Jersey.

---

Surface transportation agencies are recognizing that because of their broad policy responsibility, public accountability, large and distributed workforces, heavy equipment, and robust communications infrastructure, they are uniquely positioned among civilian government agencies to swiftly take direct action to protect lives and property. The institutional heft of such agencies also provides a stable base for campaigns to mitigate or systematically reduce risk exposure over time through all-hazards capital investments.

This is the fourteenth volume of *NCHRP Report 525: Surface Transportation Security*, a series in which relevant information is assembled into single, concise volumes—each pertaining to a specific hazard or security problem and closely related issues. These volumes focus on the concerns that transportation agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the reports will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including state departments of transportation. A topic panel of experts in the subject area was estab-

lished to guide the researchers in organizing and evaluating the collected data and to review the final document.

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

Volumes issued under *NCHRP Report 525: Surface Transportation Security* may be found on the TRB website at <http://www.TRB.org/SecurityPubs>.



# CONTENTS

1	<b>Summary</b>
3	<b>Chapter 1 Risk Management and Risk Assessment</b>
6	Threat Assessment
6	Threat Types
7	Explosives
8	Weapons of Mass Destruction
13	Armed Assault
13	Adversary Types and Motivations
15	Vulnerability Assessment
16	Security Surveys
16	Performing the Security Survey
18	<b>Chapter 2 Plans and Strategies</b>
18	Objectives of a Security Plan
19	Benefits of a Security Plan
19	Elements of a Security Plan
20	Establishing Priorities
21	Organizing Roles and Responsibilities
21	Selecting Countermeasures and Strategies
22	Maintaining the Plan
22	Security Design Processes
25	Security Funding
27	<b>Chapter 3 Physical Security Countermeasures</b>
27	Signs
30	Emergency Telephones, Duress Alarms, and Assistance Stations
31	Key Control and Locks
32	Protective Barriers
32	Fencing
34	Protective Barriers
34	Landscape Design
35	Protective Lighting
38	Lamps
38	Luminaries
38	Alarm and Intrusion Detection Systems
41	Electronic Access Control Systems
44	Surveillance Systems and Monitoring



51	<b>Chapter 4 Security Personnel and Training</b>
51	Security Forces
55	Security Experts, Consultants, and Contractors
55	Security Committees and Employee Watch Programs
56	Security Training
64	<b>Chapter 5 Infrastructure Protection</b>
64	Critical Infrastructure Designation
66	Methods to Rate and Prioritize Critical Assets
67	Building Security
71	Bridge and Tunnel Security
74	Rolling Stock and Vehicle Security
80	<b>Chapter 6 Homeland Security</b>
80	Homeland Security Laws and Statutes
83	Homeland Security Presidential Directives
85	National Response Framework
85	National Infrastructure Protection Plan
88	Transportation Systems CI/KR Sector-Specific Plan
93	<b>Appendix A Annotated Bibliography</b>
120	<b>Appendix B Additional Sources of Information</b>
126	<b>Appendix C Acronyms, Abbreviations, and Initialisms</b>
143	<b>Appendix D Glossary</b>



## S U M M A R Y

*Security 101: A Physical Security Primer for Transportation Agencies* provides valuable information about current and accepted practices associated with physical security and its applicability to surface transportation. The main audience for this document is transportation personnel **without** a security background whose work requires them to address, perform, or supervise security activities as part of their overall job responsibilities. Although this document is designed for those with minimal or no formal security training or experience, the report is also a handy reference guide sufficiently detailed to be of use to security professionals as well.

Each chapter addresses fundamental aspects of security strategy, management, or planning. Chapter summaries follow.

Chapter 1 provides a conceptual overview of risk management and then differentiates between risk management and risk assessment so as to reduce confusion resulting from nomenclature. The chapter also presents an overview of the basic steps in risk assessment with an emphasis on describing transportation-related threat and vulnerability analysis and the performance of security surveys.

After conducting its risk assessment, the transportation agency should develop a security plan. In Chapter 2, planning objectives are presented along with an examination of the core elements needed to ensure that a comprehensive plan is developed. Organizational roles and accountabilities are identified with an emphasis on plan maintenance. The chapter concludes with a multi-year overview of the security funding cycle that addresses both operating and capital budget considerations.

For security planning to be effective, appropriate risk reduction methods that can minimize or eliminate identified vulnerabilities must be deployed. Chapter 3 provides an overview of many of the tools and countermeasures that should be considered in the implementation phase of planning so as to improve the security of critical infrastructure and facilities, information systems, and other areas. Concentration is focused on physical security countermeasures, including alarm and intrusion detection systems, video surveillance, lighting, fencing, and manual and electronic locking mechanisms.

Chapter 4 begins with an explanation of the myriad issues associated with fielding a security force and the types of data that can be used to determine the best coverage options available. The advantages and disadvantages of hiring security consultants or security contractors is then discussed, followed by commentary on the importance of involving the agency's non-security personnel in the security effort. The chapter concludes with an overview of security training, starting at the awareness level and proceeding through to the conduct of full-scale exercises and drills.

The transportation operating environment creates significant challenges for security planners charged with properly determining which of the agency's assets require protection. Chapter 5 frames the question for decisionmakers and then summarizes some of the methods used to rate and prioritize critical assets. The chapter then addresses the specifics of building and facility security, transportation bridges and tunnels, and rolling stock.

Chapter 6 identifies core components of the Federal government's homeland security protection strategies. The objective of the materials is to familiarize users with the DHS-driven "national preparedness architecture" that forms the basis for governmental action. By reviewing these activities, in particular those of the executive and legislative branches, that relate to the transportation sector, agencies can gain a sense of the national strategies and supportive frameworks available to help them reduce security risks.

Additional valuable information is provided in appendixes. Appendix A provides an annotated bibliography along with information on subject matter and how or where to acquire copies of the material. Appendix B contains over 100 additional references, including additional source information. Appendix C lists more than 1,000 security-related acronyms and abbreviations compiled during the literature review. Appendix D lists over 1,000 security-related terms and definitions. In some instances, more than one definition for a term or word is given—this reflects the broad range of source documents used in the current state of accepted practice.

# Risk Management and Risk Assessment

In today's transportation operating environment, risk management is the appropriate starting point for any decisionmaking regarding homeland security. Before any plans are made or any money spent, security planners must know about the risks confronting the agency and the tactics or techniques available to them to respond to existing or potential homeland security challenges. This chapter offers a conceptual overview of risk management and then differentiates between risk management and risk assessment so as to eliminate some of the confusion associated with nomenclature. The chapter then summarizes the basic steps in the risk assessment process and describes transportation-related threat and vulnerability analysis and the performance of security surveys. (Critical asset identification is summarized, but is discussed in depth in Chapter 5, Infrastructure Protection.)

So, what is risk management and how does it differ from risk assessment or vulnerability assessment? Understanding these relationships is essential to establishing an effective homeland security and defense strategy. In practice, the terms are often confused or used interchangeably, creating unnecessary communication difficulties.

Risk management consists of the spectrum of activities that a transportation agency can take to resolve identified risks (see Figure 1-1). Such activities include the following:

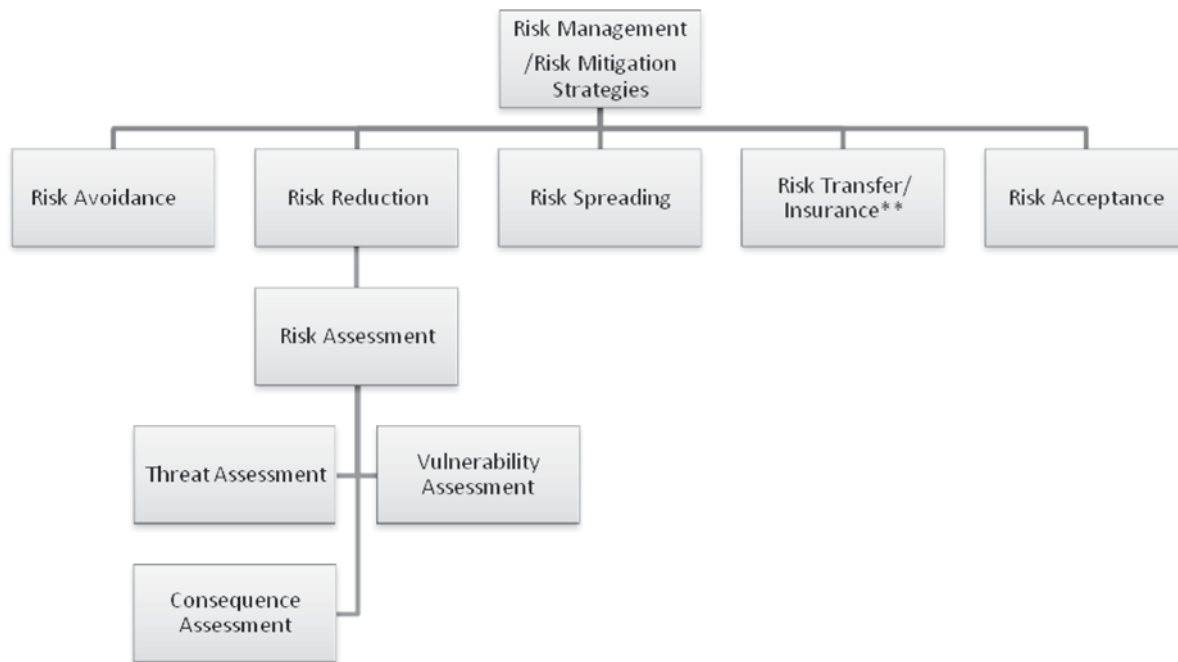
- **Risk avoidance**, accomplished by eliminating the source of the risk;
- **Risk reduction**, characterized by the implementation of actions that lower the risk to the agency;
- **Risk spreading**, through the distribution of risk across various program areas or activities;
- **Risk transfer**, by the use of insurance to cover costs that would be incurred as the result of a loss; and
- **Risk acceptance**, which reflects a knowledgeable determination that a risk is best managed by taking no action at all.

Risk assessment steps can be summarized as follows:

1. Identification and valuation of assets,
2. Enumeration of credible threats to those assets,
3. Documentation of applicable vulnerabilities,
4. Description of the potential consequences of a loss event, and
5. Production of a qualitative or quantitative analysis of resulting risks.

Risks generally are reported in order of priority or severity and attached to some description of a level of risk. Risk assessment answers the questions: What can go wrong? What is the likelihood that it would go wrong? What are the consequences?

## 4 Security 101: A Physical Security Primer for Transportation Agencies



Source: Adapted from *Vulnerability Assessment of Physical Protection Systems* – Mary Lynn Garcia Sandia National Laboratories

\*\* The use of insurance to transfer all or parts of liability to another business or entity is one of the traditional market mechanisms for estimating, pricing, and distributing risk. Risks related to natural hazards such as fire, earthquake, or flood have been identified and assessed and quantitative actuarial data about these types of incidents has been amassed as a means to value potential losses. However the process of understanding and managing terrorism risk is at its very beginning with the insurance industry now struggling to evaluate this relatively new threat. Currently terrorism risk insurance is available only on a limited basis because there is relatively little experience or actuarial data from which to draw conclusions. Prospective buyers of terrorism risk coverage do not have a reasonable basis for estimating their insurance needs. Similarly, sellers of insurance do not have a reliable means for costing out terrorism risk coverage.

**Figure 1-1. Risk management/risk mitigation structure.**

### Risk is a Function of Vulnerability and Consequence

$$\text{Risk} = [\text{Threat} \times \text{Vulnerability}] \times \text{Consequence}$$

**Threat** is a measure of the likelihood that a specific type of attack will be initiated against a specific target

**Vulnerability** is a measure of the likelihood that various types of safeguards against threat scenarios will fail

**Consequence** is the magnitude of the negative effects if the attack is successful

Source: Volpe Risk Assessment and Prioritization, *Volpe Journal*, 2003, pg. 13

The three components of risk assessment are threat assessment, vulnerability assessment, and consequence assessment.

The U.S. Department of Homeland Security (DHS) defines **threat assessment** as “a systematic effort to identify and evaluate existing or potential terrorist threats to a jurisdiction and its target assets.” More broadly, security threat assessments for transportation agencies should consider all threats of criminal activity, as well as terrorist activity. Threat definition has two areas of focus:

- Potential threat scenarios and
- Identification of likely adversaries, tactics, and capabilities.

DHS defines **vulnerability assessment** as “the identification of weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists.” Such weaknesses can occur in facility characteristics, equipment properties, personnel behavior, locations of people and equipment, or operational and personnel practices. **Consequence assessment** is an analysis of the immediate, short- and long-term effects of an event or event combination on an asset—that is, it is an estimate

of the amount of loss or damage that can be expected. In a research project concluded in 2008, consequence assessment, rather than the more normative use of threat assessment information, is used as the basis for risk-based decisionmaking for transportation agencies. As stated in the preface to *NCHRP Report 525, Volume 15*:

The *Guide* deploys a consequence driven methodology to provide a capital budgeting tool for senior transportation agency management. The Guide supplies a means to compare disparate asset classes across a range of threats and hazards on a common scale and establish risk levels for planning. It then provides guidance with regard to the development of a countermeasure program to approach threats and hazards selected by the user as likely to occur in their jurisdiction.

Vulnerability assessment is also essential to risk assessment. In terms of security, it is an evaluation, using either quantitative or qualitative criteria, to do the following:

- Predict the overall effectiveness of a system,
- Identify system weaknesses, and
- Define existing asset protection capabilities against specific threat scenarios and actors.

All risk assessment reflects the need to identify critical assets requiring security and protection. Critical assets include the people, property, and information assets required to enable a transportation agency to execute its primary responsibilities, activities, and functions. Transportation agencies are complex organizations that must integrate many different functional, technical, and operating components and systems. Integration includes physical aspects of the transportation infrastructure and integration of business- and customer-related processes. Safety and reliability, operating policies and procedures, maintenance, training, and customer needs are all important system attributes that affect critical asset identification. All systems consist of an integrated collection of smaller systems or subsystems. How these systems or subsystems are engineered determines how effectively a transportation agency performs.

Assets should be considered critical based on their value as determined by the organization and the short- and long-term consequences of their loss, damage, or destruction. The research performed under NCHRP Project 20-59(17) can help transportation agencies in accomplishing this by the inclusion of a “data threshold model” that helps formulate consequence “thresholds” to determine and prioritize what represents an acceptable or unacceptable occurrence. FEMA’s reference manuals, 426 *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, Dec 2003* and 427 *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, Dec 2003* provide similar support in the area of buildings and other facilities. DHS states, “Criticality assessments help planners determine the relative importance of assets, helping to prioritize the allocation of resources to the most critical assets.” Factors affecting the criticality of assets include

- Loss and Damage Consequences—casualty risk (threat to life and limb), environmental impact, replacement costs, and replacement/down time;
- Consequences to Public Services—emergency response functions, government continuity, and military importance; and
- Consequences to the General Public—available alternatives, economic impact, public health impact, functional importance, and symbolic importance.

Identification of critical assets must be undertaken before the performance of a risk assessment or in particular the vulnerability assessment part of the analysis.

There are four “system risk views” that represent different ways to capture data about the critical infrastructure of transportation systems:

- **Modal View.** The modal view treats all classes of assets within a mode as a system. Infrastructure information in the modal view is categorized by interdependencies and supply implications that are specific to a particular mode of transportation. In addition to focusing on individual assets, nodes, and links, information specific to the modal view includes how those assets, nodes, and links interact within the mode and with other modes, their emergent properties and governing principles, or legislative information with specific modal impact.
- **Geographic View.** The geographic risk view compiles transportation infrastructure data within specific regions of the Nation. The boundaries of those regions may vary based on the

purpose and necessary parameters of an assessment. Because regions may contain markedly different assets and systems, the risks to those systems and the types of data collected from those regions will differ as well. Data collection in this view will allow an information set to be defined by what is physically located in that region and the processes or policies affecting the specific region. Therefore, assets, links, nodes, and emergent properties within a defined geographic area are evaluated as an integrated system.

- **Functional View.** The functional view of data collection assesses the function a system fulfills in the supply chain. Examples of a functional view of systems include all of the assets, links, nodes, processes, policies, and emergent properties associated with deliver of
  - Critical medicines,
  - Chlorine for drinking water or other purposes, or
  - Heating oil to the Northeast.

By examining the function a system plays in society, the critical aspects of the system can be measured. This view is useful in identifying interdependencies with other critical infrastructure.

- **Ownership View.** The ownership view examines information on ownership of assets, including the owner/operators decision structure, policies, and procedures, and recognizes those assets owned by the same entity as an integrated system.

The *Transportation Systems Sector-Specific Plan* of the National Infrastructure Protection Plan (May 2007) identifies the individualized transportation agency approach to asset identification as the “ownership view.”

## Threat Assessment

Threat analysis associated with both terrorism risk assessment and risk insurance has focused on

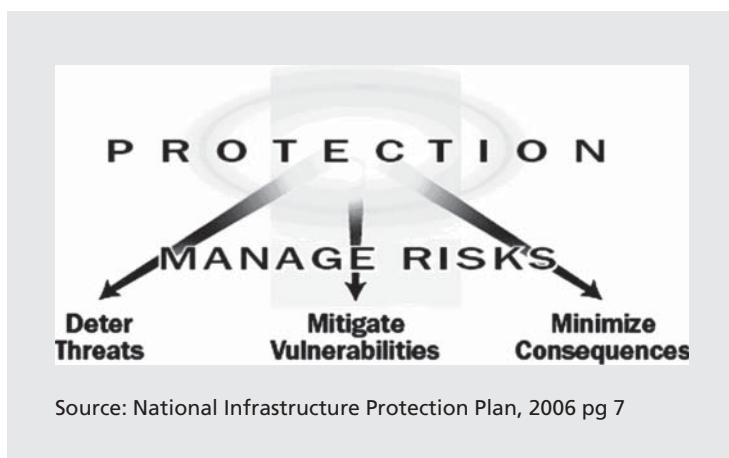
- Threat types and
- A combination of adversary motivations and capabilities.

By approaching analysis in this way, transportation agencies can identify protective strategies that result in actions that **deter the actual threat, mitigate vulnerabilities, and minimize the consequences** of an attack.

## Threat Types

The main categories of homeland security threats against transportation infrastructure are as follows:

- Explosives,
- Weapons of mass destruction,
- Armed assault,
- Arson, and
- Cyber attacks.



Using primarily international terrorist incidents as a historical frame of reference, experience has identified the following categories to describe terrorism-related event types related to physical security:

- Improvised Explosive Device (IED),
- Vehicle Borne Improvised Explosive Device (VBIED),
- Chemical, Biological, Radiological, Nuclear (CBRN), and
- Armed Assault.




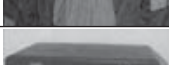






## Explosives

Explosives include both conventional explosives devices (CE) and improvised explosives devices (IEDs). CE is made of components such as Trinitrotoluene (TNT), Semtex, or Plastic Explosives (C4) manufactured either by industry or the military. IEDs can be made of the same commercial or military components or other improvised materials such as ANFO (Fertilizer Bomb), or compounds featuring Ammonium Nitrate with Aluminum, Sugar, or Potassium Chlorate. In the transportation environment, the occurrence of attacks of this type is considered as more likely than for other types of threats.

Explosives cause 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 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.

Two methods of delivery of CEs or IEDs deserve particular attention—Vehicle Borne Improvised Explosives Devices (VBIEDs) and Suicide Bombings. According to the State Department’s Bureau of Diplomatic Security, VBIEDs are “far and away the weapon of choice for terrorist attacks.” Vehicles provide concealment for the bomb as well as the delivery method. As Table 1-1 indicates, concealing a 200- to 500-pound bomb in a sedan is relatively easy.

**Table 1-1. Evacuation distance by threat and explosive mass.**

	Threat Description		Explosives Mass <sup>1</sup> (TNT equivalent)	Building Evacuation Distance <sup>2</sup>	Outdoor Evacuation Distance <sup>3</sup>
High Explosives (TNT Equivalent)		Pipe Bomb	5 lbs 2.3 kg	70 ft 21 m	850 ft 259 m
		Suicide Belt	10 lbs 4.5 kg	90 ft 27 m	1,080 ft 330 m
		Suicide Vest	20 lbs 9 kg	110 ft 34 m	1,360 ft 415 m
		Briefcase/Suitcase Bomb	50 lbs 23 kg	150 ft 46 m	1,850 ft 564 m
		Compact Sedan	500 lbs 227 kg	320 ft 98 m	1,500 ft 457 m
		Sedan	1,000 lbs 454 kg	400 ft 122 m	1,750 ft 534 m
		Passenger/Cargo Van	4,000 lbs 1,814 kg	640 ft 195 m	2,750 ft 838 m
		Small Moving Van/ Delivery Truck	10,000 lbs 4,536 kg	860 ft 263 m	3,750 ft 1,143 m
		Moving Van/Water Truck	30,000 lbs 13,608 kg	1,240 ft 375 m	6,500 ft 1,982 m
		Semitrailer	60,000 lbs 27,216 kg	1,570 ft 475 m	7,000 ft 2,134 m

<sup>1</sup> Based on the maximum amount of material that could reasonably fit into a container or vehicle. Variations possible.

<sup>2</sup> Governed by the ability of an unreinforced building to withstand severe damage or collapse.

<sup>3</sup> Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. These distances can be reduced for personnel wearing ballistic protection. Note that the pipe bomb, suicide belt/vest, and briefcase/suitcase bomb are assumed to have a fragmentation characteristic that requires greater standoff distances than an equal amount of explosives in a vehicle.

Source: Adapted from *Improvised Explosive Device (IED) Safe Standoff Distance Cheat Sheet*, National Ground Intelligence Center US Army Unclassified



Suicide bombings are characterized as an attack on a target in which an attacker intends to kill others, knowing that he or she will either certainly or most likely die in the process. The means of attack have included vehicles filled with explosives, passenger planes carrying large amounts of fuel, and individuals wearing explosives-filled vests.

## **Weapons of Mass Destruction**

Weapons of Mass Destruction or Effect (WMD)/(WME) include chemical, biological, radiological or nuclear (CBRN) devices designed to inflict mass casualties.

Harmful chemicals available for use as terrorist weapons include warfare agents developed for military use, nerve agents (e.g., Sarin and VX), blister agents (e.g., Mustard), blood agents (e.g., Hydrogen Cyanide), and choking agents (e.g., Chlorine and Phosgene).

Also of concern are toxic industrial and commercial chemicals manufactured in the making of petroleum, textiles, plastics, fertilizers, paper, foods, pesticides, household cleaners, and other products. From a transportation perspective, these types of chemicals, known as hazardous materials (HazMat), are particularly important because freight railroads and highways are used to transport them in large quantities, often through high population density areas. For passenger, commuter, or transit agencies that share railroad lines with these carriers, protective strategies designed to reduce the risks associated with transport are a high priority. Finally there are the chemical toxins of biological origin such as Botulinum or Ricin. These are highly toxic products of plants, animals, and bacteria. They can be naturally occurring or prepared in a laboratory. Botulinum toxin is the most poisonous substance known to science.

Chemical agents can be released in the form of poisonous gases, liquids, or solids. Typically liquids and vapors are more lethal than solids. Chemical agents are usually fast acting, with the major exception of mustard agents for which symptoms appear hours after exposure. Poisoning by chemicals is not contagious, but the presence of residual chemical agents on the skin or clothing of an exposed individual can cause others to be affected. Once the agent is neutralized or removed, the illness stops spreading. The toxicity, measured in parts per million (PPM) and concentration of a chemical agent determines the severity of an attack. Chemical agents are typically more deadly in confined or crowded areas such as buildings or subways. They can be deployed by spraying with wet or dry aerosol sprayers, vaporizing the chemical for release, using an explosive device to disperse the chemical, pouring, or contamination of food, water, or another ingestible such as pharmaceutical drugs. The toxicity of chemicals varies greatly. Some are acutely toxic (cause immediate symptoms); others are not very toxic at all. Table 1-2 lists the effects and treatment of some chemical weapons developed for military use. The varying toxicity of chemicals is listed in Table 1-3.

Weaponized biological agents are naturally occurring microbes or microorganisms deployed in their existing state or modified to increase virulence, designed to cause mass casualties through disease and death. The Centers for Disease Control and Prevention (CDC) groups biological agents into three categories (A, B and C), based on factors such as availability, capability of dissemination, mortality or illness rates and impact on the public health system. Category A agents include Anthrax, Botulinum Toxin, Plague, Smallpox, Tularemia, and Viral Hemorrhagic Fevers (e.g., Ebola, Marburg virus, Lassa, and Machupo). These “highest priority agents” are the so-called “bio-weapons” because they provide the building blocks for weaponization. Category B agents include Brucellosis, Epsilon Toxin, Food Safety Threats (e.g., E. coli 0157:H7, Salmonella, Shigella), Glanders, Melioidosis, Psittacosis and Q Fever, Ricin Toxin, and Staphylococcal Enterotoxin B [SEB], Typhus Fever, Viral Encephalitis, and Water Safety Threats (e.g., Cholera, Giardiasis, and

**Table 1-2. Effects and treatment of some chemical weapons developed for military use.**

	Nerve Agents		Blister Agents (injure skin, eyes, and airways)		Blood Agents (cause blood changes and heart problems)		Choking Agents	
<b>Examples</b>	Sarin	VX	Mustard	Lewisite	Hydrogen Cyanide	Cyanogen Chloride	Chlorine	Phosgene
<b>Odor</b>	Odorless		Garlic or Mustard	Geraniums	Burnt almonds		Bleach	Mown hay
<b>Persistency*</b>	Non-persistent (min. to hrs.)	Persistent (>12 hrs.)	Persistent		Non-persistent		Non-persistent; vapors may hang in low areas	
<b>Rate of Action</b>	Rapid for vapors; liquid effects may be delayed		Delayed	Rapid	Rapid		Rapid at high concentrations; delayed at lower concentrations	
<b>Signs and Symptoms</b>	Headache, runny nose, salivation, pinpointing of pupils, difficulty in breathing, tight chest, seizures, convulsions, nausea, and vomiting		Red, burning skin, blisters, sore throat, dry cough; pulmonary edema, eye damage, nausea, vomiting, diarrhea. Symptoms may be delayed 2 to 24 hrs		Cherry red skin/lips, rapid breathing, dizziness, nausea, vomiting, convulsions, dilated pupils, excessive salivation, gastrointestinal hemorrhage, pulmonary edema, respiratory arrest		Eye and airway irritation, dizziness, tightness in chest, pulmonary edema, painful cough, nausea, headache	
<b>First Aid</b>	Remove from area, treat symptomatically, Atropine and pralidoxime chloride (2-PAM chloride), diazepam for seizure control		Decontaminate with copious amount of water, remove clothing, support airway, treat symptomatically		Remove from area, assist ventilations, treat symptomatically, administer cyanide kit		Remove from area, remove contaminated clothing, assist ventilations, rest	
<b>Decontamination</b>	Remove from area, remove clothing, flush with soap and water, aerate							

\*How long a chemical remains at toxic levels

Source: *Chemical Attack Warfare Agents, Industrial Chemicals and Toxins*, National Academy of Sciences 2004

Cryptosporidiosis). Scientists have experience with Category B agents as infectious diseases but are unclear about their potential for weaponization. Category C agents include emerging infectious diseases such as Nipah virus and Hantavirus.

Biological agents are grouped as being either (1) infectious or (2) infectious *and* contagious. A microorganism that causes infectious disease invades the body, making the person sick by attacking organs or cells. Sometimes called pathogens, these microscopic organisms include both viruses and bacteria. There is usually a delay in the onset of symptoms—an “incubation period.” Diseases that are both infectious and contagious can be caught by a person who comes in contact with someone else who is infected. The level of contact required to transmit the illness between people can be slight—through a sneeze or cough. But the contagiousness of a particular disease has nothing to do with the seriousness of the illness. For example, both plague and the common cold are both highly contagious, but plague is a much more serious disease. Some infectious diseases are not contagious at all such as Botulism or Tularemia. Biological agents can enter the body through absorption, inhalation, ingestion, or injection. Biological weapons can be prepared for delivery in wet or dry form. Delivery can be through aerosol sprayers; explosive devices; transmission through insects, animals, or humans; introduction into food or water; or, in some cases, on or inside of objects (e.g., anthrax in envelopes).

**Table 1-3. Varying toxicity of chemicals.**

The more toxic a chemical, the smaller the amount of chemical required to cause harm. The table compares the lethal concentrations in parts per million (ppm) for acute (all-at-once) exposures to some chemical weapons and some common industrial chemicals.

Chemical agent	Approx. lethal concentration* (in ppm)
<b>Some Chemical Weapons</b>	
Sarin (GB)	36
Hydrogen Cyanide**	120
<b>Some Industrial Chemicals</b>	
Chlorine**	293
Hydrogen chloride	3,000
Carbon monoxide	4,000
Ammonia	16,000
Chloroform	20,000
Vinyl chloride	100,000

\*Based on LC<sub>50</sub> values in laboratory rats: exposure concentration for 60 minutes at which 50% of rats would die. Rats are used for toxicology tests in part because of similarity to humans, but they are likely to be more susceptible because they have higher metabolisms.

\*\*Used both as chemical weapons and as industrial chemicals

Source: NRC, EPA, and ATSDR

Source: *Chemical Attack Warfare Agents, Industrial Chemicals and Toxins*, National Academy of Sciences 2004

**Table 1-4. Onset, health impacts, and treatments for some agents of concern.**

Disease (agent)	Incubation period*	Symptoms
<b>HIGH THREAT AGENTS (CATEGORY A)</b>		
<b>Anthrax</b> ( <i>Bacillus anthracis</i> ) (inhalational)	typically 1–6 days, but up to 42	Fever, cough, profound sweats malaise, fatigue, myalgias
<b>Plague</b> ( <i>Yersinia pestis</i> )	1–7 days (usually 2–3 days)	Fever, cough, shortness of breath, sore lymph nodes
<b>Tularemia</b> ( <i>Francisella tularensis</i> )	1–21 days (avg 3–6)	Fever, cough, pneumonia, headache
<b>Marburg</b> (Viral hemorrhagic fever)	4–21 days	Sudden onset, fever, headache, followed by vomiting and diarrhea, rash, generalized bleeding in severe cases
<b>Ebola</b> (Viral hemorrhagic fever)	4–21 days	Sudden onset, fever, headache, followed by vomiting and diarrhea, rash, generalized bleeding in severe cases
<b>Smallpox</b> ( <i>Variola major virus</i> )	7–17 days (avg 12)	Fever, aches, after 2–4 days rash appears
<b>Botulism</b> ( <i>Clostridium botulinum</i> toxin)	12 hours–5 days	Muscle paralyzing illness
<b>LOWER THREAT AGENTS (SELECTED CATEGORY B AGENTS)</b>		
<b>Cholera</b> ( <i>Vibrio cholerae</i> )	4 hours–5 days (usually 2–3 days)	Sudden onset of voluminous watery diarrhea, vomiting, cramps, dehydration
<b>Glanders</b> ( <i>Burkholderia mallei</i> )	1–14 days via aerosol	Pneumonia with or without blood poisoning, ulcers in nose, mouth, throat and lungs
<b>Q fever</b> ( <i>Coxiella burnetii</i> )	7–41 days	Flu-like illness that can lead to pneumonia and hepatitis
<b>Encephalitis</b> (Alphaviruses)	2–6 days	Fever, aches, pain behind the eye, nausea, vomiting
<b>Ricin</b> ( <i>Ricinus communis</i> )	18–24 hours	Can shut down organ function

Source: *Biological Attack Human Pathogens, Biotoxins, and Agricultural Threats*, National Academy of Sciences, 2005

Table 1-4 outlines the disease, incubation period, and symptoms for selected Category A and Category B biological agents. Concern exists about the potential for a terrorist attack involving radioactive materials, possibly through the use of a Radiological Dispersion Device (RDD). The best known type of RDD is a “dirty bomb,” a device that uses a conventional explosion to disperse radioactive material so that the blast will contaminate an area with radioactive particles. RDDs include other means of dispersal such as opening a container of radioactive materials in a populated area or dispersing powdered or aerosolized materials using sprayers or even airplanes. Radioactive isotopes are considered to have either a high-level or low-level of radioactivity. This is based on the rate of radioactive decay. The faster an isotope decays, the faster it releases, and exhausts, its radiation. The radioactivity of a mass of material is measured in Curies (Ci; 1 Ci =  $3.7 \times 10^{10}$  disintegrations per second). Cobalt-60 (the number is the number of neutrons plus protons in the atom’s nucleus), with a half-life of 5.3 years, is highly radioactive; uranium-235, with a half-life of over 700 million years, is not. High-level radioactive materials are difficult for terrorists to acquire so there is a greater chance that the radioactive materials used in a dirty bomb would come from low-level radioactive sources. Low-level radioactive sources are found in hospitals, on construction sites, and at food irradiation plants. If low-level radioactive sources were to be used, the primary danger from a dirty bomb would be the blast itself. Most dirty bombs and other RDDs would have very localized effects, ranging from less than a city block to several square miles. The effective range would depend on factors such as the

amount and type of material, method of dispersal, and local weather conditions. According to the CDC, “at the levels created by most probable sources, not enough radiation would be present in a dirty bomb to cause severe illness from exposure to radiation.”

Radiation is energy moving in the form of particles or waves. Examples of electromagnetic radiation are heat, light, radio waves, and microwaves. Radiation strikes people constantly, but most of it, like radio waves and light, is not “ionizing,” meaning it does not have enough energy to damage cells significantly. **Ionizing radiation** is a very high-energy form of electromagnetic energy that can adversely affect health in the human body. The extent of the effect depends on the amount of energy absorbed measured in “rem.” Higher doses produce direct clinical effects, including tissue damage, radiation sickness and, at very high levels, rapid death. With chronic low-level exposure, no clinical effects are observed, but the exposed individual may have an increased lifetime risk of developing cancer. **Common types of radioactive materials** include Cobalt-60, Strontium-90, and Plutonium-238.

### What is ionizing radiation?

When radioactive elements decay, they produce energetic emissions (alpha particles, beta particles, or gamma rays) that can cause chemical changes in tissues. The average person in the United States receives a “background” dose of about one-third of a rem\* per year—about 80% from natural sources including earth materials and cosmic radiation, and the remaining 20% from man-made radiation sources, such as medical x-rays. There are different types of radioactive materials that emit different kinds of radiation:

**Gamma and x-rays** can travel long distances in air and can pass through the body exposing internal organs; it is also a concern if gamma-emitting material is ingested or inhaled.

**Beta radiation** can travel a few yards in the air and in sufficient quantities might cause skin damage; beta-emitting material is an internal hazard if ingested or inhaled.

**Alpha radiation** travels only an inch or two in the air and cannot even penetrate skin; alpha-emitting material is a hazard if it is ingested or inhaled.

\*A rem is a measure of radiation dose, based on the amount of energy absorbed in a mass of tissue. Dose can also be measured in Sieverts (1 Sievert = 100 rem)

Source: *Radiological Attack, Dirty Bombs, and Other Devices*, National Academy of Sciences, 2004

### What are some common radioactive materials used in our society?

#### GAMMA EMITTERS

**Cobalt-60 (Co-60)**—cancer therapy, industrial radiography, industrial gauges, food irradiation.

**Cesium-137 (Cs-137)**—same uses as Cobalt-60 plus well logging.

**Iridium-192 (Ir-192)**—industrial radiography and medical implants for cancer therapy.

#### BETA EMITTER

**Strontium-90 (Sr-90)**—radioisotope thermoelectric generators (RTGs), which are used to make electricity in remote areas.

#### ALPHA EMITTERS

**Plutonium-238 (Pu-238)**—research and well logging and in RTGs for space missions.

**Americium-241 (Am-241)**—industrial gauges and well logging.

Source: *Radiological Attack, Dirty Bombs, and Other Devices*, National Academy of Sciences, 2004

### Nuclear Bombs at Hiroshima and Nagasaki

The August 1945 bombings of Hiroshima and Nagasaki have been the only use or detonation of nuclear weapons except for testing purposes. The Hiroshima bomb was approximately a 16-kiloton uranium bomb; the Nagasaki bomb was approximately a 21-kiloton plutonium bomb. Both were detonated in the air at an altitude of approximately 1,600 feet. The bomb at Hiroshima destroyed buildings over roughly 4 square miles of the city, and about 60,000 people died immediately from the blast, thermal effects, and fire. Within 2–4 months of the bombings, a total estimated 90,000 to 140,000 deaths occurred in Hiroshima and about 60,000 to 80,000 deaths occurred in Nagasaki, mostly as a result of the immediate effects of the bomb and not to fallout.

In a group of 87,000 survivors exposed to radiation who were followed in health studies over the past 60 years,\* there were about 430 more cancer deaths than would be expected in a similar but unexposed population (there were 8,000 cancers from all causes compared to an expected 7,600). The additional cancer deaths are attributable to radiation. Nearly half of the people in those studies are still alive.

\*The mean dose of those survivors was 16 rad.

Source: *Nuclear Attack*, National Academy of Sciences, 2005

A nuclear attack by terrorists is a high-order-of-magnitude event that could kill a large number of people. As mentioned previously, a dirty bomb containing high-level radioactive material could be a means to deliver a nuclear attack. The use of an improvised nuclear device (IND) or a nuclear weapon must also be considered. INDs, also called “suitcase bombs or suitcase nukes,” describe a small nuclear weapon, small enough to fit in a suitcase, which can produce a nuclear blast. According to the Department of Health and Human Services “the design and destructive nature of an IND is comparable to the bomb dropped on Hiroshima Japan, at the end of World War II.” Larger nuclear weapons and the explosions that result from their use are classified based on the amount of energy they produce or “yield.” A nuclear weapon deployed by terrorists would be expected to have a yield of less than one to several kilotons. A kiloton is not the weight of the bomb but rather the equivalent energy of an amount of the explosive TNT (1kT=1,000 tons of TNT). Large military nuclear weapons are in the megaton (MT) range (1MT=1,000kT). The highly purified plutonium and uranium needed to make a nuclear weapon or suitcase bomb are difficult to acquire.

Considerable engineering skill and expertise would be required to construct a nuclear device using plutonium; devices using uranium are technically easier to construct.

A nuclear event involves nuclear fission (splitting of atoms) and a highly destructive explosion that creates instant devastation. Significant fatalities, injuries, and infrastructure damage result from the heat and blast of the explosion and persistent high levels of radioactivity are the aftermath of both the initial nuclear radiation and the subsequent radioactive fallout that occurs.

### Characteristics of a Nuclear Explosion

A **fireball**, roughly spherical in shape, is created from the energy of the initial explosion. It can reach tens of millions of degrees.

A **shockwave** races away from the explosion and can cause great damage to structures and injuries to humans.

A **mushroom cloud** typically forms as everything inside of the fireball vaporizes and is carried upwards. Radioactive material from the nuclear device mixes with the vaporized material in the mushroom cloud.

**Fallout** results when the vaporized radioactive material in the mushroom cloud cools, condenses to form solid particles, and falls back to the earth. Fallout can be carried long distances on wind currents as a plume and contaminate surfaces miles from the explosion, including food and water supplies.

The ionization of the atmosphere around the blast can result in an **electromagnetic pulse (EMP)** that, for ground detonations, can drive an electric current through underground wires causing local damage. For high-altitude nuclear detonations, EMP can cause widespread disruption to electronic equipment and networks.

Source: *Nuclear Attack*, National Academy of Sciences, 2005

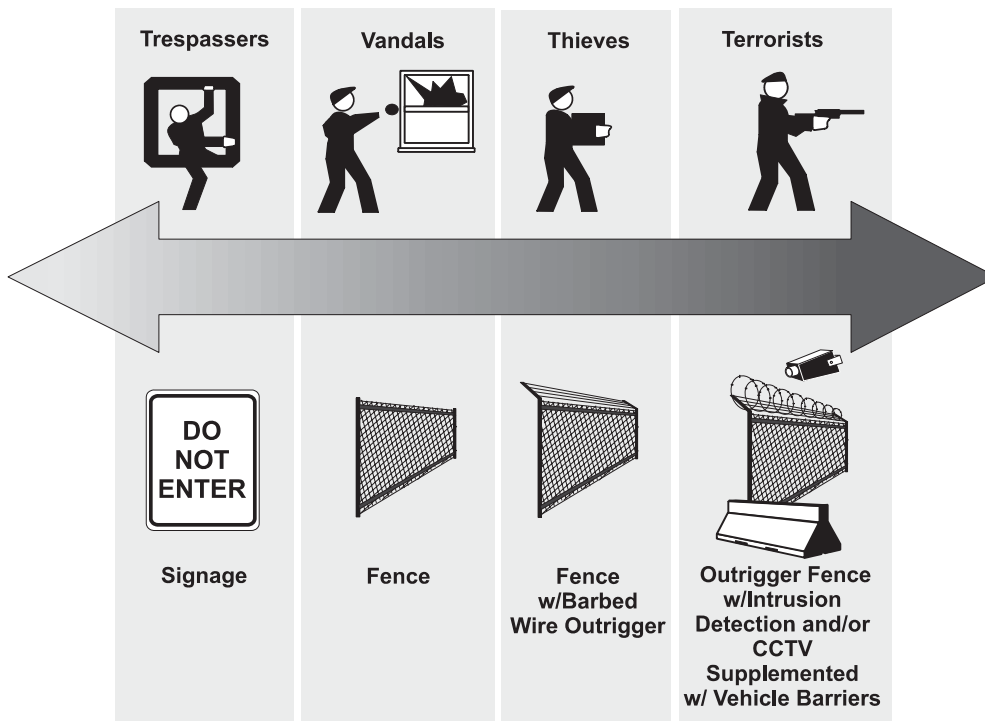
## Armed Assault

Terrorist-related Armed Assault by one or more gunmen, although rare in the United States, occurs much more frequently in other parts of the world. In particular, in Afghanistan and Iraq, terrorists have deployed “hit and run” tactics as a form of “asymmetrical warfare” designed to reduce personnel losses and inflict maximum casualties. “Hit and run” assault involves a sudden attack on a target and immediate withdrawal to avoid adversary response or retaliation. In some instances, the tactic is coupled along with the use of a massive amount of firepower without concern for target accuracy. This type of indiscriminate attack would likely prove difficult to prevent or overcome. Another tactic seen repeatedly in the school shootings at incidents like Columbine and Virginia Tech is the suicide gunman who bears multiple firearms and fires at will until either killed or committing suicide. This type of attack is carried out using small arms which can include pistols, rifles, shotguns, or submachine guns that can be either military issue or civilian weapons.

## Adversary Types and Motivations

In Figure 1-2, the FTA makes the point that security countermeasures should be designed commensurate with the type of adversary who may attack the transportation facility. Conceptually, this represents sound practice; however, transportation agencies should not draw threat-related conclusions from presumptions about adversary classification assessments taken in isolation. Care should be taken to ensure that threat assessments are also scenario-based and driven by both factual information and credible intelligence.

As a part of the Department of Defense Unified Facilities Criteria (UFC), DOD published *Security Engineering Facilities Planning Manual Draft UFC 4-020-01* in March 2006. The manual contains an overview of aggressor types, capabilities, and tactics; this material has been adapted in Tables 1-5 through 1-7 for transportation agency security planning purposes. Aggressors per-



Source: *Security Design Considerations*, FTA, 2004

**Figure 1-2. Security countermeasures by type of adversary.**

**Table 1-5. Criminals by levels of sophistication.**

Type	Description	Typical Targets
Unsophisticated	Unskilled in the use of tools and weapons and having no formal organization. Theft by insiders is also common.	Targets that meet their immediate needs such as drugs, money, and pilferable items. Opportune targets that present little or no risk. Breaking and entering or smash-and-grab techniques are common.
Sophisticated	Skilled in the use of certain tools and weapons. Efficient and organized. They plan their attacks and have sophisticated equipment and the technical capability to employ it. Often assisted by insiders.	They target high-value assets and frequently steal in large quantities, but target assets with relatively low risk in handling and disposal.
Organized Groups	Highly sophisticated, can draw on specialists, and can obtain the equipment needed to achieve their goals efficiently. These groups form efficient, hierarchical organizations which can employ highly paid insiders. Examples include drug cartels, organized crime "families," the Yakuza, and MS-13.	Organized criminal groups may target goods, commodities, or opportunities where there is a high degree of risk in handling and disposal such as large quantities of money, equipment, and arms, ammunition, and explosives.

Source: Adapted from *Security Engineering Facilities Planning Manual Draft* UFC 4-020-01, 2006

form hostile acts against assets such as equipment, personnel, and operations. The UFC presents four major aggressor objectives to describe aggressor behavior:

- Inflicting injury or death on people;
- Destroying or damaging facilities, property, equipment, or resources;
- Stealing equipment, materiel, or information; and
- Creating adverse publicity.

The three broad categories of aggressors are criminals, protesters, and terrorists. Criminals are grouped into three categories; all are assumed to share the objective of theft of assets (see Table 1-5).

The two categories of protestors are vandals/activists and extremist protest groups. Regardless of category, these groups are either politically or issues oriented and act out of frustration or anger against the actions of other social or political groups. The primary objectives of both groups commonly include destruction and publicity. Table 1-6 provides additional information.

Terrorists are grouped into three categories: domestic, international, and state-sponsored. Domestic terrorists are indigenous to the United States, Puerto Rico, and the U.S. territories and

**Table 1-6. Protesters.**

Type	Description	Objectives	Typical Targets
Vandals/Activists	Usually unsophisticated. Superficially destructive. Actions may be covert or overt.	No injury to people. Limited damage to targets.	Symbolic targets that pose little risk to them.
Extremist Protest Groups	Moderately sophisticated and usually more destructive than vandals. Actions are frequently overt	More extensive damage and may include possible injury to people	Symbolic targets and things they consider environmentally unsound

Note: In this text, only violent protesters are considered a threat.

Source: Adapted from *Security Engineering Facilities Planning Manual Draft* UFC 4-020-01 2006

**Table 1-7. Terrorists by areas of operation and levels of sophistication.**

Types	Description	Orientation	Examples
Domestic	Typically operating in distinct areas of the country. Most acts of terrorism in the United States by domestic terrorists have been less severe than those outside the United States, and operations have been somewhat limited. A notable exception was the bombing of the Alfred P. Murrah Building in Oklahoma City.	Politically oriented	Ethnic and white supremacy groups, many with ties to groups that originated during the 1960s and 1970s.
International	Typically better organized and better equipped than their domestic counterparts. More severe and more frequent attacks than those by domestic terrorists in the United States.	Politically, ethnically, or religiously oriented	Foreign terrorist groups designated by the U.S. Department of State include the Revolutionary Group 17 November, the Aum Shinrikyo Group, Basque Fatherland and Liberty (ETA), Sendero Luminoso (Shining Path), and the al-Aqsa Martyrs Brigade.
State-Sponsored	Foreign government support may include intelligence and even operational support. Often, they have military capabilities and a broad range of military and improvised weapons. They have historically staged the most serious terrorist attacks, including suicide attacks. Some have legitimate political wings in addition to their terrorist wings.	Predominantly ethnically or religiously oriented	State-sponsored terrorist groups designated by the U.S. Department of State include al Qaida, the Palestinian Islamic Jihad, Hezbollah, and the Revolutionary Armed Forces of Columbia (FARC).

\*Based on their areas of operation and their sophistication.

Source: Adapted from *Security Engineering Facilities Planning Manual* Draft UFC 4-020-01, 2006

not directed by foreign interests. International terrorists are either connected to a foreign power or they transcend national boundaries. State-sponsored terrorists generally operate independently, but receive foreign government support.

Terrorists are motivated by ideology, politics, or specific issues. They often work in small, well-organized groups or cells. They are sophisticated, skilled with tools and weapons, and can plan efficiently. Terrorist objectives usually include death, destruction, theft, and publicity. Table 1-7 provides additional information.

## Vulnerability Assessment

Managing security risk for transportation agencies is a threat- and scenario-based activity. Threat definition is the tool by which vulnerabilities of transportation operations and systems are measured. Agency police or security personnel, assisted by federal, state, and local law enforcement and homeland security professionals, must evaluate the actual and potential threats against their respective agencies in terms of both threat types and aggressor types. After the baseline of threat information has been identified, security management should collect data and information about the specific organization at risk in order to determine the existing status of systems and security countermeasures. Weaknesses and opportunities for aggressor exploitation must be analyzed so as to establish the current capabilities of the organization to block, thwart, or mitigate an attack. The performance of a vulnerability assessment, sometimes referred to as a security vulnerability assessment (SVA), is used to address this issue. Vulnerability assessment starts with an examination of the transportation agency's assets in order to establish what needs to be protected. Next, the capabilities of existing protection systems to secure those assets are



evaluated. Finally, security gaps that should be addressed to reduce or buy down security risk are determined.

## Security Surveys

The preferred means to conduct an SVA is by performing a security survey. The survey is a fact-gathering question-based process that uses various data collection tools to obtain necessary information about the characteristics of the organization, its systems and operations, and the consequences to the organization that would result from a successful attack against identified threat targets. SVA methodology varies greatly. Different approaches and techniques for assessing agency vulnerabilities are numerous. In the transportation sector, some of the more frequently used methodologies include Analytical Risk Methodology (ARM), Maritime Sector Risk Analysis Methodology (MSRAM), DHS Transit Risk Analysis Methodology (DHS-TRAM), CARVER, Sandia National Labs Risk Assessment Methodologies (RAM), and the Homeland Security Comprehensive Assessment Model (HLS-CAM).

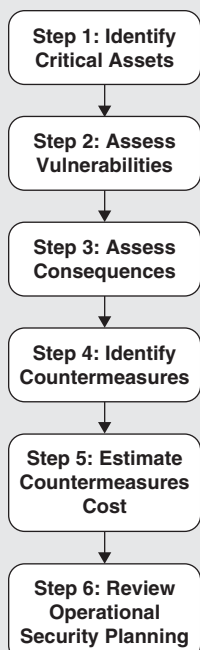
In May 2002, the American Association of State Highway and Transportation Officials (AASHTO) posted on-line a comprehensive *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. The 2002 *Guide* presents a **six-step approach to conducting a security vulnerability assessment**.

Additionally, self-directed vulnerability assessments methods and checklists are available from various organizations, including DHS, DOE, and the FBI. The plethora of methodologies has resulted partly from lack of precision in the formulation of data collection elements and a less-than-rigorous quality review of process by government and the security industry. However, this variation in methodologies also results from the fact that vulnerability assessment of industry sectors, in this case the transportation sector, is significantly industry and agency specific. In fact, different modes within the transportation sector (e.g., aviation, rail, highway, or maritime) all have unique organizational characteristics and operating environments. What works in the closed and highly regulated aviation sector from the standpoint of SVA would not transfer well to the open and ubiquitous public transit system.

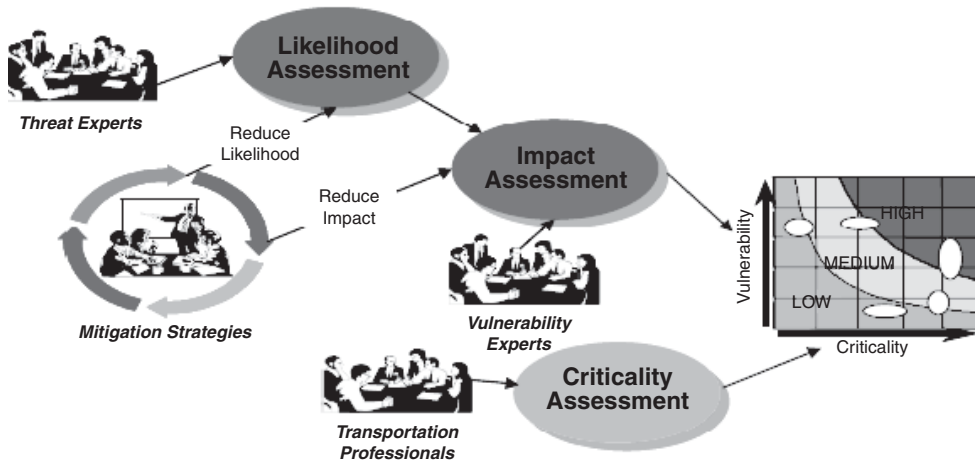
## Performing the Security Survey

Ideally, the SVA should be conducted by a trained team of security professionals using an industry-accepted methodology rather than a self-assessment question list or checklist. Assessors must be able to understand and interpret the protection objectives, operating environment, priorities, and inherent weaknesses of the transportation agency under review. The team should include a project manager responsible for the final report product of the assessment, as well as subject matter experts in transportation sector and mode security. The security-trained component of the team should be assisted by a cross-disciplinary group of management and operating personnel with expertise in agency operations, including communications, engineering, mechanical, facilities, and transportation. To the extent necessary, this group should be supported by specialists (e.g., information technology professionals, human resources trainers, finance and procurement officers, and systems analysts). Figure 1-3 illustrates how an SVA team works through the critical asset evaluation step of the 2002 *Guide* approach. Note the presence of threat experts, vulnerability experts, and transportation professionals on the SVA team.

The result of the SVA is the publication of a report that establishes the current security status of the transportation agency, in terms of



Source: *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, American Association of State Highway and Transportation Officials, 2002



Source: *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, AASHTO, 2002

**Figure 1-3. Critical asset evaluation step.**

- Critical asset identification,
- Threats and vulnerabilities existing against those assets, and
- Consequences or ramifications of successful attacks against those assets.

The efficacy of this report will be determined primarily by the comprehensiveness and derivation of facts and opinions resulting from interviews, examinations, observations, analysis, and investigations. To the extent practicable, opinions should be expressed as such. The report should conclude with findings and recommendations that can be used to help formulate the transportation agency's security needs and requirements planning documentation.



## CHAPTER 2

# Plans and Strategies

Once the transportation agency has conducted its risk assessment, the next step is to develop a security plan. In this chapter, planning objectives are highlighted and the core components or elements needed to ensure that a comprehensive plan is developed are examined. Organizational roles and accountabilities are identified with an emphasis on plan maintenance. The chapter concludes with a multi-year overview of the security funding cycle that addresses both operating and capital considerations.

### Objectives of a Security Plan

A security plan is a written document containing information about an organization's security policies, procedures, and countermeasures. The plan should include a concise statement of purpose and clear instructions about agency security requirements. The stated objectives of the security plan need to be attainable and easily understood. The plan should identify intended users and their assignments, responsibilities, and authorities to act pursuant to the plan's direction. Creating a sound security plan is often as much a management issue as it is a technical one—It involves motivating and educating managers and employees to understand the need for security and their role in developing and implementing an effective and workable security process. Organizational leaders must ensure that security planning is an actual functional activity and part of the agency's culture.

In the transportation environment, the objective of security planning is to ensure both the integrity of operations and the security of assets. Planning for security should result in the integration of protective systems and processes into the organization's daily business routine. The security plan should also ensure that agency personnel can respond effectively to security-related incidents or emergency conditions.

The Public Transportation System Security and Emergency Preparedness Planning Guide (SSEPP) published in 2003 by the Department of Transportation, Federal Transit Administration, contains the following statement of purpose:

**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.

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 document continually under review and subject to change. In developing the security plan, the need for flexibility should be reinforced. Alternatives and options should be incorporated into the plan to make the organization flexible and capable of responding to various situations or unexpected events.

## Benefits of a Security Plan

The most significant benefit of having a security plan is the help it provides in ensuring that security is integrated into the daily business of the transportation agency. The security plan directs personnel toward prevention and mitigation of the effects of security incidents by integrating approaches that have proven effective into the operating environment.

Security must compete with other system goals, including those of the operations department, engineering, maintenance and others, for limited resources and available funding. Because security is a functional area with little observable return on investment, it can be difficult to balance security costs against other more traditional or bottom line-enhancing transportation agency initiatives. Security initiatives must be seen as cost-effective and well defined in order to compete successfully. Developing a security plan is an effective way to meet cost-benefit and competitive resource challenges. The plan can also reduce litigation risk and insurance costs. When the security plan is well structured and soundly developed using the appropriate strategies and elements, the resulting product can be a blueprint for short-term and multi-year security planning. The security plan can address how future purchases would fit into the overall agency operating and capital investment strategy. Security planning also sets out the policies and procedures related to security and any special requirements or considerations unique to the specific agency. The security plan directs personnel toward preventing and mitigating the effects of security incidents by identifying security countermeasures and emergency preparedness response activities that should be taken to protect the transportation system, its employees and customers, and the surrounding communities.

### Security Plan Benefits

- Defines resource requirements for staffing and equipment
- Coordinates the activity of different departments and functions
- Establishes action steps for employees in response to an incident
- Promotes understanding of the issues involved during a crisis
- Identifies information requirements for security incidents
- Promotes a sense of ownership and buy-in by employees
- Ensures a clear division of tasks and responsibilities
- Identifies training requirements

## Elements of a Security Plan

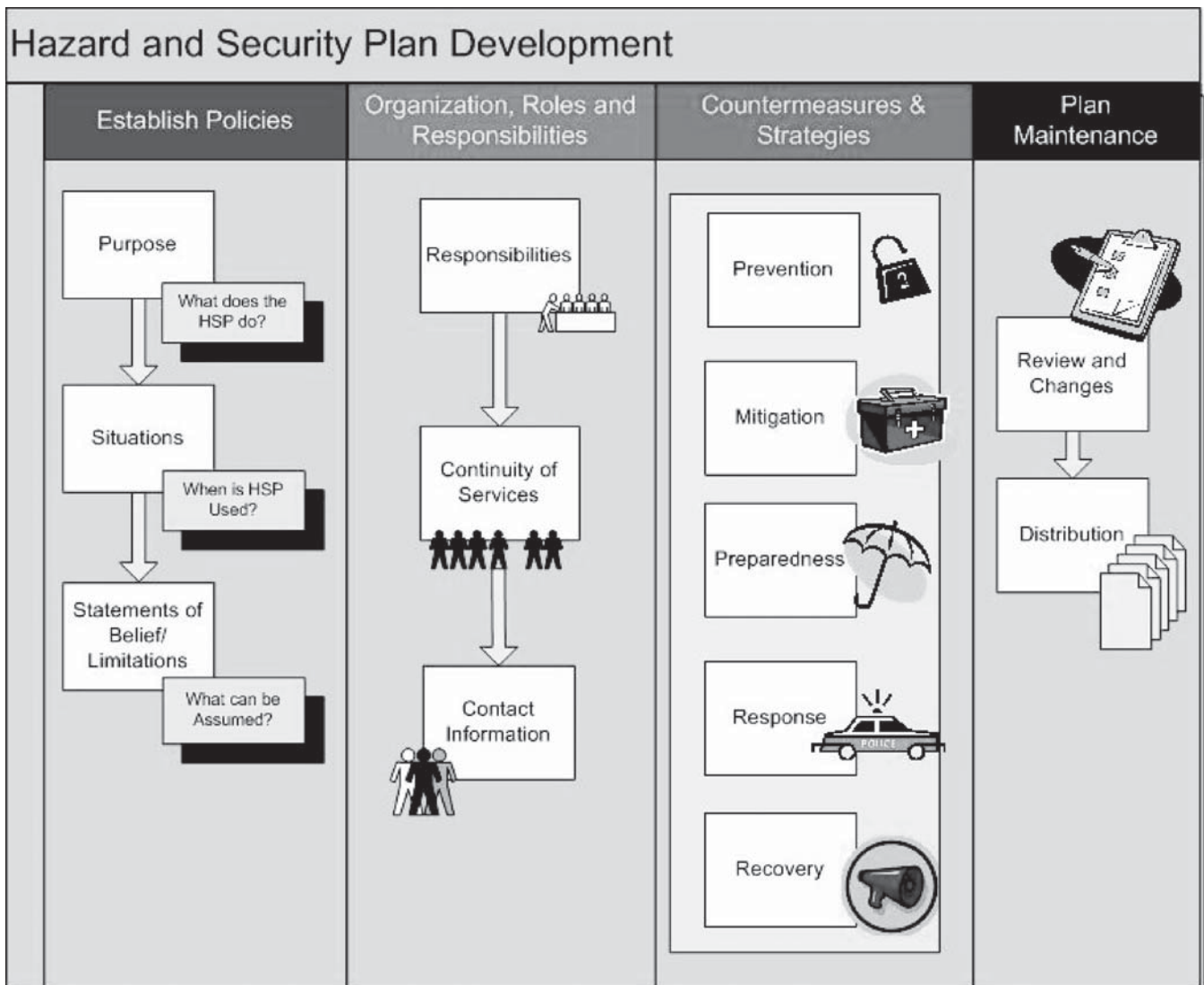
In developing an effective security plan it is necessary to establish what the essential plan elements are for the organization. *TCRP Report 86, Volume 10: Hazard and Security Plan Workshop* provides an excellent overview of the transportation security planning process. The document also presents a 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 four core planning development functions:

- Establishing priorities,
- Organizing roles and responsibilities,
- Selecting countermeasures and strategies, and
- Maintaining the plan.

### Establishing Priorities

As shown in Figure 2-1, plan development starts with identifying the purpose of the document. Although the plan should be flexible enough 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 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

- Create a written statement of purpose covering routine and emergency situations.
- Define the situations that the hazard and security plan 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.



Source: TCRP Report 86, Volume 10, Public Transportation Security Hazard and Security Plan Workshop, 2006

Figure 2-1. Hazard and security plan development.

## Organizing Roles and Responsibilities

In this phase of planning, key personnel and their security roles and responsibilities are determined. Incident-based priority security tasks should be listed and assigned to a specific individual known as the primary or principal. Secondary responsibility should be assigned to 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 objective of this phase of the security plan as development of 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 relocating essential departments
  - Developing procedures for deploying essential personnel, equipment, and supplies
  - Establishing procedures for backup and recovery of computer and paper records
- Contact information

## Selecting 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 five 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 follows:

- 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 effects of security-related incidents 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 agreements 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.

## Maintaining the Plan

Finally, the agency must ensure that security plans remain current and responsive to the dynamic changes that can occur in the transportation operating environment while creating a process that will support plan consistency with the future needs of the agency. Optimally, plans will be scalable and upgradable on a flexible timeline that has sufficient sensitivity to external security factors to allow for as-needed adjustments. The HSP recommends programmatic scheduled plan review periodically—at least every 6 months to a year. The document also provides guidelines on how this review should be conducted; suggested steps are as follows:

- 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. Such events include

- The addition of 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); and
- Changes with outside agencies, new suppliers, vendors, etc. (e.g., a new memorandum of understanding (MOU) signed with the local sheriff's department).

## Security Design Processes

A security system should be designed only after a risk assessment has been performed and a comprehensive security plan has been designed. Until these tasks have been completed, the data available will not be sufficient to permit 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 use measurable factors in reducing risk because of difficulties in establishing security-related metrics. Chapter 1 discussed risk insurance and the two types of risk cost-benefit analysis methods—quantitative and qualitative. Quantitative analysis is a numbers- or experience-based probability assessment that uses previously collected information to forecast the likelihood of a security event. The goal of quantitative security design is to decrease the ratio of unfavorable security events to total events through the analysis of data related to the known frequency of occurrence of a particular type of security incident. Once the probability aspects of a security incident have been defined, cost analysis is undertaken to rate the actual amount of loss against the costs of prospective security countermeasures available to reduce the risk associated with an occurrence. In contrast, qualitative analysis is based on characteristics, conditions, and events rather than numeric assessment. This form of analysis demands an in-depth knowledge of the organization

being assessed and an understanding of the operating environment in which work is performed. By default, qualitative analysis is the most widely used approach to risk analysis in the security industry. Some believe that qualitative analysis is sufficient and perhaps preferred to address the protection of lower value assets; however, in the most rigorous of applications, its use is by necessity because of an inherent inability to perform quantitative analysis. **Whenever feasible, a quantitative analysis based on the collection of objective data should be considered first in the performance of security risk analysis.** A typical qualitative assessment assigns relative values to assets based on factors such as criticality of loss and replacement costs. Threats against those assets are also given a relative value based on their probability of occurrence. **The result is a risk equation that computes risk as a function of impact and likelihood of occurrence.**

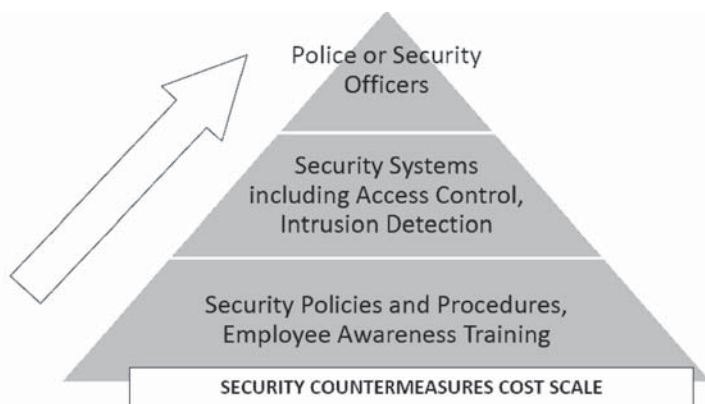
$$\text{RISK} = \text{IMPACT} \times \text{LIKELIHOOD}$$

Qualitative analysis depends on the capabilities of the analyst performing the assessment. Such analysis is more subjective because of the lack of historical information or metric data to support its assumptions. Fortunately, in most circumstances, precision can give way to the grouping of the outcomes of qualitative relative value ratings into categories such as high, medium, or low.

Although knowledge of an agency’s characteristics may be more important to qualitative analysis, irrespective of the type of assessment conducted, security strategy design requires transportation agencies to determine which security issues faced are most critical. Once identified, a strategy and timeline for reducing risks and vulnerabilities can be established. The goal of a security design strategy should be the logical and incremental “buy down” of security risk so as to provide acceptable levels of protection for transportation agency assets and operations on a continuing basis. Risk buy down should be focused on what is of priority to the organization to ensure maximized performance levels are maintained. Cost-effective security systems use a combination of countermeasures to meet security requirements. These normally include security staffing, training of employees, hardware (including electronic security systems), and security policies and procedures. Security design today demands that these component security resources be attained and then combined in a systematic way that can achieve security objectives while minimizing costs. System security should start with the basics consisting of those countermeasures that are most effective for the least amount of money, as outlined in Figure 2-2.

**Likelihood and Impact of Loss**

IMPACT	LIKELIHOOD		
	Low	Medium	High
High			Most Critical and Most Probable
Medium		↕↗	
Low	Least Critical and Least Probable		

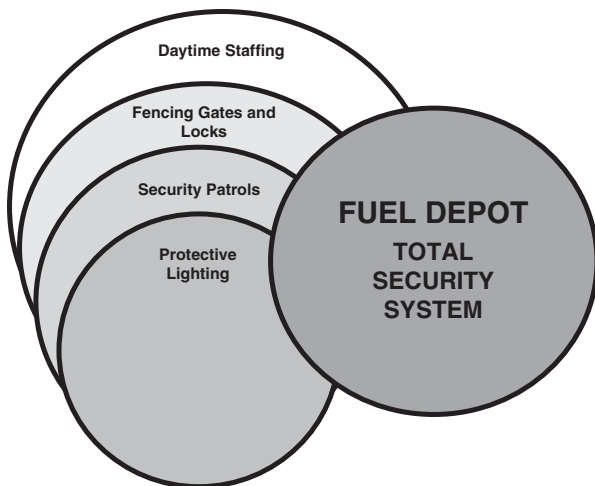


**Figure 2-2. Security countermeasures cost scale.**



Then, using assessment data obtained through analysis, the agency adds more costly system components until the level of security required to protect critical assets has been met. But developing a systems approach to security is more challenging than simply costing out security countermeasures into a hierarchy and applying them to an existing security vulnerability or situation. Transportation security issues are dynamic and evolving. Changing characteristics, conditions, and events require the synthesis of available resources in order to compensate for the weaknesses or loss of capabilities of one security countermeasure for the other. “**Layered security**” (also referred to as overlapping security) enables security design strategists to overcome uncertainty in security resource allocation and decisionmaking.

### Layered Security for a Fuel Depot



For example, the protection of a critical transportation asset such as a fuel depot may be accomplished first by establishing a procedure that employees must be present at the depot during all hours of operation without exception. During after hours, fencing, gates, lights, and locks would be used to secure the fuel facility. Finally security patrols would make periodic checks at the facility as an additional protective measure. If specific threats are received that the fuel depot is a target of attack, the configuration of security countermeasures can be adjusted to meet the new security requirements. Assuming the facility remains open, additional staff could be assigned to be present at all times. Gates could be locked during hours of operation and identification checked for all persons seeking to enter the depot. Security forces could be permanently assigned to remain on the grounds. In this simplified scenario, increased vigilance is made possible by the layers of overlapping security capabilities that already exist. However, the redeployment of personnel to increase the security at the fuel depot degrades security countermeasures available to

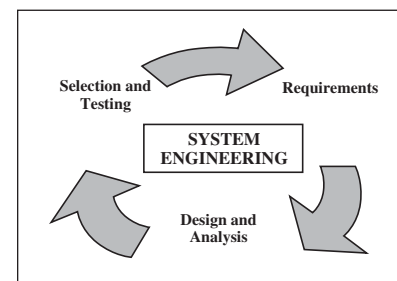
protect the agency’s other assets. Sizing the scope of this potential loss of security resource during critical periods becomes an important part of the agency’s security design strategy.

Overlapping security does not end with the layering of security countermeasures alone. As pointed out in *Making the Nation Safer*, “transportation security can best be achieved through well-designed security systems that are integrated with transportation operations.” (pg. 214) The text goes on to describe security methods and techniques that are “dual use, adaptable and opportunistic” (pg. 220) as optimal in the diverse and dynamic transportation sector. A “system” can be defined as “an integrated collection of components or elements designed to achieve an objective according to a plan.” (*Design and Evaluation of Physical Protection Systems*, April 2001, Mary Lynne Garcia) Systems can be small or large, complex or relatively simple. Complex systems usually are composed of smaller subsystems designed to work together. In the transportation sector, security systems integration can include the convergence of classic functions (e.g., safety, crime prevention, fire prevention, communications, and facility management) with functions unique to the industry (e.g., fleet management, package and cargo tracking and control, or dispatching operations). When considering the opportunities for integrating security with other transportation functions, it is important to recognize that the synergies that can be achieved are two-directional. Security-related technologies and procedures can be integrated with existing or newly created systems to produce non-security benefits and non-security systems or subsystems can be applied more broadly to reducing security risks and vulnerabilities. Central to this concept of security systems integration is recognition that, prior to making new investments, existing systems and functions should be surveyed in order to explore opportunities for expanded use. For example, rather than deploying costly new surveillance systems, cameras, and monitoring stations, a bridge operator whose function is to safely raise or lower a bridge over navigable waters may be given new security inspection requirements to periodically check

for signs of forced entry to bridge access points. Depending on the criticality of the bridge in terms of transportation operations, this approach may be optimal.

The design of an integrated security system is properly performed through a structured methodology known as **system engineering**. Security-related system engineering is defined as the protection of physical infrastructure components and logical structures and processes from threats and vulnerabilities. (Garcia, 2001) The process begins with definition of requirements, continues through to design and analysis of multiple potential solutions, and ends with selection and testing of the best design to meet requirements and goals and then begins again.

## System Engineering



## Security Funding

The familiar axiom “If you fail to plan, then plan to fail” applies to transportation security. The FTA’s SSEPP states the issue even more succinctly: “Plan first, then spend.” Security is highly sensitive to adverse consequences and prone to reactionary influences that may or may not result in an appropriate response to an incident. Crisis response to a security incident or series of security incidents demands that we exercise good judgment and sound policy so that we don’t spend money carelessly or ineffectively. Security practitioners and risk management professionals recognize that it can be difficult to establish the value of a specific security countermeasure or activity. This difficulty is compounded when measures are grouped together or security is layered in a protective system. But quantifying the operating costs, savings, and/or revenues that will result from project implementation and incorporating those results into financial planning will ensure that security funding is considered on balance with other agency funding priorities. Security programs should be well thought out and sustainable over a predetermined term. The objectives and integration of security with other operating disciplines and management processes should be conducive to the overall goals of the transportation agency.

Optimally, overlapping security funding cycles should be considered. At minimum the agency should conduct security planning on a 1-year basis for both operating and capital and on a 5-year basis for capital improvements. (Some transportation organizations may use as much as a 1-year, 3-year, 5-year, and 10-year capital investment planning strategy). Accomplishing both short- and longer term planning will provide continuity and a structured methodology for balancing the cost and effectiveness of security measures against the capabilities of the transportation organization to fund security improvements. In relation to security, most costs associated with short-term operating funding cycles are labor related. For a transportation agency that maintains its own police or security force, these operating costs can run as high as 90 to 92% of budget allocation. But determining the correct number of police and security employees is highly contingent on the threats and vulnerabilities of the agency balanced against the mix of security measures that have been deployed to reduce security risk. In particular, the transportation agency must weigh the costs of security personnel against the prospective use of other less-costly security countermeasures, such as improved policies and procedures, employee security awareness training, or security systems, including locks, access control, or intrusion detection systems.

Just like an operating budget, and in conjunction with operating budget development, planning and management of the capital improvement plan should occur in a regular, annual cycle. It is here that often security funding meets its most significant challenges in the allocation of available resources. When possible, security expenditure recommendations at this stage in the funding cycle should contribute to the overall efficiency of the transportation agency in the performance of its core mission, goals, and objectives. Although not always the case, certain

security measures such as increased lighting, improved communications, passenger flow gating, or simply directional signs can serve the dual purpose of adding to the effectiveness of service delivery.

Five-year capital planning is the point in the funding cycle where an agency can take best advantage of the development of a security plan. Longer term security improvements that seek to reduce the vulnerabilities of an agency's transportation critical infrastructure can be designed as components of larger systems and subsystems that are central to the strategic future of the organization. For example, an out-year strategy to replace the soon-to-be-antiquated or inefficient traffic control center of an agency can be augmented by the addition of security improving closed-circuit television (CCTV) technology that permits traffic controllers to observe the operating conditions at train stations or along bus routes. Similarly, a decision by management to invest in Automatic Vehicle Locator (AVL) technology for rolling stock can serve the important security and emergency response benefit of identifying the exact location of a vehicle in distress on the system. Thinking about security improvements in this way also facilitates the cost-effective designing-in of security measures at the outset of capital projects, instead of spending significantly more money to retrofit security into existing infrastructure. Security systems in and of themselves also require multi-year planning to ensure their effectiveness and continued usefulness. The replacement or upgrading of security system components should be contemplated as a continuous process that is capable of meeting the stated physical protection system requirements of the organization and flexible enough to respond to the changing security threats and vulnerabilities that occur over time.

# Physical Security Countermeasures

Consistent with effective security planning is the need to deploy appropriate risk reduction methods to minimize or eliminate identified vulnerabilities or mitigating consequences. Chapter 3 discusses many of the tools and countermeasures that should be considered in the implementation phase of planning as a means to improve the security of critical infrastructure and facilities, information systems, and other areas. Physical security countermeasures include signs; emergency telephones, duress alarms, and assistance stations; key controls and locks; protective barriers; protective lighting; alarm and intrusion detection systems; electronic access control systems; and surveillance systems and monitoring.

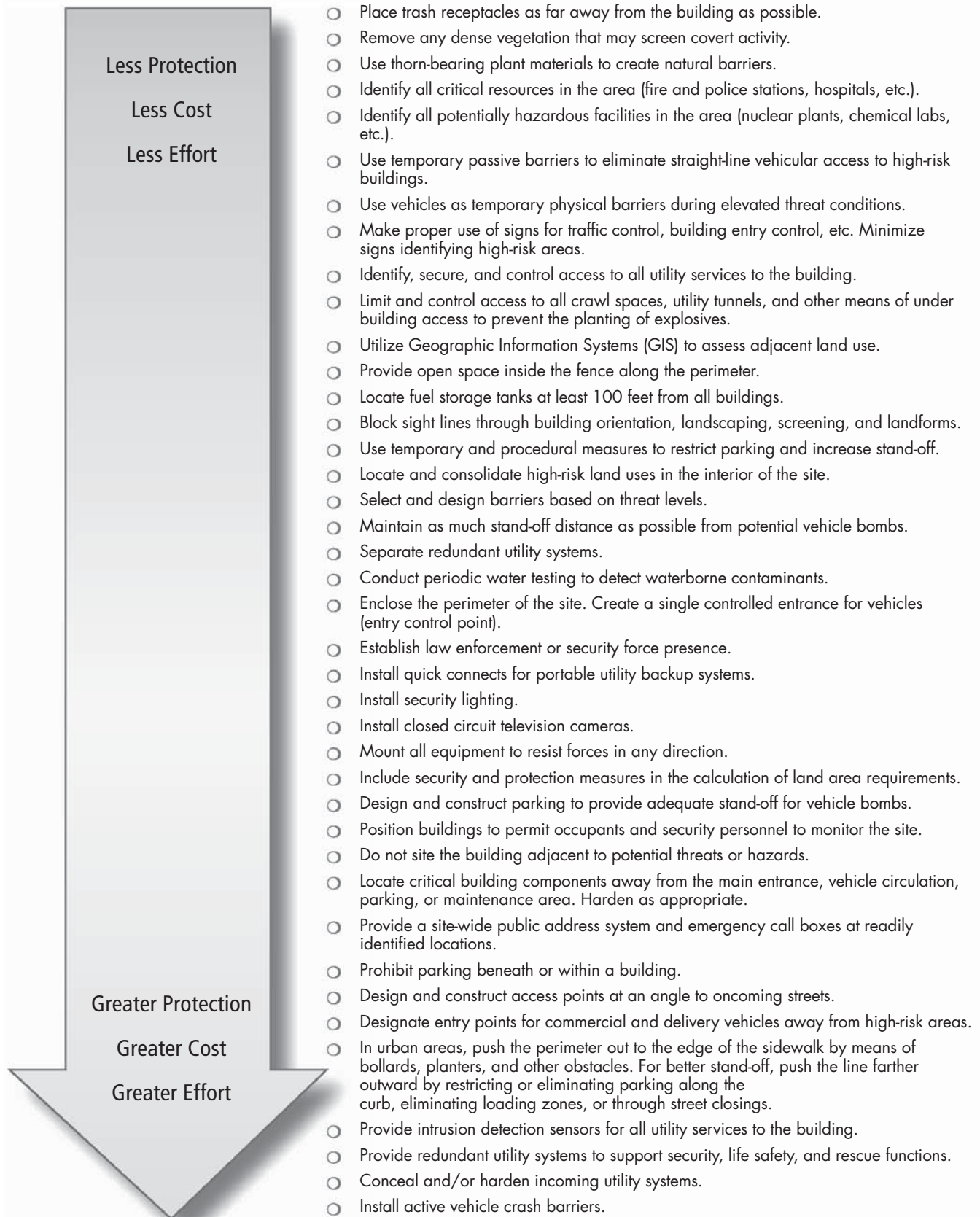
What countermeasures to use in any given situation depends on what will be most useful, that is the utility of the countermeasure. Transportation agencies must examine the threats against the organization and identify the most useful means to reduce the vulnerabilities associated with those threats to acceptable levels. Utility is not solely a measure of cost. Often less costly, but more effective solutions are available that the agency can select to meet security requirements. In making these choices, security designers can benefit from the use of a utility scale that assimilates and compares one countermeasure against the other. For example, Figure 3-1 shows security countermeasures along a sliding scale based on three utility factors—protection provided, cost, and effort required. Countermeasures appear on the scale moving from “Less Protection, Less Cost and Less Effort to Greater Protection, Greater Cost, and Greater Effort.” The figure does not provide relative comparisons of the three utility factors, but does provide them for each of the factors individually.

Once the utility of specific countermeasures has been evaluated, the agency should return to the concepts of systems approach, layered security, and systems integration (as discussed in Chapter 2 and illustrated in Figure 3-2) when deciding how to proceed in reducing security vulnerabilities. Certain security design techniques or technologies are well suited to serve as “solution sets,” capable of fulfilling security needs.

## Signs

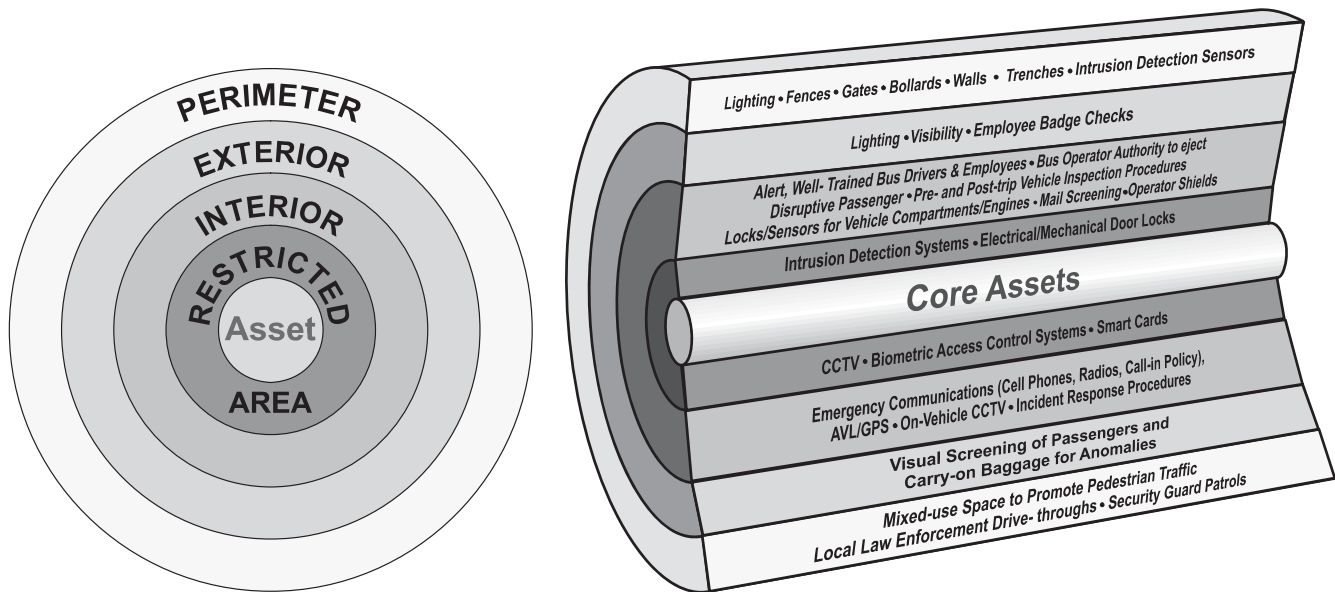
A rule of warfare that applies to homeland defense is that neither fences nor signs will deter or stop a determined enemy. However, security signs can play a very important role in the securing of transportation facilities, rights-of-way, and critical infrastructure. Security signs are relatively inexpensive and low maintenance and can help deter aggressor actions or tactics.

Maintenance of a good security sign program also helps to create a working environment in which security is perceived to be taken seriously. Employees become aware of security requirements through well-placed signs that display the status of restricted or controlled areas or signs that limit or prohibit certain activities. The signs depicted in Figure 3-3 are approved by OSHA for use in the workplace. They represent a cross-section of security designs that cover both of these categories.



Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-1. Countermeasures scale by protection, cost, effect.**



Source: FTA Security Design Considerations, 2004

Figure 3-2. Layers of security.



Source: <http://www.safetysign.com>

Figure 3-3. Security signs.

Effective use of signs starts with creation of a sign plan. This written record provides a framework for decisionmaking about the installation, replacement, maintenance, and budgeting for the program. The sign plan identifies each sign by type and legend and contains a site plan for placement and installation.

In 2006, the U.S. Army Corps of Engineers updated its Sign Standards Manual EP 310-1-6a and EP 310-1-6b. The manual's Checklist of Sign Plan Elements shows the steps necessary to implement an effective sign plan. The checklist includes

- Inventory existing signs and their condition;
- Collect or develop up-to-date pictorials, maps (optimally supported by GIS), diagrams, blueprints, or other representation of the area in need of protecting;
- Prepare the site plan and sign layout materials; and
- Implement the plan in conformance with established guidelines.

Once the implementation plan has been accomplished, a sign inspection and maintenance schedule should be developed. A budgeted coordinated sign replacement and maintenance schedule is necessary to reinforce the message to transportation system users, employees, and the public that the agency prioritizes security on its properties and facilities. Missing signs defeat the objectives of the security plan layout while damaged or vandalized security signs reflect badly on the agency's commitment to security. The Corps of Engineers recommends a formal inspection of security signs semi-annually. The inspection should identify signs requiring maintenance or replacement, signs that can be eliminated, and the need for additional signs. Vandalized, damaged, or missing signs should be repaired or replaced as quickly as possible.

## **Emergency Telephones, Duress Alarms, and Assistance Stations**

Historically, emergency alert or alarm systems have been hardwired communications systems linked to security control centers. Telephone boxes, panic alarm buttons, and intercom systems typically were linked to central stations where dispatchers or monitoring personnel answered emergency calls and sent response personnel to the location to help.

Today, wireless technology has added new dimensions and capabilities for the security-related use of these systems. For example, The State Transit Authority of Australia has a fleet of 1,800 buses in the Sydney and Newcastle area. Every bus is outfitted with Automatic Vehicle Locator (AVL) technology, a "Driver Duress Alarm," and a microphone that allows Authority central station personnel to hear what is happening on the vehicle when the driver activates the system.

Technology has also expanded the recipient group for duress alarms to include first responders themselves who can be equipped to receive a location-specific pre-recorded voice message using the officer's existing two-way radios. These systems by eliminating the monitoring station go-between can greatly improve the response time for police or security personnel in the event of a security incident. Information can be sent close to simultaneously to the command center by digital data packet transmittal.

Because of the high costs that can be associated with responding to duress alarms, transportation agencies should consider using emergency alert alarm systems to conduct a thorough risk assessment to correctly establish the size and scope of the project. Once the needs assessment has been completed, the best way to accomplish the countermeasures analysis is to engineer backwards from the response. Taking into account variables (e.g., time, distance, day of the week, and changes in staffing levels), police or security officer response capabilities, whether self-directed or through dispatch, should be examined to determine just how quickly help can arrive on the scene.

Next, prospective communications access points for deployment of emergency alert or alarm systems should be compared with estimated response capabilities, keeping in mind the potential time variation and, where applicable, the routes and locations of agency rolling stock. If additional security assets are required to make the system viable, they should be designed and planned for prior to implementation. A duress alarm or emergency communication system that often goes unanswered for an extended or unreasonable length of time creates an untenable security operating condition and should be avoided. Under such circumstances, alternative security countermeasures should be selected.

## Key Control and Locks

It has been said that security starts and ends with closing the door and locking it. But the most expensive and well-built locking mechanism can be defeated if sufficient skill and enough time are available to the adversary or aggressor. According to the *US Army Field Manual 19-30, Chapter 8*, most key locks and conventional combination locks can be picked by an expert in a matter of minutes. More sophisticated manipulation-resistant locks, locks with four or more tumblers, some interchangeable core systems, or relocking devices on safes or doors can provide an appreciable increase in difficulty, but are still subject to compromise.

Locks should be considered at best to be a deterrent and more plausibly as a delay device that does not completely restrict entry to a protected area. Locks are a widely used basic security countermeasure for protecting facilities, activities, personnel, and property. They are present not only on doors, but on windows, gates, conveyances, interior offices, supply areas, filing cabinets, and virtually all kinds of other storage containers or areas as well.

Locking hardware is designed to various levels of deterrence or entry delay. Performance standards for locks based on these capabilities exist through ANSI/BHMAA Series 156 and United Laboratories (UL) 1034, 437, 768,294, 2058 and 305. It is recommended that the agency consult with a professional locksmith for mechanical locks or security professional for electromechanical or electromagnetic locks before spending security funding on new hardware or upgrades.

Because keys and locks frequently are the only countermeasure used to protect assets and infrastructure, managing key access is fundamental to effective control. Maintaining a good key control system can mean the difference between having a robust security program and a compromised unsecure operating environment. The starting point for establishing an effective key control program is to develop a sound workable policy. The policy must be requirements-based and commensurate with the necessary levels of protection appropriate for the location or setting. Obtaining user input into the design of the key control system can help later when maintaining discipline associated with the system is important.

Management of the system should be assigned to an individual designated as the Key Control Officer (KCO). This individual should ensure the integrity of the key control process by

- Exercising approval authority over the acquisition and storage of all locks and keys,
- Overseeing the distribution of keys to agency employees,
- Conducting inspections and inventories,
- Maintaining the organization's key depository,
- Investigating key loss, and
- Establishing an official records maintenance system that serves as the control point for all agency key and lock activity.

Frequently, an organization will face a situation in which key control has been compromised, either through a lack of attention to security or by the failure of one or more employees to comply with policy. When current conditions demand the system and process be revised, the agency



should create a key control annex to their physical security plan. The newly assigned KCO should conduct a comprehensive survey of all agency physical assets needing protection to establish a baseline key control plan that can return efficiency to the program. Under this program, when a compromised key access point is identified, locks should be replaced, recoded, or otherwise upgraded as a security plan priority.

## Protective Barriers

Protective barriers include fencing, other types of barriers, and landscape design. Each of these three categories will be discussed.

### Fencing

The two main issues with the use of fencing as a protective barrier are

- Placement and
- The grade or strength of fencing material.

Substituting other types of protective barriers where fencing traditionally has been used should be considered. The transportation agency should look at the design aspects of both placement and strength of material in concert to determine how the use of fencing countermeasures can reduce risk.

#### *Placement*

The chief use of fencing for security is as a deterrent or delaying factor. When fencing is used this way, terms such as **perimeter line** and **controlled access zone** apply. The perimeter line is the outermost line of defense for an area being protected. A controlled access zone attempts to limit access to the more immediate area being protected.

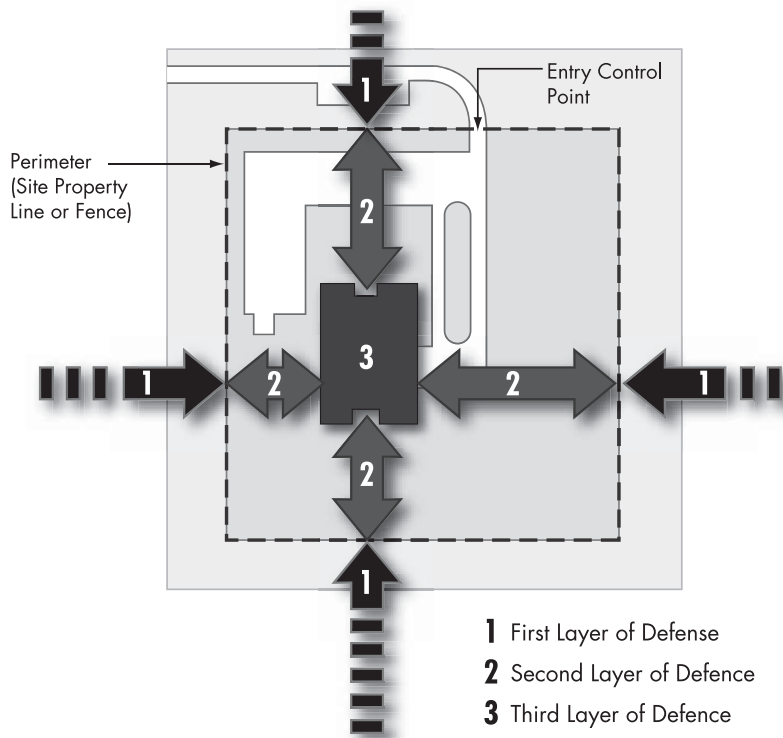
The uses of fencing in these configurations are clear. For example, a fence can be used to form the outermost perimeter line. Fencing (or more generally protective barriers) used in conjunction with layered defense principles offers a much broader range of security applications. *FEMA 430, Site and Urban Design for Security* presents a three-layer model for protecting a building against attack. Under this approach, the objective is to “create a defense in depth by creating cumulative successive obstacles that must be penetrated . . . penetration of the perimeter leads only to further defense systems that must be overcome.”

Figure 3-4 illustrates the use of fencing as a security countermeasure in conjunction with the first and second defensive layers. In this configuration, the greater the distance between the building exterior and the perimeter line, the better. This “open space” concept of security permits designers to use an array of different security countermeasures to defend the organization’s assets, including line of sight observation, video surveillance, motion detection, and other intrusion detection technologies.

#### *Material*

Security planners can use fencing to prevent as well as deter. Depending on the deployment and K Certification class of fencing material, certain aggressor tactics can be completely defeated.

Primarily, threats that can be prevented relate to explosives mitigation and involve barrier-related interception of the threat at a point that creates sufficient stand-off distance to absorb dangerous explosive blast levels. K Certification anti-ram standards originated at the Department of State. The rating is determined from perpendicular barrier impact results of a truck weighing 15,000 lb (6810 kg) striking the barrier straight on. To meet the standard, the truck’s cargo bed cannot penetrate the barrier by more than 1 meter. Figure 3-5 provides additional

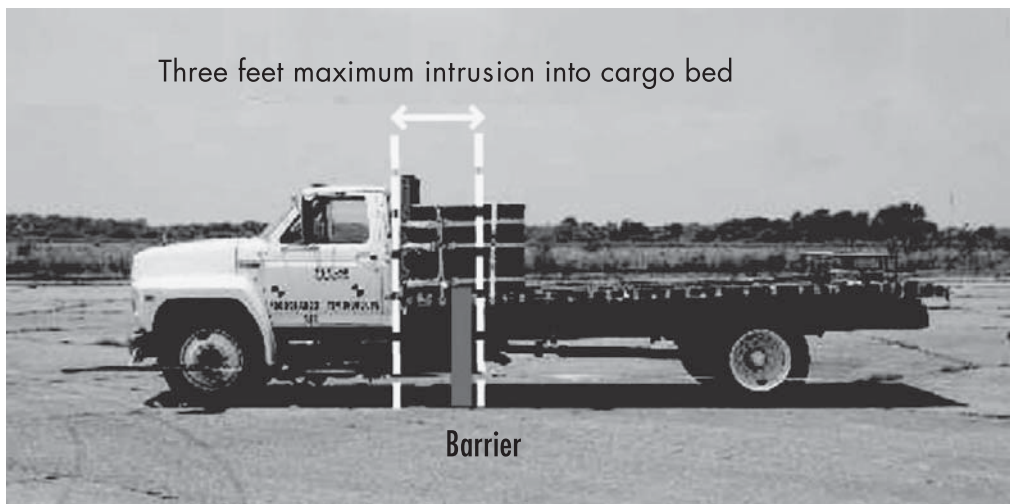


Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-4.** Use of fencing as a security countermeasure with defensive layers.

Certification Class	Speed (mph)	Speed (kph)
K12	50	80
K8	40	65
K4	30	48

(a)



(b)

**Figure 3-5.** Vehicle and crash ratings (a) and truck striking barrier (b).



Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-6. Crash-rated fence.**

information about the vehicle and crash ratings associated with the truck striking the barriers at speeds of 30, 40, and 50 mph. Figure 3-6 shows a crash-rated fence that, according to the manufacturer, can be reinforced with an integrated cable system to meet K8 standards. Figure 3-7 shows a cable barrier that can be used for fencing reinforcement.

### Protective Barriers

Fences are one type of protective barrier available to security designers. Other types of barriers include anti-ram vehicle barriers categorized as either passive or active. Anti-ram barrier effectiveness is based on a formula:

$$KE = \frac{Mv^2}{2}$$

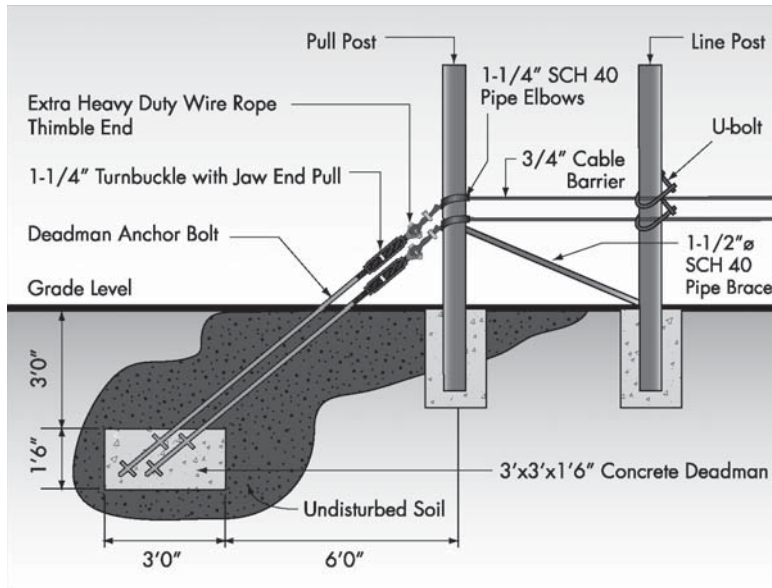
Source: FEMA 426, *Building Design for Homeland Security*, 2004

Where  $M$  is the mass of the vehicle and  $v$  is the velocity at the time of impact. Passive barriers are fixed countermeasures and include bollards (concrete-filled steel pipe), reinforced street furniture, concrete walls, planters, and berms (see Figure 3-8).

Active barriers are movable or retractable in some way so as to allow passage when needed. Such barriers can include retractable bollards, crash beams, rotating wedge systems, or rising barricades as shown in Figures 3-9 through 3-11.

### Landscape Design

Natural barriers, such as trees or water, can be used to reduce vulnerabilities. In addition, actual site planning for protected areas can be security minded with landscape design serving the dual purposes of aesthetics and function (see Figure 3-12).



Source: DOD Handbook: Selection and Application of Vehicle Barriers, MIL\_HDBK: 1013/14, 1999

**Figure 3-7. Cable barrier deployable as a means for fencing reinforcement.**

## Protective Lighting

Security professionals, emergency response personnel, and safety practitioners extol the value of manufactured light to protect people and property from harm or unreasonable risk of injury. **Used as a security countermeasure during hours of darkness, protective lighting can create an operating environment that provides better security than in the daytime.** This can occur when

Top: Combination of low retaining walls and low bollards.  
Bottom, left: Combination of oversize bollard and large planters placed on very wide sidewalk.  
Bottom, right: Combination of tree and bollards.



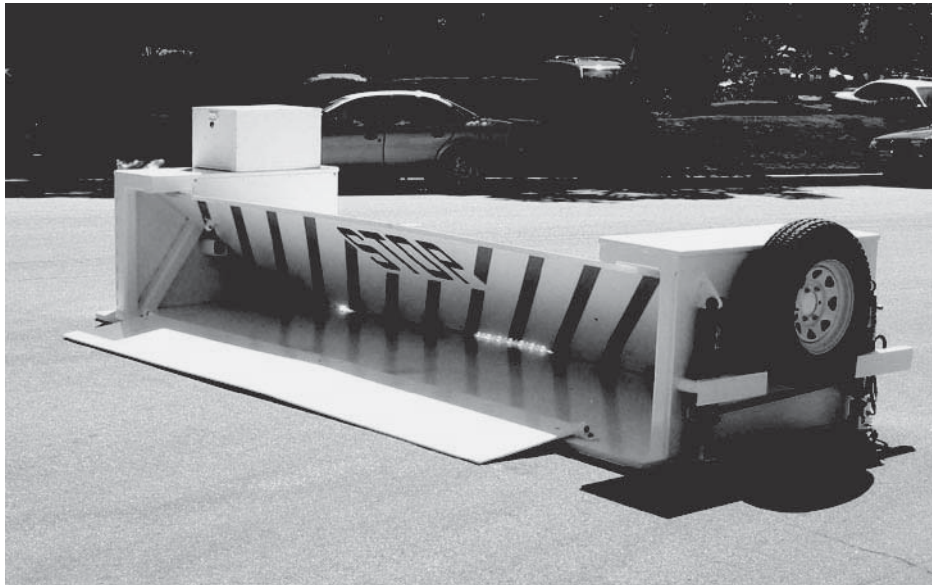
Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-8. Barriers as countermeasures.**



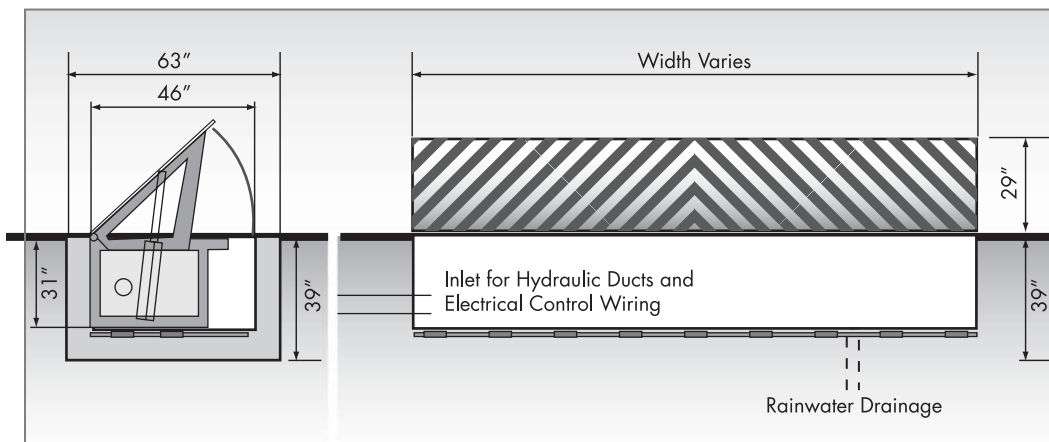
Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-9. Examples of retractable bollards and crash beams.**



Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-10. Mobile wedge barrier.**



Source: FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

**Figure 3-11. Rising barricade.**

This proposal for the re-design of the Washington Monument grounds uses water to create a barrier. The meandering canal is beautiful as well as functional.



Source: Michael Van Vandenburgh and Associates

**Figure 3-12.** *Proposal for the re-design of the Washington Monument grounds.*

security designers use capabilities such as glare projection to reduce the ability of an adversary to see inside a protected area. Protective lighting objectives include the following:

- Adherence to acceptable industry standards for outdoor protective lighting levels as promulgated by the Illuminated Engineering Society of North America (IESNA) or the guidelines of the New Buildings Institute's *Advanced Lighting Guidelines*, 2003 Edition;
- Illumination of all exterior points within the perimeter of the protected area, including walkways, vehicle entranceways, fence lines, and critical structures or assets;
- Non-transgressing illumination of approach areas to the perimeter line;
- Deterrence of aggressor attempts at entry to protected areas;
- Support for other security countermeasures (e.g., video surveillance cameras, motion-activated sensors, or security forces); and
- Resistance to tampering, vandalism, neutralization, or defeat.

As with other measures, protective lighting security planning requires thoughtful and careful study to make the most of the benefits of the program. In particular, because of the open access of the environment, prospective dual-use aspects of lighting should be examined for potential integration into mainstream transportation operations. Similarly, the security applicability of agency lighting configurations should be factored into operational planning and decisionmaking.

Planners should also determine the upgrade prospects of the existing lighting system. Taking advantage of opportunities to retrofit existing lighting systems (luminaries) can improve lighting quality, reduce electricity use, and extend time between required maintenance and replacement, while providing benefits such as improved security or safety.

In this regard, although relatively inexpensive when compared with other security strategies, lighting plans also require a strong continuing commitment to maintenance and upkeep.

**Table 3-1. Lamp types.**

Type	Life (in hrs)	Efficiency*	Advantages**	Disadvantages**
Incandescent	500 – 4000	17 – 22	Inexpensive	Relatively short life
Fluorescent	9,000 – 17,000	67 – 100	Longer life than incandescent and metal halide	Shorter life than mercury vapor and HPS
HID Mercury Vapor Metal Halide HPS	24,000+ 6,000 24,000	31 – 63 80 – 115 80 – 140	Longest life. Good efficiency More efficient than mercury vapor Long life and excellent efficiency	May not be optimal in conditions where full illumination is required immediately on activation. Depending on the type of lamp—mercury vapor, metal halide, or high-pressure sodium (HPS), the time required for HID lamps to reach full light output can range from 3 to 7 minutes. Re-strike times (cooling time required before the lamp will re-start) can be even longer— ranging from 3 to 15 minutes.

\*in lumens per watt

\*\* compared with other lamps

(Source: Adapted from *NFPA 730 Guide for Premises Security*, 2006)

Agencies must budget for scheduled cleaning and replacement of luminaries. Different types of lighting systems can reduce the overall costs associated with upkeep while improving the efficiency of the lighting output, measured luminance (footcandles or lux).

### Lamps

Three principal sources of light are in common use:

- Incandescent lamps,
- Fluorescent lamps and,
- High-intensity discharge (HID) lamps.

All three types convert electrical energy to light or radiant energy. Table 3-1 compares the three types of lamp categories.

### Luminaries

Luminaries (consisting of a complete lighting unit, lamp, housing, and power supply connectivity) are categorized as follows:

- Floodlights,
- Streetlights,
- Fresnel lenses, and
- Searchlights.

Table 3-2 provides a comparison of these categories.

## Alarm and Intrusion Detection Systems

Alarms can detect various types of incidents (e.g., intrusion, smoke or fire, temperature change, gas, or water flow rates), as well as other emergency conditions. Their basic physical security application, however, relates principally to intrusion detection. The functionality also applies to chemical, biological, and radiological sensors, although they are more complex depending on the technology associated with the types of sensors.

Intrusion detection alarm systems are an important countermeasure in the security planning toolkit. Their main purpose is to work as a force multiplier to allow for more efficient use of staffing by reducing the number of security personnel required to patrol or monitor a protected area. Assuming that a response force is nearby, alarm systems can eliminate the need for a dedicated security patrol force.

**Table 3-2. Comparison of lights.**

Type	Purposes	Description	Lamps Used
Floodlight	To project to distant points To illuminate perimeter fence lines, critical facilities, and high-priority assets	Designed with a focused beam width that can be projected to distant points, thereby illuminating a specified area or location. Use in homeland defense is vital. Used to illuminate perimeter fence lines, boundaries, critical facilities, and high-priority assets.	Incandescent HID
Streetlight	To illuminate large areas and entranceways.	Used to illuminate large areas. Their light distribution patterns can be either symmetrical or asymmetrical. Symmetrical street light luminaries are placed in locations that will cascade light throughout the area to be covered. Asymmetrical street lights direct light by reflection or refraction into the area to be lighted. Mercury vapor lamps are widely used in street lighting because of their long life.	Mercury vapor
Fresnel lens	To protect high-security locations where transgressing light will not affect the neighboring community	Directional high-glare units that project a fan-shaped light beam approximately 180 degrees in the horizontal and 15 to 30 degrees in the vertical	Incandescent HID
Searchlight	To augment fixed lighting at a given location	Provides a powerful concentrated beam. Ranges from 12 to 24 inches in diameter of reflection and from 250 to 3,000 watts. Often portable	Incandescent

Alarm systems can be used

- In place of other security countermeasures that are not viable because of safety concerns or operational requirements or
- As a supplemental security measure.

The main elements of an intrusion detection alarm system are the sensors, the alarm processor, the monitoring system, and the communications architecture that connects these elements. The components of an alarm system include the following:

- Main Control Unit,
- Keypad,
- Input Devices (Sensors),
- Transformer,
- Power Supply,
- Telecommunications, and
- Output Devices.

An alarm system can be hard wired (the system uses wires to connect all input and output devices to the main control unit) or wireless (the system uses radio waves or RF to transmit intrusion alarms). Some systems, known as hybrids, use a combination of both hard-wired and wireless signal carrying methods to communicate intrusion or status.

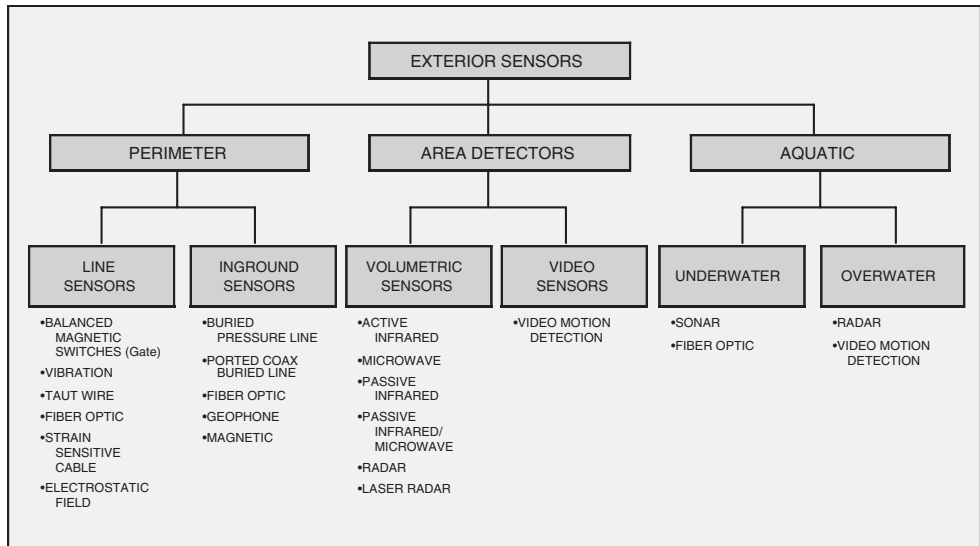
The physical security deployment of intrusion detection systems usually occurs with other security countermeasures such as natural and manmade barriers, access control systems, and other sensor technologies. For an intrusion detection alarm system to be effective, there must be both an active or passive monitoring capability and a security or law enforcement personnel response team capacity.

Sensors are the input devices for intrusion detection systems. Intrusion sensors can be either interior or exterior as illustrated by Figures 3-13 and 3-14.

Interior sensors detect intruders

- Approaching or penetrating a secured boundary (e.g., a door, wall, roof, floor, vent, or window);
- Moving within a secured area (e.g., a room or hallway); and
- Moving, lifting, or touching a particular object.



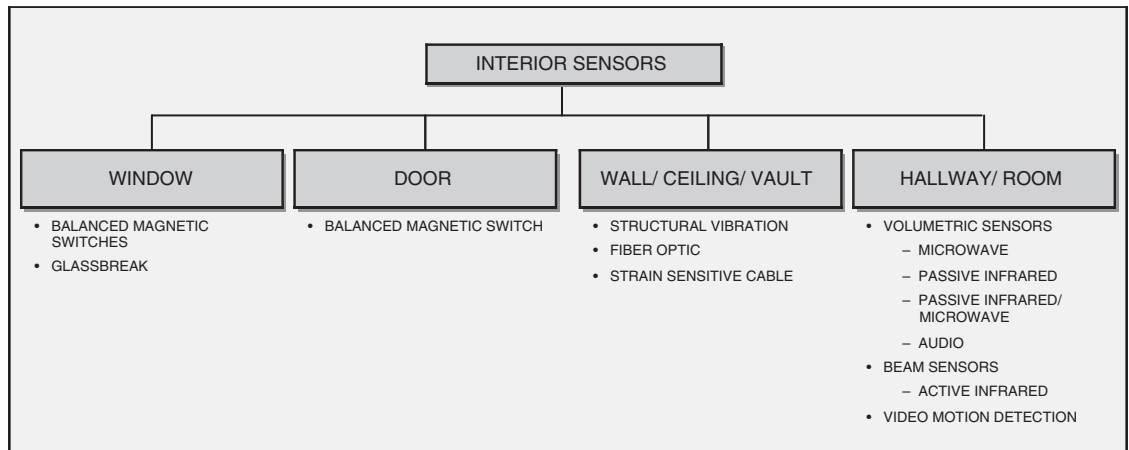


Source: SAVER Summary; Handbook of Intrusion Detection Sensors, 2004 <http://www.dhs-saver.info>

**Figure 3-13. Exterior intrusion sensors—applications index.**

Exterior sensors detect intruders crossing a perimeter or boundary or entering a protected zone. Although many interior sensors should not be exposed to weather, exterior sensors must be able to withstand outdoor weather conditions. Exterior sensors have a higher nuisance alarm rate than their interior counterparts and a lower probability of detection, primarily because of uncontrollable environmental factors.

Many different types of sensors are used in intrusion detection alarm systems. These sensors detect through sound, vibration, motion, and electrostatic and/or light beams. Determining which sensors to deploy in response to security vulnerability depends on both operational considerations (e.g., the facility’s hours of operation; the presence of system users, staff, or other personnel; the value of material, equipment, or other critical assets; and the response time of security forces) and technological limitations (e.g., concerns about radio and electrical interference, sound levels, weather and climate, and other environmental factors). Ideally, the agency should seek professional security assistance in planning for intrusion detection alarm systems.



Source: SAVER Summary; Handbook of Intrusion Detection Sensors, 2004 <http://www.dhs-saver.info>

**Figure 3-14. Interior intrusion sensors—applications index.**

## Electronic Access Control Systems

Access control systems limit or restrict the access of personnel or vehicles either into or out of a controlled zone or area. The technology used can be basic or complicated, depending on the needs and requirements of the resource or area to be protected. Systems can stand alone to control access to a single entry point or be multi-portal, computer-based, and capable of controlling access to hundreds of doors and managing thousands of identification credentials.

Before implementing an access control system, the agency should have a well-defined understanding of the threats and vulnerabilities to be addressed. In addition, sensitivity to the following factors is important:

- The nature and tempo of activity in and around the protected area;
- The size of the authorized population;
- Variation in degrees of accessibility in terms of access levels and time;
- The physical characteristics of the area being protected;
- Limitations or restrictions caused by the operating environment;
- Climate and weather conditions affecting system operations;
- Staffing, training, and support levels available for operating and maintaining the system; and
- The availability of security forces to respond to a report of an unauthorized entry.

Protecting transportation agency operations and assets can be a difficult proposition. Because of the open and ubiquitous operating environment, it is not always possible to control people's movements. Inappropriate screening of system users may create an untenable level of inconvenience that results in the loss of customers. Similarly, an agency whose employees are confronted with unnecessary, time-consuming access control regimens will, at best, suffer a loss of productivity through queuing or, at worst, have the system itself compromised by activities such as door propping. Access control performance must correspond to the needs of the organization by being responsive to throughput requirements, defined as "the measure of the number of authorized persons or vehicles that can process through an ingress or egress point within a period of time." (SAVER Summary; *Handbook of Intrusion Detection Sensors*, 2004 <http://www.dhs-saver.info>)

The accurate identification of controlled or restricted areas through a rigorous determination of what locations, assets, or resources need protection is essential to achieving acceptable throughput. The difference between the two is based on the necessity of access. Controlled area access should be limited to persons who have official business within the area. Restricted area admittance should be limited to personnel assigned to work in the particular area or other personnel who have been expressly cleared and authorized.

Other individuals entering restricted areas should be accompanied at all times by an authorized individual. The following criteria can assist in defining agency-controlled areas or restricted areas:

- Operating areas critical to continued operation or provision of services,
- Locations where uncontrolled access would interfere or disrupt personnel in the performance of their duties,
- Storage areas that contain valuable equipment or materials,
- Locations where operations can result in the existence of hazardous or unsafe conditions,
- Office areas where sensitive or confidential information is located, and
- Command and control areas that house critical functions.

The main elements of an access control system are

- Barriers,
- Verification or identification equipment,
- Panels, and
- The communications structure that connects these elements.



Source: SAVER Summary; *Handbook of Intrusion Detection Sensors*, 2004 <http://www.dhs-saver.info>

**Figure 3-15. Cipher access control barrier.**

The system must also be able to communicate either directly or indirectly through human interface with response security forces.

Access control barriers are identification-based, requiring the person or vehicle requesting access to possess some form of information or technology that can be read by the system. Electronic systems are computer-controlled with access determinations made through the query of an authorized user database.

Figure 3-15 shows a **cipher** access control barrier widely used in areas that require frequent entry by authorized users. The cipher lock controls access using information the individual knows (a combination).

Figure 3-16 shows a **token-based drop arm barrier system** used to supplement security personnel at the vehicle entranceway to a controlled area. The vehicle contains some form of a readable proximity sticker, such as a bar code or other device, that automatically lifts the drop arm barrier once the authorized user database has been interrogated.



Source: SAVER Summary; *Handbook of Intrusion Detection Sensors*, 2004 <http://www.dhs-saver.info>

**Figure 3-16. Token-based drop arm barrier system.**

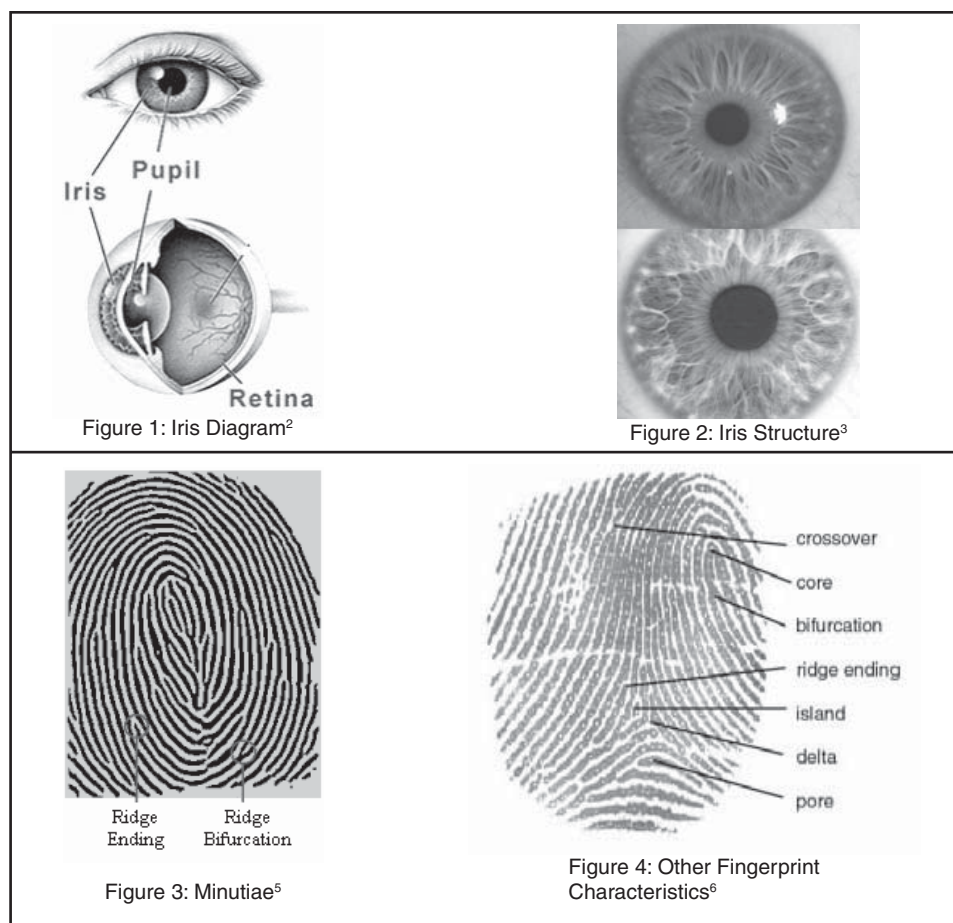
There are many types of access control system barriers and perhaps even more identification methods—there are at least nine different card-encoding technologies available, including the better-known technologies such as magnetic stripe or proximity.

Today **smartcard technology** and biometric systems are becoming more and more prevalent. Smart card technology is used to describe a single card that performs more than one function (e.g., access control and photographic identification).

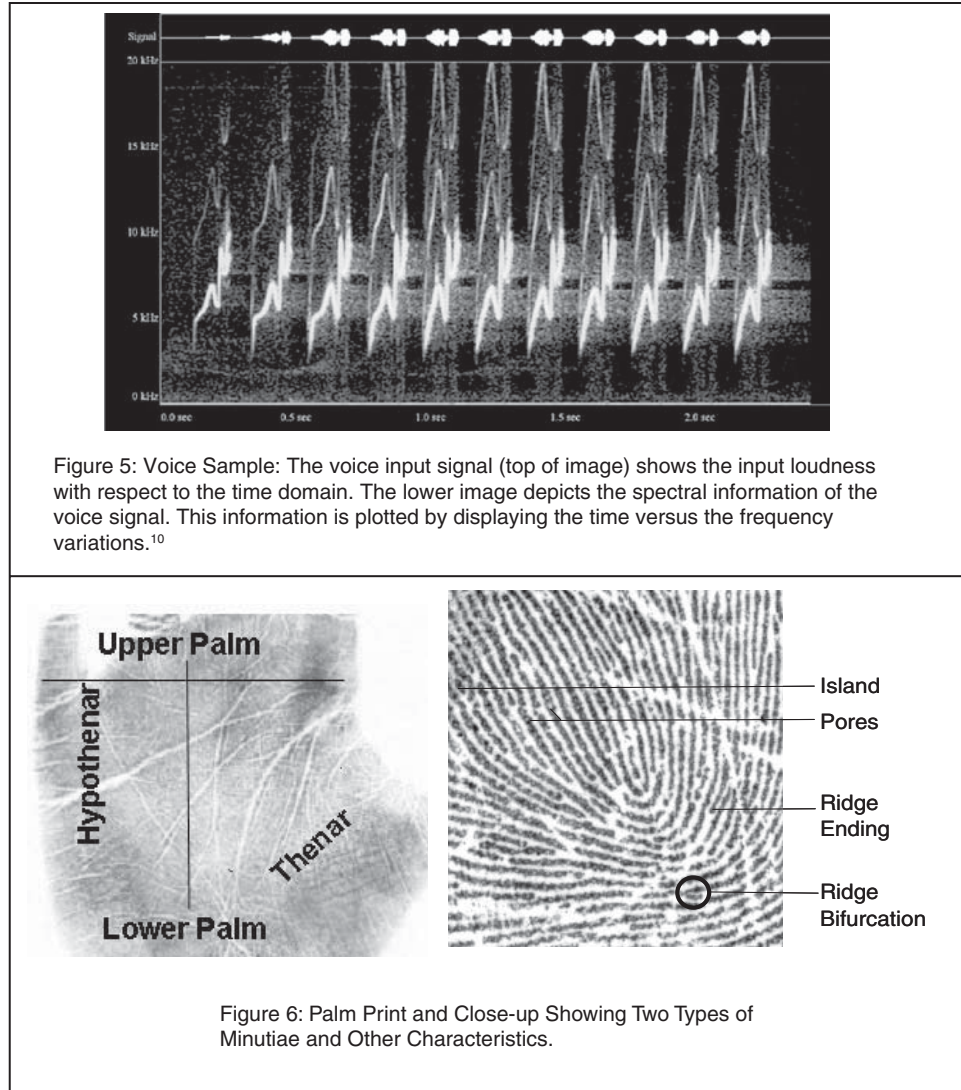
Access control-related biometric technology differs from cipher in that the individual seeking entry knows authorizing information and a token, based on something the individual possesses, is read by the barrier. As shown in Figure 3-17, biometric technology is based on who the individual is.

*TCRP Report 86, Volume 4: Intrusion Detection for Public Transportation Facilities Handbook* contains a checklist for sizing or engineering an access control system (see Table 3-3). However, this list should only be used in conjunction with the help of security professionals specializing in designing and implementing access control systems. Establishing an integrated access control system can be complex, given that the effort involves both short- and long-term issues of design, maintenance, continued operation, training, and testing.

Access control systems can be expensive and costs are easy to underestimate. Expenditures associated with system infrastructure can climb quickly as the organization's needs grow and



**Figure 3-17. Biometric technologies including iris recognition, fingerprint identification, voice recognition and palm print identification.**



Source: Adapted from National Science and Technology Council (NSTC) Subcommittee on Biometrics  
<http://www.biometriccatalog.org/NSTCSubcommittee>

**Figure 3-17. Continued.**

mature. Security planners should contemplate access control implementation based on lifecycle costs and multi-year capital planning.

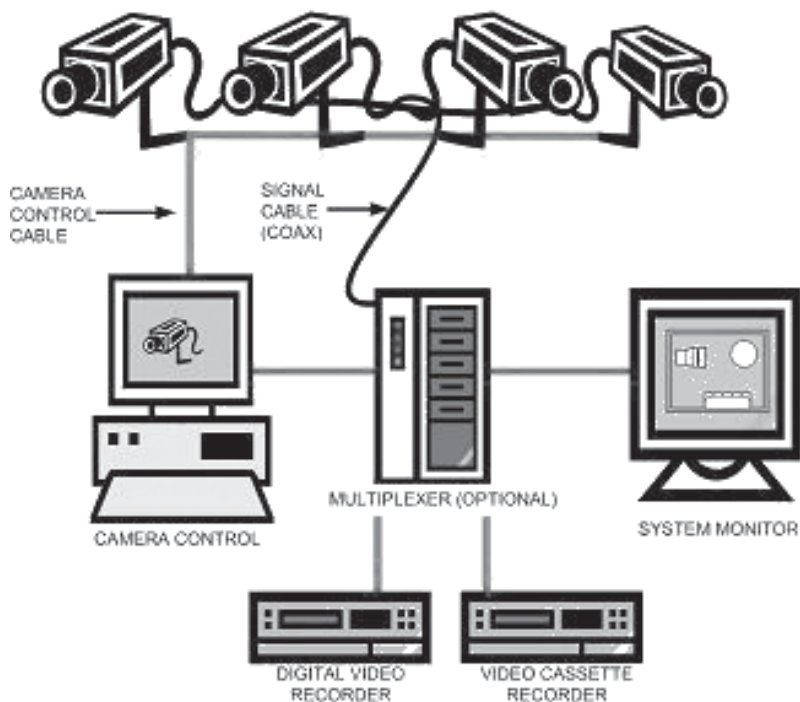
## Surveillance Systems and Monitoring

More and more every day CCTV is being used as a security countermeasure for both homeland security and crime prevention. The public has, for the most part, accepted the presence of videocameras in public places as a routine part of their daily coming and goings. Video systems can now be observed in use in facilities such as banks, shopping centers, transportation facilities, casinos, gas stations, convenience stores, and stadiums. Outdoor surveillance cameras are being mounted in downtown districts in major cities, highways, parks and recreation areas, and even at intersections where traffic violators are being caught on film running red lights.

**Table 3-3. Checklist for sizing or engineering an access control system.**

Order	System Characteristic	Explanation	Information Needed
1	Number of Locations	Is this system for one physical location or multiple locations?	List of locations
2	Network Connectivity	If multiple locations, what kind of network connectivity exists between the sites?	Example T-1 data line, or via Internet
3	Area of Containment	Is area enclosed by security barriers? Fences, Walls, Building, Gates/Portals	Area map with barriers and gates identified for each location
4	System Zones	How many security zones? These are areas of limited access (by time, training, need, etc.)	Defined zones on map
5	Access Rules	Need to determine rules for access to systems zones. A matrix of personnel and business/safety rules that allow access. Example – Chief of Security has full access all the time. Office janitor has access to public administration building during work hours only.	Full list in matrix form
6	Gates/Doors/Portal	What are the number of personnel and vehicle portals? (Portal = gate, door, etc.)	A count of portals by type
7	Personnel Tracking	Is there a need to know if people are either in or out? Or just secure check in is needed? Secure in & out requires ACS readers on both sides of gate / portal	Secure in & out or just secure in—by location
8	Material Tracking	Is there a need to track vehicles, trucks, computers or other 'materials'?	Yes or no. If yes provide a list.
9	Number of Badges	How many people = number of badges. (Badges = Access Cards)	Count
10	Number of Trackers	If tracking materials is needed, how many?	Count by type
11	Hazardous Conditions	Area card reader installed in hazardous locations?	Limits types of readers
12	Biometrics	Are biometrics used, and if so what type?	Yes or no. If yes what type?
13	Reader Type	What type of reader? Examples – RF proximity, Biometric	Reader Type
14	Badge Type	What type of badge is needed?	Follow Reader Type
15	Badge Information	What information is needed on badge? Name, photo, employee number, etc.	Graphic of front & back of badge with ALL data
16	Badge Production	Need to determine number & type of badging stations. Input included number, type, and physical locations	Count & location of badging production stations.
17	Tracker Information	What information is needed on the material tracker 'badge'?	Full description
18	Traffic	How many people use the system on a daily basis?	Number of accesses. In & Out = 2
19	History	How much data is to be saved. Including badges issued, portals transferred, access changes, period of data retention.	Study of traffic to size ACS data storage requirements
20	Data Integration	Does the ACS interface with other systems? Examples include HR, time & attendance, etc.	Data integration plan with database mapping
21	Intrusion Detection	Is an IDS present? If so what type of integration is required?	Yes or no. If yes list interfaces
22	Video Interface	Is there an interface between ACS and video systems?	Video at portals? Badge photo pop up upon access?
23	Computer OS	Is there a preferred Computer Operating System?	Influence on chosen ACS
24	Installation Support	Is support labor for installation readily available?	In house, contract, turnkey?
25	System Support	Is support labor for maintenance & repair available?	In house or outsource?
26	System Operation	Is support labor available for system operation?	In house or outsource?

Source: TCRP Report 86, Volume 4 Intrusion Detection for Public Transportation Facilities Handbook



Source: SAVER Highlight, CCTV Technology, 2005 <http://www.dhs-saver.info>

**Figure 3-18.** SAVER highlight CCTV.

The term CCTV is synonymous with surveillance technology and has come to be used as a generic descriptor for video systems. Originally the term was used to differentiate between broadcast television and private video networks. In general, CCTV is a system of one or more video cameras connected in a closed circuit or loop. The cameras provide input images to a television monitor for viewing. Depending on security objectives, the CCTV system may also include a recording and playback capability (see Figure 3-18).

Effectively integrating CCTV into a transportation agency's security program demands that planners exercise a high level of conceptual understanding of the capabilities of the technology and its ability to meet organizational requirements and needs. Video systems do not provide any form of denial of attack or delay in response to aggressor tactics or actions. They present no physical barrier, nor do they control access or reduce exposure to dangerous conditions. In the strictest sense, CCTV seeks to deter aggressor actions or targeting through an increase in the aggressor's perceived risk of capture or his belief in the successful interdiction and prevention of an attack. Recognition of this circumstance means that to effectively deploy CCTV as a deterrent requires aggressor knowledge of the presence of the system. In addition the aggressor must believe that the CCTV system will indeed prevent or reduce the likelihood of success (see Figure 3-19).



With an overt CCTV camera, the public (and offenders) can clearly see the surveillance camera and determine the direction in which it is facing.

Source: US DOJ, *Video Surveillance of Public Places* by Jerry Ratcliffe, 2006

**Figure 3-19.** Overt CCTV camera.

CCTV also serves a second almost equally important role as a security tool capable of greatly improving the performance and responsiveness of security forces and intrusion detection systems, including alarm and access control. By adding video surveillance to these systems, an agency can remotely monitor and assess security conditions during a security incident. In fact currently available advanced video surveillance technologies can further expand the

effectiveness of video monitoring. Switchers that permit operators to select between video images, multiplexers that facilitate simultaneous viewing, and new video analytic capabilities are in use to aid operators by directing their attention to priority images (see Figure 3-20). Technology such as facial recognition software and thermal imaging systems can further increase the value of video surveillance (see Figure 3-21).

In 2007, the American Public Transportation Association (APTA) published *The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for use in Transit related CCTV Systems*, as a part of its IT Standards Program Recommended Practice (RP) Series. APTA IT-RP-001-07 V1.2 is a valuable technical resource for transportation agencies considering implementation or upgrading of CCTV systems. The document covers the selection and use of cameras for CCTV at stations as well as on moving transportation conveyances such as buses or train cars. Recording devices and backbone architecture for support of CCTV are discussed in detail. In its overview section the APTA RP states:

This level of quality is intended to facilitate the requirements of the systems design through a formal 'Systems Requirement Specification' (SRS) allowing the systems to be designed for every day safety and security requirements as well as revenue protection and anti crime and anti terrorist applications requiring the identification of unknown people and objects depicted within images and allow systems to be designed to meet the 4 industry accepted categories known as *Detect, Monitor, Identify and Recognize*

The industry-accepted categories of Detect, Monitor, Identify, and Recognize are used by APTA to frame the functional requirements of CCTV systems. Specifications are based on image resolution criteria that depend on the security purpose and use for the video system. Figure 3-22 provides a comparison of screen size image projections for these categories.

Operational context and applicability for each of the categories is provided in Table 3-4.



This semi-covert CCTV camera may have a crime prevention advantage over an overt system because offenders can never be sure in which direction that camera is facing.

Source: US DOJ, *Video Surveillance of Public Places* by Jerry Ratcliffe, 2006

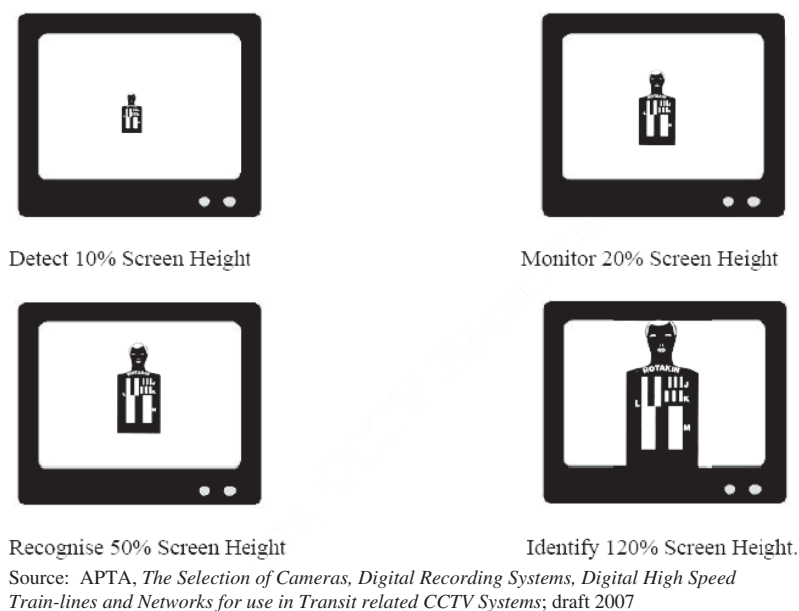
**Figure 3-20. Overt CCTV camera.**



Source: SAVER Summary; *Closed Circuit Television Technology Handbook*, 2006 <http://www.dhs-saver.info>

**Figure 3-21. Thermal imaging camera (a) and photo (b).**





**Figure 3-22. Screen size image projections.**

Figures 3-23 and 3-24 illustrate the categories by focusing on image resolution requirements for successful “identification” of a suspect. The photographic images in the bottom two pictures are cropped, enlarged, and enhanced from the photos immediately above them.

The determination of image resolution requirements is perhaps the most important aspect of CCTV system design. Without usable images, security personnel cannot discharge their responsibilities. However, the costs attributable to CCTV design can increase exponentially when security planners overreach the system capabilities to meet criteria that serve no objective purpose. This problem extends not just to image quality but also to the functionality of the other component parts of video systems. CCTV design should start with a needs and requirements analysis based on the findings of the agency’s risk assessment. Activity-driven performance functions should be identified that articulate each vulnerability or security objective that the CCTV system should address.

**Table 3-4. Operational context and applicability.**

<b>Function</b>	<b>Screen image</b> (size of image when viewed on a monitor without zoom)	<b>Typical applications</b> (not limited to and for example only as specific areas will vary according to local conditions)
Detect	<b>Not less than 5%</b> A figure occupies at least 5% of the screen height. From this level of detail an observer should be able to monitor the number, direction and speed of movement of people, providing their presence is known to him.	Perimeter security Long range images over parking lots, etc.
Monitor	<b>Not less than 10%</b> The figure now occupies at least 10% of the available screen height. After an alert an observer would be able to search the display screens and ascertain with a high degree of certainty whether a person is present or not.	Entrance areas. Perimeter security medium range. Medium range security of entrance halls, platform areas, etc.
Recognize	<b>Not less than 50%</b> When the figure occupies at least 50% of screen height viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before.	Mobile applications: interior car and bus surveillance at door or call button area. Front facing applications on vehicles or areas where bus or train exteriors are viewed. Short range security for hallways, revenue and ticket areas, railroad crossings, call buttons and parking garage entrances/exits. Elevator lobbies.
Identify	<b>Not less than 120%</b> With the figure now occupying at least 120% of the screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.	Mobile applications for cash boxes/fare machines and crew safety. Short range applications at ticket barriers, fare machines, cash rooms, garage barriers and secure door entrances (licence plate and payment machine).

Source: APTA, *The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for use in Transit related CCTV Systems*; draft 2007



(a)



(b)

Source: APTA, *The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for use in Transit related CCTV Systems*; draft 2007

**Figure 3-23. Closed-circuit television image likely to be suitable for personal identification.**



(a)



(b)

Source: APTA, *The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for use in Transit related CCTV Systems*; draft 2007

**Figure 3-24. Closed-circuit television image unlikely to be suitable for personal identification.**

# Security Personnel and Training

Developing and maintaining an effective security posture depends on the security expertise, diligence, and level of training of the employees of the transportation agency's workforce. Chapter 4 begins with an explanation of the myriad issues associated with fielding a security force and the types of data that can be used to determine the best coverage options available. A transportation security force planning flowchart that clarifies the decision points leading to a decision to deploy a dedicated police force is included. The pros and cons of hiring security consultants or security contractors is then discussed, followed by commentary on the importance of involving the agency's non-security personnel in the security effort. The chapter concludes with an overview of security training, starting at the awareness level and proceeding through to the conduct of full-scale exercises and drills.

## Security Forces

The costs associated with deploying personnel are the most expensive security countermeasure a transportation agency can undertake. The labor costs associated with the agency's operating budget for security can exceed 90 to 92% of total annual expenditure. However, 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. Security personnel provide a vital capability for which there is no substitution—the ability to comprehend and apply reason. Security personnel can perceive the nature of a threat and 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 predominating in both the homeland security and public safety context. Absent a response, aggressors or criminals would quickly disregard other security countermeasures as irrelevant.

Deciding on the necessity for security personnel or the extent to which forces should be deployed can be a significant challenge for security decisionmakers. The answers depend on the threats facing the agency and issues such as size, population served, and operating locale. For example, transportation systems operating in high-density population areas probably are at higher risk of attack than more rural systems. Other external factors can affect security personnel decisions (e.g., 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. In general, transportation agency decisionmakers have an initial—spend or no spend—hurdle to clear in thinking about security personnel deployment. To do so will require significant interaction with local authorities to establish the level of protection and response to security incidents that can be expected.

Once accomplished and tested, the response must be balanced against the agency's risk assessment. Assuming there is budget, spending operating money 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 who 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 invested in a security force should strive to ensure that the rationale for security personnel staffing is objective and consistent with both an established threat profile and other organizational needs and requirements.** If 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. When the transportation agency objectively determines that a security presence, beyond that available from the locale's public safety community, is necessary to protect the system and its users, several planning options should be analyzed. Figure 4-1 depicts the decision points that should be considered.

Questions include

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

The tradeoffs associated with these options affect the transportation agency's overall security posture significantly. At one end of the spectrum of 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. What the agency selects will affect the capabilities of not just the security labor force but also the performance and effectiveness of all other integrated system security countermeasures.

Regardless of what underlying qualitative factors drive the decision about fielding security personnel, the best way to make accurate staffing level determinations is through the use of quantitative analysis. Two different sets of quantifying data are available:

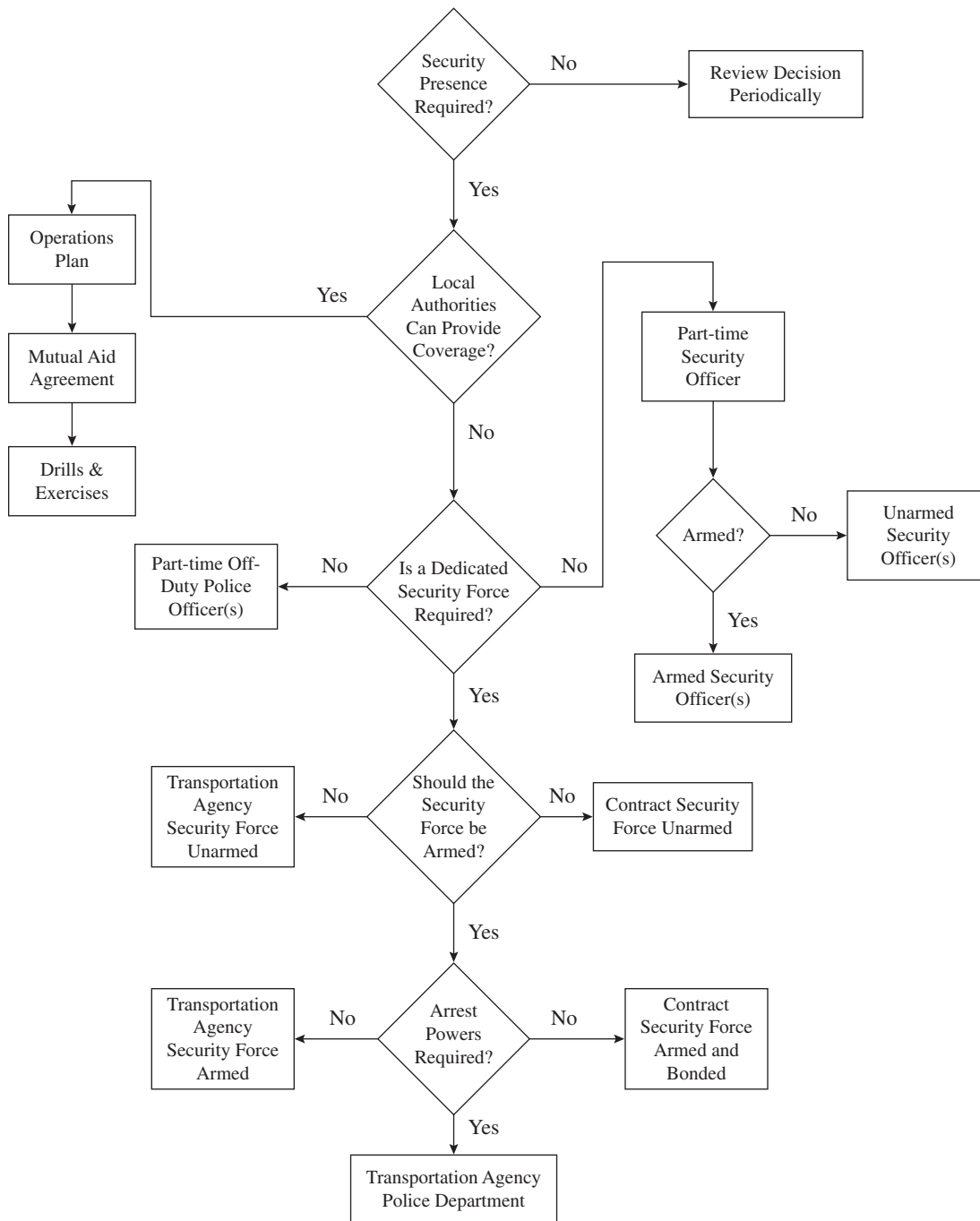
- Information based on security breaches or crime incidents, including calls for service and self-initiated incident responses; and
- Policy and procedure supported staffing deployment based on activities and scenarios.

This latter data set depends heavily on the capture of baseline response data obtained through actual security incidents, drills, and exercises. Using crimes information and related data for security analysis is common in both police departments and security organizations.

The needs of normal police work and those of transportation agencies differ. For example, police work may focus on combating the use of guns and drugs and on civil strife, while transportation agencies focus on quality-of-life issues. Often, coordinating transportation security forces with community policing forces will be beneficial; however, written agreements and clarification of jurisdiction are needed when organizations share resources and expertise.

Statistics on the occurrence of specific types of crimes or incidents typically is used to plan future crime control, security management, and risk reduction efforts. From the quality-of-service perspective, most transportation agencies experience a low level of serious criminal incidents. Known as "Part 1 Crimes" in conformance with FBI Uniform Crime Reporting (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

**TRANSPORTATION SECURITY FORCE  
PLANNING FLOW CHART**



**Figure 4-1. Transportation security force planning flowchart.**

**Table 4-1. Sample staffing level for trespass incidents.**

Officers on Duty	Trespass Incidents	Response Time (in minutes)
10	50	30.0
15	50	22.5
20	50	15.0
30	50	7.5

**Table 4-2. Staffing level for tunnel checks.**

Officers on Duty	Tunnel Checks	Response Time (in minutes)
10	50	30.0
15	50	22.5
20	50	15.0
30	50	7.5

Trespass Incidents at Location ÷ Number of Security Officers = Response Time

Patrol Activity Time ÷ Total Shift Time = % Patrol Activity per Officer

Critical Infrastructure Tunnel Checks ÷ Number of Security Officers = Response Time

Vulnerability Reduction Activity Time ÷ Total Shift Time = % Vulnerability Reduction Activity per Officer

analysis standpoint. When the situation exists where quantifying serious crime data is inadequate to assist in establishing staffing levels, officer productivity data, including total calls for service and self-initiated security or police officer activities, should be used. For example, calls for service to respond to complaints of trespassers on agency property can be totaled for a specific period. The calls can be broken down by location, time of day, day of week, and other criteria. Then the information is measured against existing staffing levels and response times for responding security forces as a means to identify an acceptable security operating condition where risk is maintained within tolerable limits. Assuming the agency establishes a 15-minute response to a trespass incident as acceptable risk, Table 4-1 indicates that a staffing level of 20 officers would be required.

Self-initiated patrol activity associated with the security of parking lots, rest stops, maintenance facilities, or other agency areas can be similarly documented and measured as a percentage using a ratio of patrol activity time calculated against total shift time. This data can then be aggregated to establish the agency’s acceptable risk goal as a total number. (Assuming data collection shows that 50% of officer time is spent performing patrol activity, if the agency establishes a goal of 200 hours of shift time as acceptable risk, then a staffing level of 50 officers would be required.)

By extending this concept of data collection productivity quantification to those security-related issues most important to the agency, security planners can approximate how large the security force should be. Other factors such as prior existing assignments of security or police to a given location will also affect staffing decisions; however, 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 obtaining a reasonable approximation of security force workflow. For example, knowledge by the transportation agency that aggressor tactics may include attempts to place IEDs at critical infrastructure points such as tunnel entrances can result in periodic patrol checks at such locations. Similar to the above trespassing checks, security force response times can be measured by location, time of day, day of the week and so forth simply by treating the tunnel infrastructure check as a call for service. Assuming the agency establishes a 15-minute response to a tunnel check as acceptable risk, Table 4-2 indicates that a staffing level of 20 officers would be required.

The time ratio data on self-initiated vulnerability reduction activities to protect critical assets and infrastructure would be measured as well. Assuming data collection shows that 50% of officer time is spent performing vulnerability reduction activity, if the agency establishes a goal of 200 hours of shift time as acceptable risk, then a staffing level of 50 officers would be required.

The response to trespass calls or performing tunnel checks as cited in the examples would not be mutually exclusive with patrol activities or vulnerability reduction activities. In fact, the transportation security force would integrate these activities together to optimize total security effectiveness.

## Security Experts, Consultants, and Contractors

In previous sections of this report, express recommendations have been made to transportation agencies regarding the need to use security professionals to help in certain aspects of risk assessment, security planning, and countermeasures identification. It is specifically recommended that security consultants be contracted to assist in the performance of security vulnerability assessment (SVA) and security plan development. Obtaining professional help in security workforce planning may also be appropriate. Security contractors should be retained to assist in security systems integration, particularly in connection with the selection and implementation of hardware and electronics such as intrusion detection, alarm systems, access control, and CCTV. Frequently, an organization will hesitate to formalize a consulting arrangement with a security practitioner or firm; this hesitancy does not always make good business sense. Even the most professional in-house security departments, as expert as they may be in all phases of security risk management, processes and procedures, and security technologies, use independent outside contractors. Competent security consultants are available to perform research, analyze conditions, and develop comprehensive security programs that can reduce the risks associated with conducting transportation operations. Of course, this assumes that the agency has identified the right consultant or consulting service.

The two main factors to be evaluated when selecting professional security consulting assistance are

- Review of the documented qualifications of the security firm and
- The backgrounds of the individuals who will perform the security work.

Ideally, the agency will be able to identify a security firm with a successful record of past contracted employments performing work in the specific transportation sector and discipline (e.g., rail, port, airport, pipeline, highway, or transit). In addition, the security firm's leading experts will be available and on the team assigned to conduct the security work contemplated. **Hiring an independent security consultant is not the same as accepting security "recommendations" from a manufacturer or retailer's representative.** Independent consultants can be called on to provide objective opinions without bias or predetermination. Salespersons, especially those with high technology products, are usually limited in approach and biased toward the company they work for. Out of loyalty to their companies and sometimes their commissions, the sales pitches of security contractors may propose security staffing or technology that does not fit the risk profile or operating environment of the agency. Overemphasis on guards, alarms, or surveillance systems can drain operating and capital budgets unnecessarily when the proper solution is the integrated balancing of security policy and procedure with the other countermeasures in the agency's toolkit.

## Security Committees and Employee Watch Programs

As with safety, security in a transportation agency is a "top-down" organizational activity. This is because executives, by necessity, must support cross-disciplinary functions in order for the activities to succeed. By lending support to important agency functions, leadership drives the prioritization of work to comport with the direction provided. Unfortunately, security as a function within an agency is often deemphasized until an incident occurs. Managers, many times because of their lack of familiarity with the subject matter, can be reluctant to broach the issue of security. Then when an incident happens, impromptu crisis thinking can intrude on disciplined managerial decisionmaking, causing "knee jerk" reactions that defeat security planning and preparedness. To overcome this tendency, senior management of an organization must be active in determining the course of the security-related activities of the agency. **It is recommended that the chief executive establish a senior advisory group consisting of executives from various departments who are designated oversight authority for systemwide security.** This senior committee should meet regularly to establish direction and develop strategic-level security policies and guidelines.



The agency should also involve front-line and mid-management level employees in security. Representative individuals from across the agency should be selected to serve as security coordinators and as participants in security committees. Where the agency maintains a dedicated security force, department coordinators should be responsible for day-to-day security interface and liaison. In those agencies without a dedicated security force, a committee of department security coordinators should be empowered with the authority to manage security activities systemwide. The key objectives of program coordination are as follows:

- Deploy a broad-based systemwide security management process that identifies, tracks, and responds to all security threats, vulnerabilities, and occurrences;
- Maintain a workplace where security incidents are routinely reported and contributions to improve security are received from every staff and operating department; and
- Ensure that front-line and mid-management employees promote security awareness and communications throughout the organization.

Employee watch programs have long been recognized as an important security tool available to employers. However, most of these programs fail or are moderately effective because of a lack of guidance and support. It is not sufficient for an agency to enlist participants and then send them out to “do security.” The agency’s security planners must work aggressively to define the security awareness roles, responsibilities, and criteria for such programs. This includes a basic security issues assessment, formulation of either step-by-step implementation plans or fresh start “invigorators,” and creation of calendar initiatives designed to keep employee watch participants actively engaged in security. Participants should also receive priority enrollment for attendance at security training.

## Security Training

The employees of transportation agencies are a critical resource for maintaining a safe and secure operating environment. They represent an omnipresent team of experienced people who are knowledgeable and insightful about the work of the agency, as well as the operating norms and environmental conditions that affect the workplace day to day. **Because of their continued presence in and on agency properties or conveyances employees are uniquely positioned to identify issues, problems, and deviations from what is usual.**

In security, this capability takes the form of recognizing suspicious activities and identifying dangerous or hazardous conditions. For example, in response to a bomb threat in an administrative area, an office worker is better equipped to find a suspicious item or package in his workplace than first responders who are unfamiliar with the surroundings. Employees are also at the forefront of organizational activities, performing work in stations, on vehicles, in plants and warehouses, and on roadways and rights of way. As such, they are often the first to observe that something is wrong. But transportation agencies cannot assume that employees will focus on security issues without training. Employees need to receive security awareness orientation to prepare them for their security roles. Thereafter, employees must be able to practice what they have been taught to reinforce a security awareness culture at the agency. Establishing a security culture for all employees is mandatory for maximizing the security effectiveness of an organization.

The responsibility for development, oversight, and enhancement of security awareness programs and activities should be given to a specific individual or function. This assignment can be full- or part-time, depending on agency size and operations balanced against security risk. But similar to safety, regardless of size or risk, transportation agencies at minimum should implement a security awareness program that enables all personnel to contribute to the security of the operating environment.

The main objective of a security awareness program is the creation of sustainable processes and methods to indoctrinate and educate employees, contractors, and other agency stakeholders about workplace security requirements. Program elements include the following:

- Centralized security information dissemination of policy and procedures reminders, security alerts, and updates;
- Promulgation of employee security handbooks and tip cards;
- Design of coherent, multi-phased, security awareness training curricula, including use of “train the trainer,” self-directed, computer-based, and multi-media methodologies;
- Scheduling of security awareness training;
- Promotion and distribution of security-related training products;
- Identification of employee security training needs;
- Systemwide research to identify security weaknesses;
- Creation of training solutions to overcome vulnerabilities and deficiencies;
- Documentation of training activities and accomplishments;
- Maintenance of training records and materials;
- Support for security planning and initiatives and vetting of proposed security policies and procedures;
- Support for staff and operating division security leadership in the creation of performance-driven security components;
- Acquisition of feedback to determine the effectiveness of programs;
- Terrorism threat recognition and suspicious activity reporting;
- Bomb threat and unattended item management;
- Chemical, biological, and radiological threats;
- Computer and cyber security;
- Mail and delivery handling;
- Theft prevention;
- Vendor and contractor security;
- Employee travel, both domestic and international; and
- Workplace violence.

The transportation industry, its associations such as AASHTO and APTA; research organizations; educational institutions; and government agencies such as DOT, DOJ, TSA, FHWA, FTA, and CDC have developed a significant body of security awareness information important to the transportation sector. Available information resources include the following:

1. *Responding to Threats: A Field Personnel Manual NCHRP Report 525: Surface Transportation Security Volume 1*, National Cooperative Highway Research Program 2004 [www.trb.org/TRB/publications/Publications.asp](http://www.trb.org/TRB/publications/Publications.asp)
2. *System Security Awareness for Transportation Employees NCHRP Report 525: Surface Transportation Security Volume 7—System Security Awareness for Transportation Employees*, National Cooperative Highway Research Program 2005 [www.trb.org/TRB/publications/Publications.asp](http://www.trb.org/TRB/publications/Publications.asp)
3. *Employee Guide to System Security Commuter Rail*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
4. *Employee Guide to System Security Bus Operations*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
5. *Employee Guide to System Security Light Rail*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
6. *Employee Guide to System Security Commuter Bus*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
7. *Employee Guide to System Security Bus Maintenance*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

8. *Employee Guide to System Security Heavy Rail*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
9. *Employee Guide to System Security Workplace Violence Prevention*, (Pocket Guide) National Transit Institute <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
10. *System Security Awareness for Transit Employees Student Guide*, National Transit Institute 2003 <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
11. *System Security Awareness for Transit Employees—Warning Signs*, National Transit Institute 2003 <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
12. *Security Incident Management for Transit Supervisors Student Guide*, National Transit Institute 2003 <http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)
13. *Federal Bureau of Investigation (FBI) Guide to Concealable Weapons*, Federal Bureau of Investigation (FBI) 2003 <http://www.cutr.usf.edu/security/reports.htm>
14. *ATF Bomb Threat Checklist ATF 1613.1*, Bureau of Alcohol Tobacco and Firearms June 1997 [http://www.state.tn.us/homelandsecurity/bomb\\_checklist.pdf](http://www.state.tn.us/homelandsecurity/bomb_checklist.pdf)
15. *Improvised Explosive Device (IED) Safe Standoff Distance Cheat Sheet*, US Army National Ground Intelligence Center
16. *Terrorist Bomb Threat Stand-Off Card*, (Pocket Guide) Technical Support Working Group
17. *Best Practices for Safe Mail Handling*, DHS Interagency Committee September 2006
18. *Biological Attack Human Pathogens, Biotoxins, and Agricultural Threats*, National Academy of Sciences 2004 [www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)
19. *Chemical Attack Warfare Agents, Industrial Chemicals, and Toxins*, National Academy of Sciences 2004 [www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)
20. *Nuclear Attack*, National Academy of Sciences 2004 [www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)
21. *Radiological Attack Dirty Bombs and Other Devices*, Academy of Sciences 2004 [www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)
22. *Worker Training in a New Era: Responding to New Threats*, Department of Health and Human Services NIOSH October 2002
23. *Dirty Bombs Fact Sheet*, United States Nuclear Regulatory Commission March 2003
24. *Dirty Bombs—Fact Sheet*, Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) July 2003 PDF <http://www.cdc.gov>
25. *What You Should Do To Prepare For and Respond to Chemical, Radiological, Nuclear and Biological Terrorist Attacks*, RAND Corporation 2003
26. *Suicide Bombing Awareness Guide*, DHS
27. *Highway Security Awareness*, Transportation Security Agency, [www.tsa.gov/what\\_we\\_do/tsnm](http://www.tsa.gov/what_we_do/tsnm)

In addition to security awareness training, transportation agencies should consider providing transportation managers and employees with a working knowledge of security concepts, guidelines, nomenclature, and processes. The emphasis of such follow-on security training programs should be to help personnel to understand the following:

- The nature of threats against the agency,
- The methods and strategies available to minimize or reduce those threats and,
- The implementation process for improving security.

Employee knowledge of the underlying rationale for deploying security countermeasures will go a long way toward ensuring that an appropriate level of risk reduction becomes a part of the agency's operations. Security practitioners are aware that to be competent in their profession the extent of required knowledge, expertise, and experience in security management is increasing. So too must managers and employees improve their grasp of the security function. Mainstreaming security into the organizational culture ultimately demands greater understanding by more

and more employees of what is at stake. By providing security training, the agency will broaden the perspective and exposure of employees to security thinking while improving the capabilities of the workforce.

Resources to conduct employee security training can be acquired from either in-house training departments or externally from security training contractors. However, in most agencies in-house trainers lack the specific instructional background necessary to teach security courses effectively. External security courses are available that can be attended by agency employees. Usually agencies can also contract for delivery of these courses at agency-selected locations. In many instances, courses are free. Federal grant monies are also available for use in paying for any resultant training costs. Tables 4-3 and 4-4 list some of the authorized training courses published by the Department of Homeland Security in the 2007 Transit Security Grant Program (TSGP). From this list, agencies can select courses covering topics such as terrorist threat recognition, transit system security design, and managing transit emergencies. They can use monies obtained through the grant program to conduct the security training. (Similar grant programs exist covering other transportation sectors.)

Ensuring that agency personnel can perform a security role requires repetitive reinforcement of information obtained through training. An important aspect of accomplishing this requirement is the use of training exercises, such as “tabletops” and “full scale.” Tabletops are discussion-based exercises while “full scale” is a training method in the “operations-based exercises” group.

Figures 4-2 and 4-3 illustrate the array of exercise types and briefly describe the purpose as identified by DHS in the Homeland Security Exercise and Evaluation Program Guidance Documents (HSEEP Vol# I, II, III, IV and V).

The significant differences between discussion-based and operations-based exercises are size and scope. For example, a tabletop exercise is a facilitated desktop discussion during which key personnel discuss scripted hypothetical scenarios in a classroom setting or perhaps at some other stationary location such as a command or operations center. Full-scale exercises are multidisciplinary, multiagency field simulations that use role players, controllers and other forms of logistical support to actively work through mock hypotheticals designed to resemble one or more actual conditions. *TCRP Report 8, Volume 9: Guidelines for Transportation Emergency Training Exercises* includes the Full-Scale Exercise Checklist (provided as Figure 4-4).

Regardless of the training exercise used, it is the design and development of well-conceived hypothetical scenarios that determines the effectiveness of the training regimen. Such scenarios must be drawn individually to address the types of security threats that face the specific transportation agency conducting the training. HSEEP recommends that scenario planning objectives be “simple, measurable, achievable, realistic, and task-oriented (SMART).”

A scenario provides the storyline that drives an exercise. The first step in designing a scenario is determining the type of threat/hazard (e.g., chemical, explosive, cyber, or natural disaster) to be used in an exercise. The hazards selected for an exercise should realistically stress the resources an entity is attempting to improve through its exercise program. The scenario should also be a realistic representation of potential threats and hazards faced by the exercising entity. The next step in designing a scenario is to determine the venue (i.e., facility or site) in which exercise play will take place. Venue selection should reflect the hazard selected, allowing for realistic, exercise-based simulation of the hazard.

Effective use of scenario-developed data sets can help the agency to develop policy and procedure and even make staffing-level deployment decisions. The importance of such security planning strategies cannot be overstated.

**Table 4-3. Training matrix: basic mass transit security training program.**

BASIC MASS TRANSIT SECURITY TRAINING PROGRAM												
Training Description	Focus	Standard	Categories of Employees to Receive									
			Front-Line Employees	Station Managers	Administrative and Support Staff	Maintenance Workers	Mid-Level Management	Senior Management	Operations Control Center Staff	Law Enforcement Officers	Security Guards	Law Enforcement
<b>Security Awareness</b>	Enhance capability to identify, report, and react to suspicious activity and security incidents	2 Hours Annually (minimum) Recurring	X	X	X	X	X	X	X	X	X	X
<b>Behavior Recognition</b>	Recognize behaviors associated with terrorists' reconnaissance and planning activities, including the conduct of surveillance. Applies lessons learned from the Israeli security meeting.	2 Hours Annually (minimum) Recurring	X	X		X	X	X	X	X	X	X
<b>Immediate Emergency Response</b>	Prepare passenger rail train operators to deal with explosive detonations, incendiaries, released chemical hazards, and similar threats in the confines of trains and system infrastructure.	4 Hours Annually (minimum) Recurring	X	X					X	X		X
<b>National Incident Management System (NIMS)</b>	Ensure transit agency emergency preparedness and response personnel gain and retain the knowledge and skills necessary to operate under NIMS in accordance with the National Response Plan (NRP).	Train on NIMS once; reinforce in drills and exercises		X				X	X	X		X
<b>Operations Control Center Readiness</b>	Identify security vulnerabilities. Understand and exercise role of OCC personnel in preventing terrorist attacks. Distinguish characteristics of improvised explosive devices (IEDs) and weapons of mass destruction. Specify priorities during a terrorist attack and manage incident response. Apply transit agency's operational plans for response to IED and WMD scenarios, directing and coordinating activities in the system.	Train for OCC readiness once; reinforce in drills and exercises							X			

Source: Department of Homeland Security in the 2007 Transit Security Grant Program (TSGP)

**Table 4-4. Training matrix: mass transit security follow-on courses.**

Training Description	Focus	MASS TRANSIT SECURITY FOLLOW-ON COURSES								
		Front-Line Employees	Station Managers	Administrative and Support Staff	Maintenance Workers	Mid-Level Management	Senior Management	Operations Control Center Staff	Security Guards	Law Enforcement
<b>Management of Transit Emergencies I (4-day course)</b>	Ensure employees throughout the transit agency understand individual roles in emergency response and the transit system's role in emergencies or disasters in the system and the broader community.	X	X	X	X	X	X	X	X	X
<b>Management of Transit Emergencies II (1-day course)</b>	Ensure employees throughout the transit agency understand individual roles in emergency response and the transit system's role in emergencies or disasters in the system and the broader community.	X	X	X	X	X	X	X	X	X
<b>Coordinated Interagency Emergency Response</b>	Advance interoperability of the transit agency with multiple responding entities in emergency response.	X	X		X				X	X
<b>Managing Counterterrorism Programs</b>	Enable transit agency management officials to develop and manage a counterterrorism program in a transit system.		X			X	X	X		
<b>Prevention and Mitigation - IEDS and WMD: T4 3-day course</b>	Enhance capabilities to identify threats from improvised explosive devices and weapons of mass destruction (chemical, biological, radiological, nuclear) to identify, report, and react to suspicious activity and security incidents	X	X	X	X				X	X
<b>Prevention and Mitigation - IEDS and WMD: CBRNE Incident Management 1-day course</b>	Enhance capabilities to identify threats from improvised explosive devices and weapons of mass destruction (chemical, biological, radiological, nuclear) to identify, report, and react to suspicious activity and security incidents	X	X	X	X				X	X
<b>Transit Vehicle Hijacking Prevention and Response</b>	Enable employees to develop and implement plans and procedures to respond to transit vehicle hijackings and workplace violence	X	X		X			X	X	X
<b>Integrated Anti-Terrorism Security Program</b>	Enhance capabilities of transit agency security officials, law enforcement personnel, and others with interaction with passengers to detect, deter, and prevent acts of terrorism.					X	X		X	X
<b>Transit System Security Design</b>	Expand integration of security considerations into designs of new transit systems and improvements of existing systems.					X	X			

Source: Department of Homeland Security in the 2007 Transit Security Grant Program (TSGP)



Source: DHS Homeland Security Exercise and Evaluation Program Guidance Documents (HSEEP Vol# I, II, III, IV, and V)

**Figure 4-2. Security exercise types by planning/training requirements.**

	Utility/Purpose	Type of Player Action	Duration	Real-Time Play?	Scope
Discussion-Based Exercises	Familiarize players with current plans, policies, agreements, and procedures; develop new plans, policies, agreements, and procedures	Notional; player actions are imaginary or hypothetical	Rarely exceeding 8 hours	No	Varies
Seminar	Provide overview of new or current plans, resources, strategies, concepts or ideas	N/A	2-5 hours	No	Multi- or Single-agency
Workshop	Achieve specific goal or build product (e.g., exercise objectives, SOPs, policies, plans)	N/A	3-8 hours	No	Multi-agency/ Single function
Tabletop Exercise (TTX)	Validate plans and procedures by utilizing a hypothetical scenario to drive participant discussions	Notional	4-8 hours	No	Multi-agency/ Multiple functions
Game	Explore decision-making process and examine consequences of those decisions	Notional	2-5 hours	No (though some simulations provide real- or near-real-time play)	Multi-agency/ Multiple functions
Operations-Based Exercises	Validate plans, policies, agreements, and procedures; clarify roles and responsibilities; identify resource gaps	Actual; player action mimics reaction, response, mobilization, and commitment of personnel and resources	May be hours, days, or weeks, depending on purpose, type, and scope of the exercise	Yes	Varies
Drill	Validate a single operation or function of an agency	Actual	2-4 hours	Yes	Single agency/ Single function
Functional Exercise (FE)	Evaluate capabilities, functions, plans, and staffs of Incident Command, Unified Command, intelligence centers, or other multi-agency coordination centers (e.g., EOCs)	Command staff actions are actual; movement of other personnel, equipment, or adversaries is simulated	4-8 hours or several days or weeks	Yes	Multiple functional areas/ Multiple functions
Full-Scale Exercise (FSE)	Validate plans, policies, procedures, and cooperative agreements developed in previous exercises through their actual implementation and execution during a simulated scenario; includes actual mobilization of resources, conduct of operations, and integrated elements of functional exercise play (e.g., EOCs, command posts)	Actual	One full day or several days or weeks	Yes	Multi-agency/ Multiple functions

Source: DHS Homeland Security Exercise and Evaluation Program Guidance Documents (HSEEP Vol# I, II, III, IV, and V)

**Figure 4-3. Security exercise description of purpose.**

<b>Full-Scale Exercise Checklist</b>	
<b>Participants:</b>	
<input type="checkbox"/>	Controller(s)—sufficient to manage all event sites
<input type="checkbox"/>	Actors (mock victims)—different age groups, body types, physical characteristics
<input type="checkbox"/>	Players (most functions, all levels—policy, coordination, operation, field)
<input type="checkbox"/>	Evaluators
<input type="checkbox"/>	Simulators—to convey messages and actions for agencies or individuals who could not participate in the exercise
<input type="checkbox"/>	Safety Officer
<b>Site Selection:</b>	
<input type="checkbox"/>	Adequate space for number of victims, responders, and observers
<input type="checkbox"/>	Space for vehicles and equipment
<input type="checkbox"/>	As realistic as possible without interfering with normal traffic or safety
<input type="checkbox"/>	Credible scenario and location
<b>Scene Management:</b>	
<input type="checkbox"/>	Logistics (who, what, where, how, when)
<input type="checkbox"/>	Believable simulation of emergency
<input type="checkbox"/>	Realistic victims
<input type="checkbox"/>	Preparation of simulators to realistically portray roles
<input type="checkbox"/>	Number of victims consistent with type of emergency, history of past events
<input type="checkbox"/>	Types of injuries consistent with type of emergency, history of past events
<input type="checkbox"/>	Victim load compatible with local capacity to handle
<input type="checkbox"/>	Props and materials to simulate injuries, damage, other effects
<b>Personnel and Resources:</b>	
<input type="checkbox"/>	Number of participants
<input type="checkbox"/>	Number of volunteers for scene set-up, victims, etc.
<input type="checkbox"/>	Types and numbers of equipment
<input type="checkbox"/>	Communications equipment
<input type="checkbox"/>	Fuel for vehicles and equipment
<input type="checkbox"/>	Materials and supplies
<input type="checkbox"/>	Expenses identified (wages, overtime, fuel, materials and supplies)
<b>Response Capability</b>	
<input type="checkbox"/>	Sufficient personnel kept in reserve to handle routine nonexercise events
<b>Safety</b>	
<input type="checkbox"/>	Safety addressed through development
<input type="checkbox"/>	Each design team member responsible for safety in own discipline
<input type="checkbox"/>	Hazards identified and resolved
<input type="checkbox"/>	Safety addressed in pre-exercise briefing, simulator, and evaluator packets
<input type="checkbox"/>	Each field location examined for safety issues
<input type="checkbox"/>	Safety officer designated, given authority
<b>Legal Liability</b>	
<input type="checkbox"/>	Legal questions of liability researched by local attorney
<b>Emergency Call-Off</b>	
<input type="checkbox"/>	Call-off procedure in place, including code word or phrase
<input type="checkbox"/>	Call-off procedure tested
<b>Media</b>	
<input type="checkbox"/>	Role of media addressed in planning, used as a resource
<input type="checkbox"/>	Media and observers considered in logistical planning

Source: TCRP Report 86, Volume 9, Guidelines for Transportation Emergency Training Exercises, 2006

**Figure 4-4. Full-scale exercise checklist.**





## CHAPTER 5

# Infrastructure Protection

The transportation operating environment creates significant challenges for security planners charged with determining which of the agency's assets require protection. This chapter frames the question for decisionmakers and then summarizes some of the methods used to rate and prioritize critical assets. Later sections address the specifics of building and facility security, bridges and tunnels, and rolling stock.

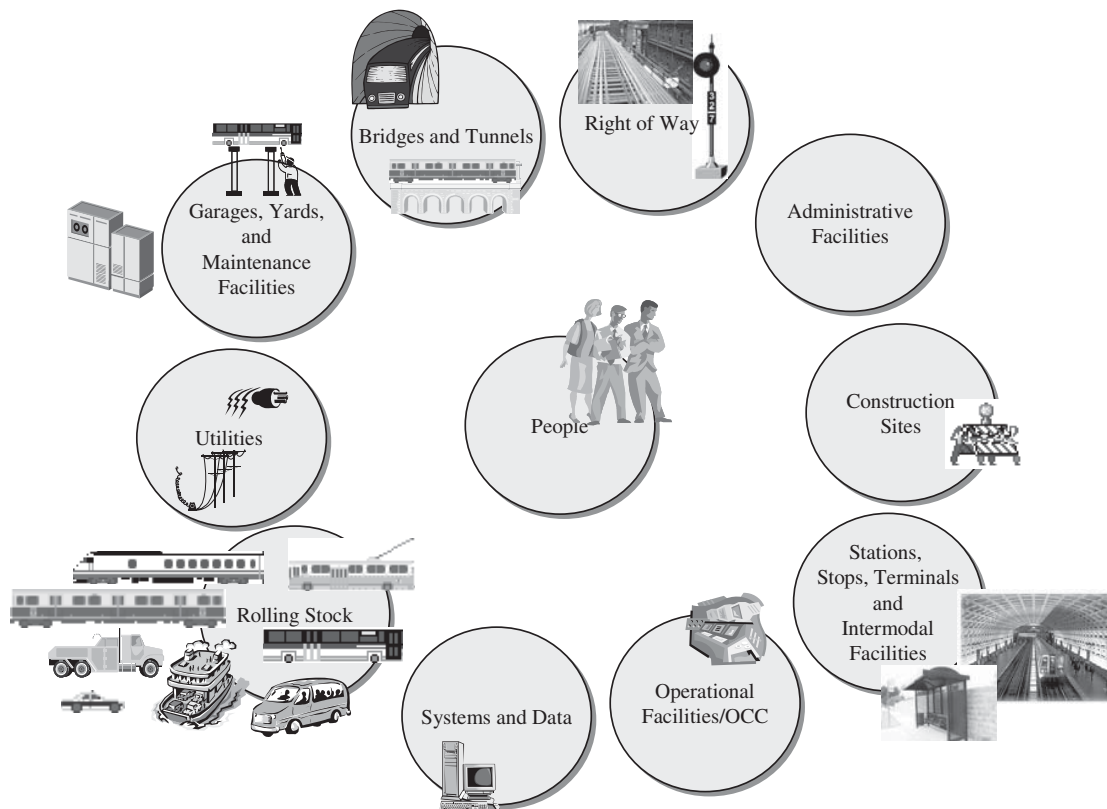
### **Critical Infrastructure Designation**

The critical infrastructure of a transportation agency includes the people, property, and information assets required to enable the organization to execute its primary responsibilities, activities, and functions. Deciding what assets or infrastructure are critical is not always as easy as it might seem. The initial sets of questions that must be answered are definitional. Should the agency use operational importance as its criteria? If so, what does that mean—importance to business continuity, quality of service, or maybe the bottom line? What about the contribution of the asset to the mission? If alternatives to using the asset are available, does that make the asset non-critical? What about the time or cost to repair assets? If the asset can be replaced quickly or at low cost, does that affect its criticality?

Other questions that need answering are about perspective. Should the agency decide what is critical based on threat assessments or target attractiveness? Are the adversaries or aggressor's eyes the right viewpoint? What about customer perceptions of security? Or perhaps even government agencies? Is national significance or the symbolic value of an asset an appropriate factor for consideration by transportation officials? These questions and many more confront security planners attempting to balance the actual security needs of an organization against the wide array of sometimes countervailing opinions.

Ultimately, most transportation agencies should take the "ownership view" which "examines information on ownership of assets, including the owner/operators decision structure, policies, and procedures, and recognizes those assets owned by the same entity as an integrated system." Taking this approach to critical infrastructure identification yields the following list of assets for transit and rail as identified in Figure 5-1. Similar infrastructure categories exist for highway infrastructure. The *AASHTO Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002 contains the following chart, provided as Figure 5-2, listing critical transportation assets.

Critical infrastructure should be identified during the preliminary stages of risk assessment. However, the transportation agency would be well served to conduct criticality reviews continuously to become better informed about ongoing security needs. Questioning assumptions about definition and perspective can be beneficial in terms of security efficiency and performance.



#### Transit Agency Assets

**Transit Stations**—used for boarding and alighting of transit passengers and for fare collection; they can be below-grade, at-grade, or elevated. Their high-profile, large-volume pedestrian traffic and central locations integrated with surrounding uses make them likely targets for terrorist attack.

**Transit Stops**—usually smaller and more open than transit stations. Typically on public land where passengers can board buses and light rail vehicles, the category includes 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.

**Operations Control Centers (OCCs)/Administrative Facilities**—used for operating and administering the transit system, they 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 are critical to the transit system and have value as strategic targets.

**Garages, Yards, and Maintenance Facilities**—used for the repair and storage of transit vehicles; they include vehicle garages, yards, and repair facilities. They often contain many assets to be protected, including 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 free, while preventing access by unauthorized vehicles and people.

#### Bridges and Tunnels:

1. 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.
2. 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.

**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.

**Remote and Unmanned Structures**—all other physical assets. This category includes power substations and 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.

Source: Adapted from *FTA Transit Security Design Considerations*, 2004

**Figure 5-1. Transit security assets.**

<b>INFRASTRUCTURE</b>	<b>FACILITIES</b>	<b>EQUIPMENT</b>	<b>PERSONNEL</b>
<ul style="list-style-type: none"> <li>▪ Arterial Roads</li> <li>▪ Interstate Roads</li> <li>▪ Bridges</li> <li>▪ Overpasses</li> <li>▪ Barriers</li> <li>▪ Roads Upon Dams</li> <li>▪ Tunnels</li> </ul>	<ul style="list-style-type: none"> <li>▪ Chemical Storage Areas</li> <li>▪ Fueling Stations</li> <li>▪ Headquarters Buildings</li> <li>▪ Maintenance Stations/Yards</li> <li>▪ Material Testing Labs</li> <li>▪ Ports of Entry</li> <li>▪ District/Regional Complexes</li> <li>▪ Rest Areas</li> <li>▪ Storm Water Pump Stations</li> <li>▪ Toll Booths</li> <li>▪ Traffic Operations Centers</li> <li>▪ Vehicle Inspection Stations</li> <li>▪ Weigh Stations</li> </ul>	<ul style="list-style-type: none"> <li>▪ Hazardous Materials</li> <li>▪ Roadway Monitoring</li> <li>▪ Signal &amp; Control Systems</li> <li>▪ Variable Messaging System</li> <li>▪ Vehicles</li> <li>▪ Communications Systems</li> </ul>	<ul style="list-style-type: none"> <li>▪ Contractors</li> <li>▪ Employees</li> <li>▪ Vendors</li> <li>▪ Visitors</li> </ul>

Source: *AASHTO Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002

**Figure 5-2. Critical transportation assets.**

## Methods to Rate and Prioritize Critical Assets

There are as many different approaches to performing the criticality analysis as there are available risk and vulnerability assessment methodologies. But regardless of the method undertaken, the basic steps remain the same—inventory, factor, value, rank, order, and prioritize. Critical infrastructure identification begins with developing an inventory, an “all-inclusive list” that describes the character of the agency’s assets sufficiently. Care should be taken to ensure that the assets are properly delineated into distinct individual elements of infrastructure rather than division into component parts, systems, or subsystems.

For example, according to the *FHWA Recommendations for Bridge and Tunnel Security*, *AASHTO Blue Ribbon Panel on Tunnel and Bridge Security*, many component parts, systems, and subsystems are associated with a suspension and cable-stayed highway bridge (e.g., suspender ropes, stay cables, tower leg, orthotropic steel deck, reinforced and prestressed bridge decks, cable saddle, approach structures, connections, anchorage, and piers). Even though some parts of the bridge structure may be more important for structural stability than others, ergo more critical, breaking critical infrastructure into these subparts will confuse rather than clarify critical assets. Once each asset has been delineated, the categories of personnel (human), property (physical), or information (cyber) can be used to group the individual elements so that the second “factoring” aspect of critical infrastructure identification can be accomplished. Factors can refer to any number of important issue areas so long as they are relevant to the agency performing the analysis. Sample areas include

- Casualty impact—the potential for loss or serious injury to human life;
- Business continuity—the extent to which loss or serious damage to the asset would impair the ability of the agency to continue to operate;
- Economic impact—the extent to which loss or serious damage to the asset would affect the viability of business going forward;
- Replacement cost—the capital investment required to replace the asset;
- Replacement downtime—the length of time before the asset can be returned to service;

- Redundancy—the availability of alternatives for use if the asset is lost; and
- Symbolic importance—the national significance of the asset.

The third part of the identification process is the establishment of relative “values” that indicate the importance of the assets to the operations of the agency. Generally, a numerical scale is used to compare the relative values. Table 5-1 illustrates relative value in the center column. This table also provides an overview of Steps 1 through 3 in critical infrastructure identification.

The final step is the rank ordering and prioritization of critical assets. Table 5-2 provides the *FHWA Recommendations for Bridge and Tunnel Security, AASHTO Blue Ribbon Panel on Tunnel and Bridge Security* example of bridge and tunnel critical asset prioritization. Note the inclusion of a “risk reduction score,” achieved through a form of algebraic analysis of the factoring and relative value steps of the process. Table 5-2 contains a rough order-of-magnitude (ROM) cost column that presents the security designer with an economic cross reference.

## Building Security

A vast body of knowledge and information is available from federal government departments and agencies about the protection of buildings. The government has gone a long way toward establishing comprehensive building security standardization requirements and criteria for federal facilities. The work began in earnest on April 20, 1995, one day after the bombing of the Alfred P. Murrah Building in Oklahoma City, when the President directed the Department of

**Table 5-1. Critical asset value.**

CRITICAL ASSET FACTOR	VALUE	DESCRIPTION
<i>Deter/Defend Factors</i>		
A) Ability to Provide Protection	1	Is there a system of measures to protect the asset?
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (Due to location, prominence, or other factors)
<i>Loss and Damage Consequences</i>		
C) Casualty Risk	5	Is there a possibility of serious injury or loss of life resulting from an attack on the asset?
D) Environmental Impact	1	Will an attack on the asset have an ecological impact of altering the environment?
E) Replacement Cost	3	Will significant replacement cost (the current cost of replacing the asset with a new one of equal effectiveness) be incurred if the asset is attacked?
F) Replacement/Down Time	3	Will an attack on the asset cause significant replacement/down time?
<i>Consequences to Public Services</i>		
G) Emergency Response Function	5	Does the action serve an emergency response function and will the action or activity of emergency response be affected?
H) Government Continuity	5	Is the asset necessary to maintaining government continuity?
I) Military Importance	5	Is the asset important to military functions?
<i>Consequences to the General Public</i>		
J) Available Alternate	4	Is there a substitute that is designated to take the place of the asset, if necessary, to perform the same or similar duties? (i.e., Is there another bridge that crosses the river in a nearby location that could be used if the main bridge is damaged or destroyed?)
K) Communication Dependency	1	Is communication dependent upon the asset?
L) Economic Impact	5	Will damage to the asset have an effect on the means of living, or the resources and wealth of a region or state?
M) Functional Importance	2	Is there an overall value of the asset performing or staying operational?
N) Symbolic Importance	1	Does the asset have symbolic importance?

Source: *AASHTO Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002

**Table 5-2. Bridge and tunnel critical asset prioritization.**

Rank	Facility	Location	Reduction in Risk Score	Project Cost (x\$1,000)
1	Bridge 1	Main Pier Base B	0.16	753
2	Other Facility 1	Element A	0.30	1,872
3	Tunnel 1	Vent Buildings – Buildings	0.48	7,857
4	Other Facility 1	Element B	0.34	8,243
5	Bridge 1	Anchor Element B	0.11	2,840
6	Bridge 1	Anchor Element A	0.10	2,840
7	Other Facility 1	Element C	0.23	6,982
8	Tunnel 1	Approach Viaduct	0.12	3,891
9	Bridge 1	Main Pier Base A	0.32	13,937
10	Bridge 4	Tension Hangers	0.05	2,944
11	Tunnel 1	Vent Buildings – Tunnel Ceilings	0.16	12,619
12	Tunnel 1	Approach Plaza	0.03	2,787
13	Tunnel 2	Vent Buildings – Buildings	0.10	9,142
14	Tunnel 2	Vent Buildings – Tunnel Ceilings	0.13	12,523
15	Bridge 1	Deck Level	0.30	30,869
16	Bridge 2	Main Piers	0.10	12,048
17	Other Facility 1	Element D	0.05	7,432
18	Tunnel 1	Administration Building	0.01	434
19	Bridge 1	Tension Hangers	0.07	12,363
20	Bridge 1	Approach Highway	0.15	32,686
21	Other Facility 2	Element A	0.01	1,950
22	Bridge 4	Main-Span Abutment	0.02	5,891
23	Bridge 3	Main Piers	0.09	24,649
24	Other Facility 1	Element E	0.10	31,754
25	Other Facility 2	Element B	0.02	6,896
26	Tunnel 1	Tunnel Structure	0.51	222,723
27	Tunnel 2	Tunnel Structure	0.35	186,735
28	Other Facility 1	Element F	0.03	20,516
29	Bridge 4	Compression Members	0.01	8,687
30	Bridge 2	Main Span	0.08	64,996
31	Bridge 3	Main Span	0.07	108,718
32	Tunnel 1	Portals	0.01	16,040
33	Tunnel 2	Portals	0.01	14,287

Source: FHWA Recommendations for Bridge and Tunnel Security, AASHTO Blue Ribbon Panel on Tunnel and Bridge Security, 2003

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*, 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 5-3).

The standards addressed four general areas of security and supplied 52 minimum compliance requirements for countermeasures in the following:

- Perimeter Security—Parking, Lighting, Physical Barriers;
- Entry Security—Receiving/Shipping, Access Control, Entrances/Exits;

**Table 5-3. Criteria for security levels.**

LEVEL	CRITERIA
I	<ul style="list-style-type: none"> <li>• 10 Federal employees</li> <li>• 2,500 sq ft</li> <li>• Low volume of public contact</li> </ul>
II	<ul style="list-style-type: none"> <li>• 11 to 150 Federal employees</li> <li>• 2,500 sq ft – 80,000 sq ft</li> <li>• Moderate volume of public contact</li> <li>• Routine operations similar to private sector and/or facility shared with private sector</li> </ul>
III	<ul style="list-style-type: none"> <li>• 151-450 Federal employees</li> <li>• 80,000 – 150,000 sq ft</li> <li>• Moderate/high volume of public contact</li> <li>• Contains agency mix such as               <ul style="list-style-type: none"> <li>○ Law enforcement operations</li> <li>○ Court functions</li> <li>○ Government records</li> </ul> </li> </ul>
IV	<ul style="list-style-type: none"> <li>• More than 450 Federal employees</li> <li>• Multi-story facility</li> <li>• More than 150,000 sq ft</li> <li>• High volume of public contact</li> <li>• High risk law enforcement intelligence agencies</li> <li>• District Courts</li> </ul>
V	<ul style="list-style-type: none"> <li>• Level IV profile and agency/mission critical to national security</li> </ul>

Source: Adapted from DOJ Vulnerability Assessment of Federal Facilities, 1995

- Interior Security—Employee/Visitor ID, Utilities, Occupant Emergency Plans; and
- Security Planning—Intelligence Sharing, Training, Admin Procedures.

In October of 1995, Executive Order (E.O.) 12977 was signed by the President “to establish policies for security in and protection of federal facilities and to provide a permanent body to address continuing government-wide security for federal facilities.” The E.O. established the Interagency Security Committee (ISC) with member agencies including DOJ, DOS, DOL, DOT, GSA, DOD, DOE, HHS, and EPA. Since 1995, the ISC, as well as other federal agencies, has published numerous building security standards documents. Available information resources follow (in some cases, a specific request for the documents must be made to the respective federal agency):

1. Vulnerability Assessment of Federal Facilities, DOJ 1995
2. ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, ISC May 2001
3. ISC Security Standards for Leased Space, ISC 2004
4. GSA Lease Security Standards, GSA November 2005
5. Standard Guide for Developing a Cost-Effective Risk Mitigation Plan for New and Existing Constructed Facilities: E 2506—06 ASTM Committee on Standards, Copyright © 2006 ASTM International [www.astm.org](http://www.astm.org)
6. GSA Facilities Standards for the Public Buildings Service General Services Administration March 2005 <http://www.gsa.gov>
7. DoD Minimum Antiterrorism Standards for Buildings (Unified Facilities Criteria UFC 4-010-01) Department of Defense October 2003 [www.wbdg.org/ccb/DOD/UFC/ufc\\_4\\_010\\_01.pdf](http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf)
8. *DoD Security Engineering Facilities Planning Manual (Draft)* UFC 4-020-01 Department of Defense March 2006 [www.wbdg.org/ndbm/DesignGuid/pdf/Final%20Draft\\_UFC\\_4-020-01.pdf](http://www.wbdg.org/ndbm/DesignGuid/pdf/Final%20Draft_UFC_4-020-01.pdf)

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:

- Air Intakes
- Computer Rooms

- Dining Facilities
- Elevators
- Equipment and Maintenance Spaces
- Fuel Storage Areas
- General Office Space
- Loading Docks
- Lobbies and Waiting Areas
- Mailrooms
- Parking Garages
- Pedestrian Entranceways
- Public Corridors
- Public Toilets and Service Areas
- Refuse Collection Sites
- Retail Areas
- Roofs
- Shipping and Receiving Areas
- Stairwells
- Utility Feeds
- Vehicular Access and Circulation
- Water Supply

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

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

FEMA 426 *Reference Manual to Mitigate Potential Terrorist Acts against Buildings* further illustrates the concept of security levels in determining the appropriate security countermeasures footprint. Building directly on the DOJ criteria, countermeasures solution sets are presented in table format in the manual. The listed security countermeasures are to be based on the performance of an on-site risk assessment (see Table 5-4).

Transportation agencies have unique types of buildings and facilities that will demand vulnerability reduction solutions that are atypical. For example, if deemed a priority target, a toll facility on an interstate highway will likely require an extensive level of structural hardening, shielding, stress-bearing systems, and anti-ram barriers either to protect the toll plaza, collectors, and vehicle occupants from an explosives blast, or to mitigate its effects. Similarly, a transit or commuter train that enters the building envelope of an underground train station creates risk vulnerability and exposure elements for building occupants through any number of different threat scenarios. As has been recommended throughout this text, agencies must specifically address such

**Table 5-4. Security levels for determining security countermeasures.**

Level**	Typical Location	Examples of Tenant Agencies***	Security Measures (based on evaluation)
<b>I</b>	10 Employees (Federal) 2,500 Square Feet Low Volume Public Contact Small "Store Front" Type Operation	Local Office District Office Visitor Center USDA Office Ranger Station Commercial Facilities Industrial/Manufacturing Health Care	High Security Locks Intercom Peep Hole (Wide View) Lighting w/Emergency Backup Power Controlled Utility Access Annual Employee Security Training
<b>II</b>	11 - 150 Employees (Federal) 2,500 - 80,000 Square Feet Moderate Volume Public Contact Routine Operations Similar to Private Sector and/or Facility Shared with Private Sector	Public Officials Park Headquarters Regional/State Offices Commercial Facilities Industrial Manufacturing Health Care	Entry Control Package w/Closed Circuit Television (CCTV) Visitor Control/Screening Shipping/Receiving Procedures Guard/Patrol Assessment Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm w/Central Monitoring
<b>III</b>	151 - 450 Employees (Federal) Multi-Story Facility 80,000 - 150,000 Square Feet Moderate/High Volume Public Contact Agency Mix: Law Enforcement Operations Court Functions Government Records	Inspectors General Criminal Investigations Regional/State Offices GSA Field Office Local Schools Commercial Facilities Industrial Manufacturing Health Care	Guard Patrol on Site Visitor Control/Screening Shipping/Receiving Procedures Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt/Zoom System) Duress Alarm w/Central Monitoring
<b>IV</b>	>450 Employees (Federal) Multi-Story Facility >150,000 Square Feet High Volume Public Contact High-Risk Law Enforcement/Intelligence Agencies District Court	Significant Buildings and Some Headquarters Federal Law Enforcement Agencies Local Schools, Universities Commercial Facilities Health Care	Extend Perimeter (Concrete/Steel Barriers) 24-Hour Guard Patrol Adjacent Parking Control Backup Power System Hardened Parking Barriers
<b>V</b>	Level IV Profile and Agency/Mission Critical to National Security	Principal Department Headquarters	Agency-Specific

SOURCE: U.S. DEPARTMENT OF JUSTICE, VULNERABILITY ASSESSMENT OF FEDERAL FACILITIES, JUNE 28, 1995

NOTES: \*\* ASSIGNMENT OF LEVELS TO BE BASED ON AN "ON-SITE" RISK ASSESSMENT/EVALUATION

\*\*\*EXAMPLES OF TYPICAL (BUT NOT LIMITED TO) TENANT AGENCIES FOR THIS LEVEL FACILITY

Source: FEMA 426 *Reference Manual to Mitigate Potential Terrorist Acts Against Buildings*, 2003

uniqueness in their operating environment when making security improvements. Buildings such as warehouses, car shops, maintenance facilities, plants and industrial areas, dispatch centers and fuel depots may all demand specialized security countermeasures or solution sets.

## Bridge and Tunnel Security

The U.S. surface transportation sector is a vast and open series of roadways, skyways, tracks, rails, pedestrian walkways, bike paths, and other routes that facilitate the travel of people and goods throughout the country. These routes are connected and interconnected by a system of



bridges and tunnels engineered to traverse difficult terrain or geography, shorten travel distances, or simply improve the journey of system users.

Although the infrastructure of the entire route is an important part of transportation agency security planning, bridges and tunnels, by virtue of their engineering, placement or cost, often are among the most critical assets of the agency. Land-based bridges are also integral to the maritime sector because these bridges cross the Nation's waterways thereby affecting the movement of ships and other vessels, particularly on inland rivers. Protecting bridges and tunnels can be complicated. In the *FHWA Recommendations for Bridge and Tunnel Security, AASHTO Blue Ribbon Panel on Tunnel and Bridge Security* the following comment was made:

Among the 600,000 bridges in the United States, preliminary studies indicate that there are approximately 1,000 where substantial casualties, economic disruption, and other societal ramifications would result from isolated attacks. Additionally, the U.S. transportation system includes 337 highway tunnels and 211 transit tunnels; many are located beneath bodies of water, and many have limited alternative routes due to geographic constraints.

Such a vast number of bridge and tunnel structures interspersed throughout the Nation's landscape points out the difficulty associated with creating a workable security protection scheme; particularly when the remoteness, inaccessibility, and reduced visibility of many of these structures has been factored in. However, looking at the extent of the assets "makes the case" that rigorous critical infrastructure identification processes are justified. The panels' estimation of 1,000 bridges (1 out of every 600) that meet critical infrastructure criteria creates a much more manageable number for consideration. Regardless, the security planning tasks in this regard are daunting and exacerbated by the various types of bridge or tunnel structures, each having unique engineering design characteristics.

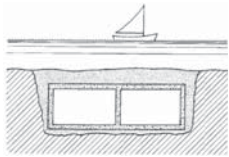
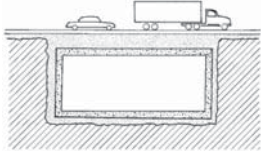
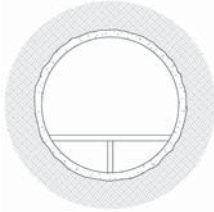
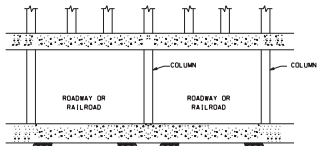
Figure 5-3 illustrates four different types of transportation tunnels, each with unique engineering characteristics that likely would call for individual countermeasures or countermeasures solution sets.

A discussion of bridge and tunnel security issues is an excellent opportunity to further explain concepts of security strategy in terms of goals and objectives. In *Making the Nation Safer*, several overarching goals for countering terrorism were identified:

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

These overlapping goals have been drawn differently in other publications, e.g., prevention, detection, deterrence, response and mitigation, or the four Ds—deter, detect, deny, and defend. Nonetheless, a significant part of the purpose and underlying message of these goals is that **certain tactics can either prevent an attack against a given target, positively influence the target selection of an aggressor, or perhaps disrupt such an attack in progress.** In fact, because of the catastrophic potential of a successful attack against some key bridge or tunnel assets, front-end efforts to defend against the loss can become an even higher priority.

Primarily, vulnerability reduction countermeasures focused on the defense of bridges and tunnels should include visible signs of security, such as fencing, lights, surveillance systems, and rapid response by security forces. The objective is to present a potential adversary with a perception

Type	Description	Sketch
Immersed Tube Tunnel	<ul style="list-style-type: none"> <li>Employed to traverse a water body</li> <li>Preconstructed sections are placed in a pre-excavated trench and connected</li> <li>Typical materials include steel and concrete immersed tunnel sections</li> <li>After placement, tunnel is covered with soil</li> </ul>	
Cut-and-Cover Tunnel	<ul style="list-style-type: none"> <li>In urban areas</li> <li>Excavated from the surface, then constructed in place and backfill placed to bury structure</li> <li>For subway line structures, subway stations, and subsurface highway structures</li> <li>Typically concrete cast-in-place or precast sections</li> <li>Steel framing and concrete fill</li> </ul>	
Bored or Mined Tunnel	<ul style="list-style-type: none"> <li>In urban or remote locations in land, on mountains, or through water bodies</li> <li>Bored using a variety of techniques</li> <li>Supported by initial and final support systems</li> <li>Soft ground or rock tunneling</li> <li>Structure may have various liner systems, including rock reinforcement, shotcrete, steel ribs and lattice girder, precast concrete segment, cast-in-place concrete, and fabricated steel lining</li> </ul>	
Air-Rights Structure Tunnel	<ul style="list-style-type: none"> <li>In urban areas</li> <li>Created when a structure is built over a roadway or trainway using the roadway's or trainway's air rights</li> <li>The limits that an air-rights structure imposes on the emergency accessibility and function of the roadway or trainway that is located beneath the structure should be assessed</li> </ul>	

Source: NCHRP Report 525: Volume 12 – Making Transportation Tunnels Safe and Secure, 2006

**Figure 5-3. Transportation tunnel types.**

that his attack will be unsuccessful or that he will be captured. More important, the absence of such visible signs of security may induce target selection by an adversary.

In particular, the approaches to critical bridges or tunnels and the undetected opportunity time or “time on target” that an aggressor can acquire are factors that deserve thoughtful security planning. For example, the approach on both sides of a critical underwater tunnel portal entrance could be lined with high security anti-ram fencing for an extended distance (e.g., one-half mile) to prevent vehicle breach. Lighting, audible alarms, surveillance, and intrusion detection systems could be deployed in tandem so that any attempted access to the portal on foot would require the aggressor to walk or run for an extended time just to reach a mission-sensitive location. Responding security forces or officers on directed patrol capable of disrupting or interdicting the attack would add a final layer of protection for the asset.

Time on target has additional ramifications for bridge and tunnel security. For example, an aggressor with sufficient time can improve the payload and blast effect of an IED by attaching or even drilling into a bridge’s critical structural elements (e.g., cable anchors, box girders, and cable towers).

Notwithstanding the stated requirement that transportation agencies must perform rigorous critical asset identification, it is accurate to presume that a recommendation for extensive security countermeasures for bridges and tunnels is somewhat incongruous with preceding

commentary about the vast and expansive number of such assets in the United States. An additional recommendation, maximizing portability in bridge and tunnel security countermeasures deployment, may help overcome this security planning dilemma. By establishing one or more portable countermeasures solution sets containing deployable sensors, cameras, alarms, and other perimeter protection devices, security designers can prioritize security equipment use through temporary placements at critical bridge or tunnel locations. A deployment of this type would serve as a temporary security force multiplier capable of alerting responders of a potential security breach. The placement decision would be based on threat information/intelligence or tactical or strategic considerations.

## **Rolling Stock and Vehicle Security**

Transportation vehicle security today comprises two main areas:

- The safety and protection of vehicle passengers or occupants and
- Avoiding the use of the conveyance as a weapon of destruction or mass destruction (WMD).

Regarding the safety and protection of vehicle passengers or occupants, the major potential threats include

- Improvised explosives devices (IEDS),
- Armed assault against the driver or passengers, and
- Chemical, biological, or radiological attack.

The second area (avoiding the use of the conveyance as a WMD) has assumed much greater importance since the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. (Chapter 1 discussed the threat of VBIEDs as a significant area of transportation agency security that deserves prioritization by security planners). Not only must agencies protect against aggressor use of their own supplied vehicles, but also against the commandeering of a vehicle transporting hazardous loads or the conversion of the transportation agencies' own rolling stock.

According to the FTA, lessons learned from prior events suggest that the following security strategies will help protect the vehicle fleet:

- Limit the ability to place or hide explosives on or under vehicles,
- Improve the ability to see into and out of vehicles,
- Reduce the damage that would result from an explosion,
- Reduce the damage that would result from a fire,
- Reduce the damage that would result from contaminants,
- Enhance emergency egress through doors and windows,
- Protect the driver from physical threat,
- Network the vehicle with the Operation Control Center,
- Enable communications between the vehicle operator and passengers, and
- Secure the vehicle from theft/unauthorized operations.

In recognition of these issues, transportation agencies and homeland security professionals from government and industry have sought to improve the security of conveyances while in-transit or when housed or stored at facilities. For example, the short-line freight railroad industry is conducting vulnerability assessments and security planning focused on preventing,

eliminating, reducing, or mitigating the potential use of the freight rail system as a target for terrorism or criminal attack or as a delivery system for a weapon of mass destruction. The program is partially funded by DHS grants under the FY08 Freight Railroad Security Plan (FRSP). The planning is intended to address the presence of Toxic Inhalation Hazards (TIH) materials within high population density areas as well as the following:

- Establishment of secure storage areas for railcars carrying TIH such as chlorine or anhydrous ammonia;
- Expedited movement of railcars carrying TIH materials
- Positive and secure handoff of TIH railcars at points of carrier interchange and points of origination and delivery; and
- Minimization of unattended, loaded tank cars carrying TIH materials.

In regard to passenger safety and security, in 2004 APTA conducted a security-related survey of transit agencies. According to the report, the 120 agencies who participated represented a cross section of transit operators in all modes of transit service, in communities of all sizes, and in all areas of the United States. The agencies surveyed carried 73.2 percent of all transit passenger trips in 2001, provided 71.7 percent of all transit passenger miles of service, and operated 46.8 percent of all transit vehicles.

The most important needs for capital improvement security upgrades identified in the survey were in the following five priority areas: Radio Communications Systems Including Operational Control Redundancy:

- Security Cameras On-Board Vehicles,
- Controlled Access to Facilities and Secure Areas,
- Security Cameras in Stations, and
- AVL Systems.

Table 5-5 provides more detail.

**Table 5-5. 2004 survey of transit agency on capital funding needs.**

Security Measure or Investment	Capital Funding							
	Very Important		Important		Somewhat Important		Not Important	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Automated Vehicle Locator Systems	76	67.9	21	18.8	13	11.6	2	1.8
Radio Communications Systems	96	85.7	12	10.7	2	1.8	2	1.8
Passenger-Operator Intercoms	22	21.6	44	43.1	24	23.5	12	11.8
Security Cameras On-Board Vehicles	82	72.6	23	20.4	5	4.4	3	2.7
Security Cameras in Stations	78	75.0	17	16.3	7	6.7	2	1.9
Public Address Systems On-Board Vehicles	46	42.2	40	36.7	19	17.4	4	3.7
Public Address Systems in Stations	42	42.4	38	38.4	14	14.1	5	5.1
Security Fencing Around Facilities	62	54.4	37	32.5	12	10.5	3	2.6
Chemical/Biological/Radiological Detection Devices	21	19.8	36	34.0	35	33.0	14	13.2
Intrusion Detection Devices	48	42.1	38	33.3	22	19.3	6	5.3
Controlled Access to Facilities and Secure Areas	91	71.1	27	23.7	5	4.4	1	0.9

Source: Adapted from APTA Survey of Transit Agencies, 2004

The need for improved radio communications was the highest rated requirement in the survey, receiving 96.4% in the “very important” and “important” categories. Controlled access to facilities was slightly lower at 94.8%. Although the need for security cameras in stations was listed higher in the “very important category” at 75%, security cameras on board vehicles came in third overall at 93% in the two highest rated categories.

All three of the highest rated needs listed pertain in whole or in part to rolling stock and conveyance security:

- Radio communications with the fleet;
- Controlling access to transit vehicles while in depot, yards, or maintenance facilities; and
- Surveillance capabilities on board vehicles.

One additional highly rated security upgrade requirement listed was AVL systems which scored 86.7% in the survey. As discussed in Chapter 3 (under the category of duress alarms):

The State Transit Authority of Australia has a fleet of 1800 buses in the Sydney and Newcastle area. Every bus is outfitted with Automatic Vehicle Locator (AVL) technology, a driver duress alarm and a microphone that allows Authority central station personnel to hear what is transpiring on-board the vehicle when the driver activates the system.

A 2002 International Transit Studies research effort sponsored by the TRB’s Transit Cooperative Research Program (TCRP) provides further information about security countermeasures currently deployed on passenger buses. The study of Western European systems disclosed the following:

- Widespread use of CCTV cameras,
- Shadowing of en-route buses by security forces,
- Security awareness training for employees,
- Two-way radio communications or mobile phones,
- Emergency alarms,
- Internal and external displays,
- Anti-assault partitions for drivers,
- Double-glazed side windows,
- Driver escape hatches, and
- GPS/AVL systems.

FTA’s *Security Design Considerations* expands on this information and provides additional recommendations, breaking out vehicle types into bus and train. Table 5-6 displays some of this information.

**Table 5-6. Bus security countermeasures.**

<b>Design Consideration</b>	<b>State of Technology Maturity Scale of 1 (least mature) to 5 (most mature)</b>	<b>Cost Scale of 1 (low) to 10 (high)</b>	<b>Retrofit: New Buses / Overhaul / All</b>
<b>1. Networking of bus to operations control center</b>			
Install automatic vehicle locator (AVL) system to allow bus operations to monitor bus location	3 – Has been deployed to various degrees widely. Multiple technologies used to determine location and transmit messages	Range of 6 to 10 – Requires significant investment and support infrastructure. High increment of system maintenance required	All
Install mobile data terminals (MDT) to allow for electronic transmission of messages	3 – Can be integrated into AVL systems. Wide variety of commercial technologies	Range of 4 to 8 – Wide variety of commercial technologies available. Less infrastructure and management	All
Utilize GPS to allow bus operations to track the vehicle location	4 – GPS is widely used and commercially viable. Communication technologies for data transfer must be integrated for command and control	Range of 3 to 10 – Varies based on functionality requirements. From stand-alone units to full system integration	All
Install silent alarm system (panic button) with connection to bus operations, bus destination sign, and police department	5 – Silent alarm features triggered manually are incorporated in most transit system radio systems. Typically linked to on-board exterior signage for emergency alert	Range of 1 to 5 – Has been done in a variety of ways. Simple to do on vehicle; compatible with most communication systems	All
Install CCTV cameras. Cameras can either record for later viewing or broadcasting of sample images live to a control center	5 – Mature technology widely available. Real time transmission of video information is not widely available. Concerns are data management and evidence chain of custody	Range of 3 to 5 – CCTV technology has a relatively low cost if information does not require wireless communication	All
Real time transmission of CCTV data	2 – Currently a number of communication approaches are being used to provide real time transmission of on-board video images to command and security personnel	Range of 8 to 10 – Cost is high since technology is new and firm commercial processes are still under development	All

*(continued on next page)*

Table 5-6. (Continued).

Design Consideration	State of Technology Maturity Scale of 1 (least mature) to 5 (most mature)	Cost Scale of 1 (low) to 10 (high)	Retrofit: New Buses / Overhaul / All
<b>2. Limiting ability to place or hide explosives/Securing compartment doors</b>			
Design compartments (fuel, storage areas, engine, and others) to be protected against unauthorized access	5 – Mature; already available for most applications	Range of 1 to 3 – Various technologies and solutions can be employed	New
Design compartments to be locked by specialized wrench	5 – Commonly used in current production vehicles	Range of 1 to 2 – Cost is nominally different than standard hardware	All
Design compartments to be locked by key	5 – Can be specified on production vehicles	Range of 1 to 3 – Minimal cost differential	All
Reduce or fill spaces that could be used to hide foreign objects	5 – Traditionally included in bus	1 – No cost	New, Overhaul
Install radiological, biological or chemical detector pagers inside bus to detect presence of these materials. The pager could be connected with the OCC	1 to 3 – New technology for this application. Not widely deployed; however, a number of projects and field evaluations are underway	Range of 5 to 10 – Acquisition cost of ownership for these technologies will be significant	All
<b>3. Reducing the damage resulting from a threat (explosion, hijacking, fire, etc.)</b>			
Review fire resistant and fire retardant standards (ASTM E162-02a and E662-03) for interior fixtures	3 – Can be done easily in new vehicles	Range of 1 to 4 – Materials meeting these standards generally have moderate cost increase vs. non-compliant materials	New
Harden exposed wiring and fuel lines	4 – Requires very little development investment	Range of 2 to 6 – Wide range of cost based on various strategies to limit access	New, Overhaul
Install silent alarm system (panic button) with connection to bus operations, bus destination sign, and police department	See item below	See item below	All
Design so that external destination signs and lights are integrated with silent alarm to issue alert of an emergency situation	5 – Already incorporated in base design of electronic signage	1	N/A
Place vehicle number on roof of vehicle to enhance identification from above	5 – Commonly done	1	All

Harden windows to prevent shattering	5 – Typical bus glazing is safety glass or polycarbonate	Range of 1 to 3	New
Provide video surveillance system	4 – Widely available	Range of 6 to 10 – Systems without wireless communications are in wide use; integration with communication system adds significant cost	All
Ensure windows are free from any coverings and provide clear view in/out	5 – Many agencies have banned covering windows with advertising wraps	1– Low	All
<b>4. Isolating the driver from physical threats</b>			
Enclose driver compartment	3 – Deployed to varying degrees	5	All
Provide operator shield	3 – Deployed to varying degrees	5	All
<b>5. Hardening fuel storage compartments</b>			
Harden fuel tanks of alternative fuel vehicles against intentional attack	4 – Most gaseous fuels are contained in roof-mounted storage vessels with limited access	3	New
<b>6. Enhancing emergency egress through doors and windows</b>			
Install emergency door release to allow for manual operation of doors	4	1	All
Improve window release to facilitate easier emergency egress	5	1	New
Strengthen window to be more shatterproof in case of onboard explosion	5	3	New
<b>7. Securing the vehicle from unauthorized operation</b>			
Design ignition system to require a keyed switch in addition to master run switch to start bus	5	1	All
Design ignition system to operate with a smart card technology that only allows permitted users to start and operate bus	5	Range of 3 to 5 – Easily integrated in current vehicle designs	All

Source: Adapted from FTA's *Transit Security Design Considerations*, 2004





## CHAPTER 6

# Homeland Security

Since 2001 all modes of transportation—aviation, maritime, and land-based have experienced a concentration of government efforts on security that is both of major proportion and unparalleled in American history. Understanding their roles as partners with government in the protection of the homeland has required transportation agencies to become familiar with a host of new legislative initiatives, presidential orders, and federal department mandates, regulations, and guidelines. Chapter 6 identifies core components of the federal government’s homeland security protection strategies that focus on surface transportation. The objective of the materials is to familiarize readers with the DHS-driven “national preparedness architecture” that forms the basis for governmental action. The Federal Government, all three branches—executive, legislative, and judicial—has been intensely involved in creating law, policy, procedures, and protocols to safeguard the Nation against homeland security threats. By reviewing some of these activities, in particular those of the executive and legislative branches, that relate to the transportation sector, agencies can obtain a sense of the national strategies and supportive frameworks available to help them in reducing security risks.

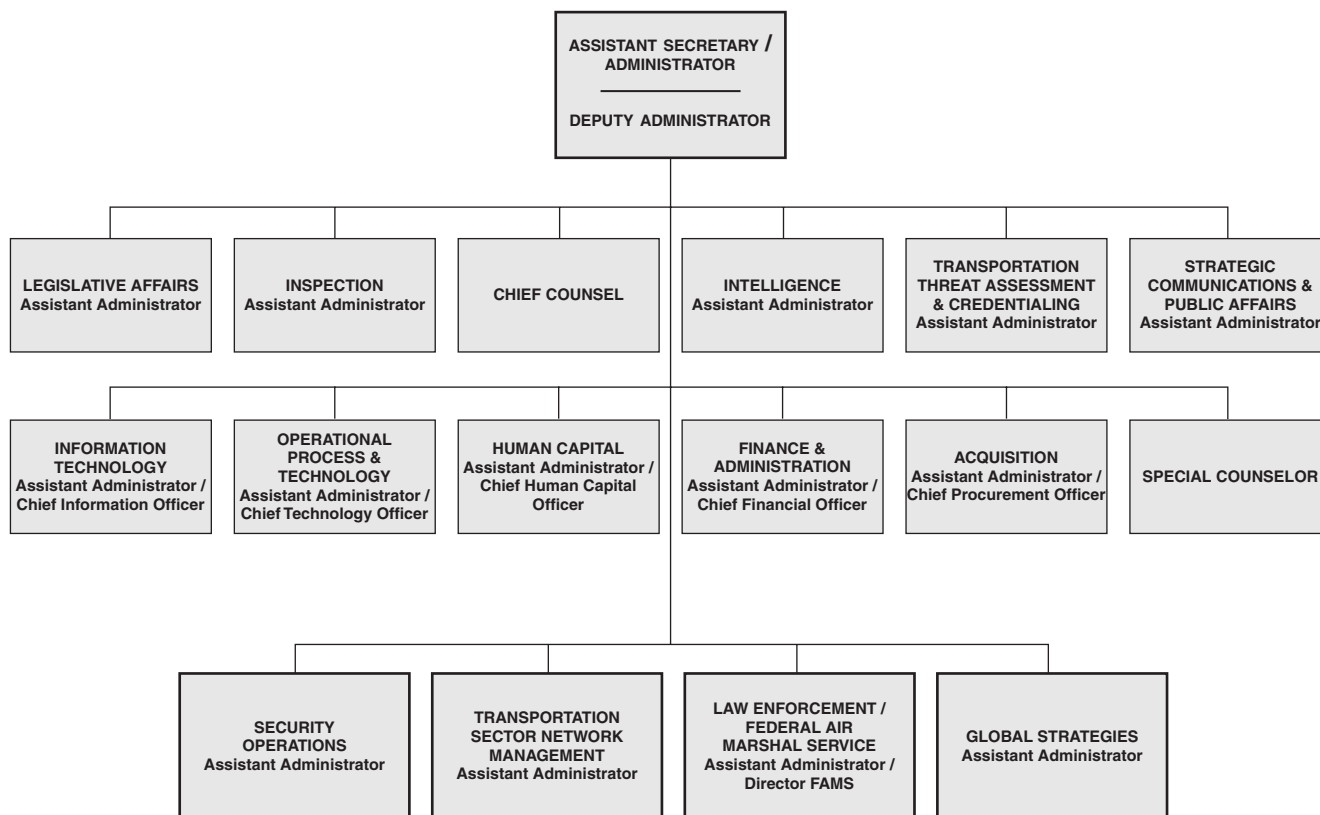
### **Homeland Security Laws and Statutes**

Congress has passed some important laws that relate specifically to transportation. These include the Aviation and Transportation Security Act (ATSA), the Homeland Security Act of 2002, and the Safe Port Security Act. ATSA was signed soon after the terrorist attacks of September 11, 2001, with the goal “to secure the air travel system.” The Act also referenced the security of other modes of transportation. ATSA created the Transportation Security Administration (TSA) under the Department of Transportation. TSA has since been reorganized as an administration under the Department of Homeland Security. Figure 6-1 shows the TSA Organization Chart as of March 20, 2008.

The Homeland Security Act of 2002, a sweeping piece of legislation, established the Department of Homeland Security 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.” The Act created the position of 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 works in the civilian sphere to protect the United States within, at, and outside its borders. Its goal is to prepare for, prevent, and respond to domestic emergencies, particularly terrorism.

The establishment of DHS resulted in a massive reorganization of federal agencies. In total, over 22 federal departments or agencies including FEMA, the Secret Service, the U.S. Coast

## TRANSPORTATION SECURITY ADMINISTRATION



Source: [www.dhs.gov](http://www.dhs.gov)

**Figure 6-1. Transportation Security Administration organization chart, March 20, 2008.**

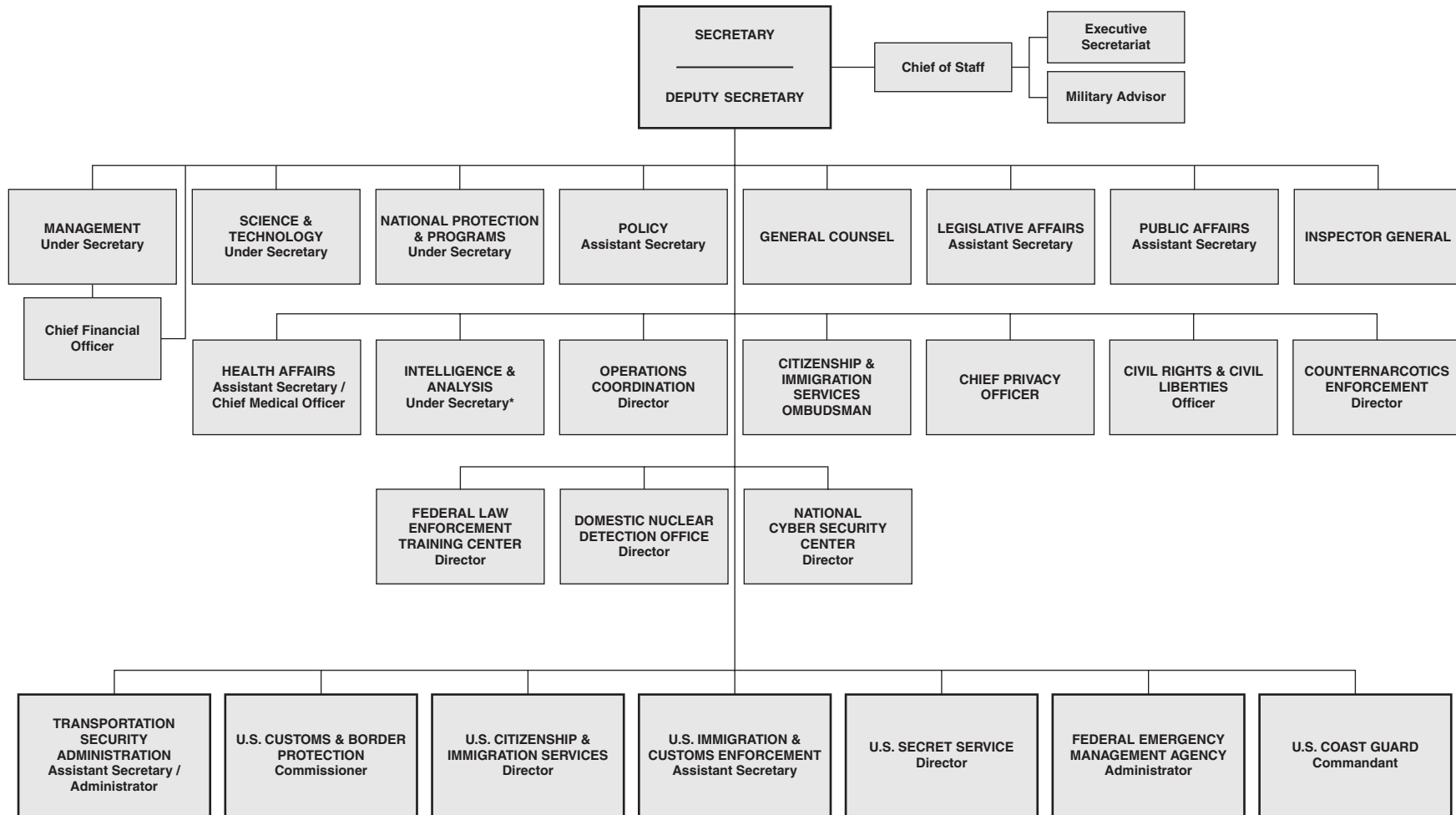
Guard, TSA, and the Immigration and Naturalization Service (INS), were moved under the new department. Title IV of the Act also expressly created the Undersecretary for Border and Transportation Security (BTS) whose primary duties include the following:

- Preventing the entry of terrorists and the instruments of terrorism into the United States;
- Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States;
- 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;
- Ensuring the customs laws of the United States; and
- Ensuring the speedy, orderly and efficient flow of lawful traffic and commerce in carrying out these responsibilities.

Figure 6-2 is a top-level organization chart of DHS current as of 2007.

The Security and Accountability For Every (SAFE) Port Act (signed into law on March 30, 2006) focuses on enhancing security at U.S. ports, preventing threats and attacks before they reach the United States, and the security of shipping containers bound for the United States.

# U.S. DEPARTMENT OF HOMELAND SECURITY



\* Under Secretary for Intelligence & Analysis title created by Public Law 110-53, Aug. 3, 2007  
 Approved 3/20/2008  
 Source: [www.dhs.gov](http://www.dhs.gov)

**Figure 6-2. Department of Homeland Security top level organization chart.**

## Homeland Security Presidential Directives

Presidential Decision Directives (PDDs) and Homeland Security Presidential Directives (HSPDs) are Executive Orders (E.O.s) promulgated by the President of the United States. Prior to the terrorist attacks of September 11, 2001, presidential decisions were communicated by PDD. On October 29, 2001, the first HSPD was signed by President Bush and pronounced as “the first in a series of Homeland Security Presidential Directives that shall record and communicate presidential decisions about the homeland security policies of the United States.” The most significant PDD affecting Homeland Security was PDD-63 issued by President Clinton on May 22, 1998. The intent of PDD-63 was “to assure the continuity and viability of critical infrastructures . . . the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.” All HSPDs, by definition, affect Homeland Security; however, some are more relevant to the protection of the transportation sector than others. Table 6-1 summarizes the purpose of important HSPD Executive Orders that affect transportation.

**Table 6-1. Purpose of HSPD executive orders affecting transportation.**

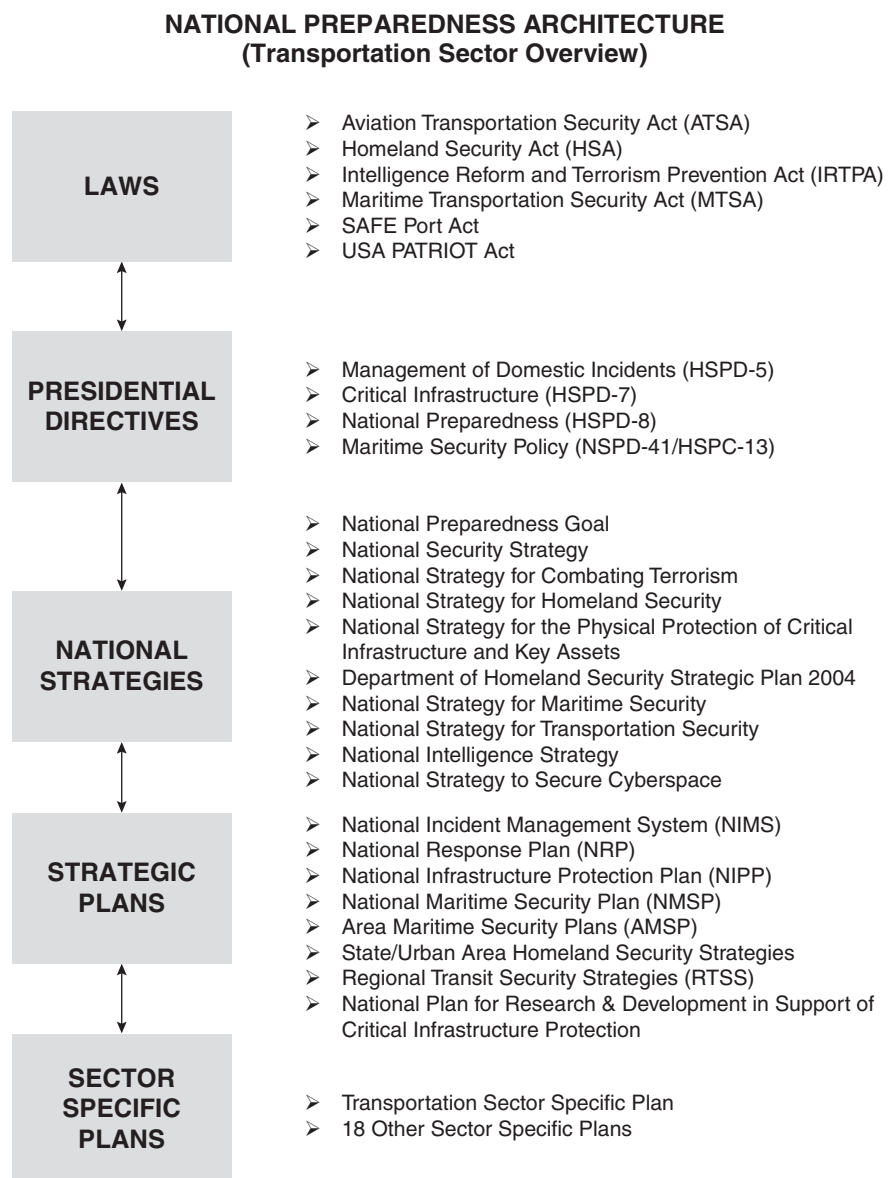
<b>HSPD Exec. Order No.</b>	<b>Purpose</b>
<b>HSPD – 3 (May 22, 2002)</b>  Homeland Security Advisory System	Establishes a Homeland Security Advisory System (HSAS) to provide a comprehensive, effective means to disseminate information on the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases.
<b>HSPD – 5 (Feb 28, 2003)</b>  Management of Domestic Incidents	Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
<b>HSPD – 7 (Dec 17, 2003)</b>  Critical Infrastructure Identification, Prioritization, and Protection	Establishes a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks.
<b>HSPD – 8 (Dec 17, 2003)</b>  National Preparedness	Establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.
<b>HSPD – 13 (Dec 21, 2004)</b>  Maritime Security Policy	Establishes U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests. It directs the coordination of U.S. Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private-sector entities.
<b>HSPD – 16 (Jun 22, 2006)</b>  National Strategy for Aviation Security	Strategies for the prevention of the Air Domain from being exploited by terrorist groups, hostile nations-states, and criminals to commit acts against the United States, its people, its infrastructure and its other interests; safe and efficient use of the Air Domain; and the continued facilitation of travel and commerce.

Source: US Government, the White House

The above-mentioned laws and E.O.s are part of what is known as the federal government's National Preparedness Architecture (NPA). Other significant components important to transportation are as follows:

- National Strategy for Homeland Security,
- National Strategy for Transportation Security,
- National Strategy for Maritime Security,
- National Response Framework,
- National Incident Management System,
- National Infrastructure Protection Plan,
- Regional Transportation Security Strategies, and
- Transportation Sector-Specific Plan.

Figure 6-3 illustrates the five categories of the NPA—Laws, Presidential Directives, National Strategies, Strategic Plans, and Sector Specific Plans. The alignments to the NPA of three other



Source: Adapted from Department of Homeland Security in the 2007 Transit Security Grant Program (TSGP)

**Figure 6-3. Categories of the NPA.**

strategic preparedness components—the National Response Framework (NRF), National Infrastructure Response Plan (NIPP), and the Transportation Specific Sector Plan—are also vitally important to the transportation sector.

## National Response Framework

The NRF (formerly the National Response Plan) identifies the key personnel, roles, responsibilities, and mechanisms for the Nation’s response to incidents. Considered applicable at all levels of government—federal, state, and local—as well as to the private sector, the NRF defines “response” as “save lives, protect property and the environment and meet basic needs.” The NRF builds on the National Incident Management System (NIMS) by outlining how the federal government is organized to support communities and the States in the event of a catastrophic occurrence. Transportation’s role under such circumstances is defined under Emergency Support Functions (ESF) 1. The 15 ESFs are as follows:

1. Transportation
2. Communications
3. Public Works and Engineering
4. Firefighting
5. Emergency Management
6. Mass Care, Emergency Assistance, Housing, and Human Services
7. Logistics Management and Resource Support
8. Public Health and Medical Services
9. Search and Rescue
10. Oil and Hazardous Materials Response
11. Agriculture and Natural Resources
12. Energy
13. Public Safety and Security
14. Long-Term Community Recovery
15. External Affairs

The lead federal agency for ESF#1 is the U.S. Department of Transportation. DOT is responsible for planning and coordinating activities affecting transportation throughout all incident areas—prevention, preparedness, response, recovery, and mitigation. During a national incident, DOT will activate the Crisis Management Center (CMC), which serves as the department’s focal point for emergency response and communications with the National Response Coordination Center (NRCC). DHS’ document *ESF# 1 Transportation Annex* captures information related to the responsibilities and action steps of the various entities and partners under the framework (see Figure 6-4). This includes scope, concept of operations, and policy requirements. The ESF #1 Annex Policies Section is provided as Figure 6-5.

## National Infrastructure Protection Plan

The 2006 National Infrastructure Protection Plan aligns with the National Preparedness Architecture in effect as a plan document designated to bring to life HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection. HSPD-8, National Preparedness is addressed as well in the context of the NIPP being an overarching priority area critically necessary for the Nation to meet its National Preparedness Goal of “helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events to minimize the impact on lives, property and the economy.”

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture <sup>a</sup> Department of Health and Human Services <sup>b</sup>	Agriculture and Food
Department of Defense <sup>c</sup>	Defense Industrial Base
Department of Energy	Energy <sup>d</sup>
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water <sup>e</sup>
Department of Homeland Security <i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
<i>Office of Cybersecurity and Communications</i>	Information Technology Communications
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration United States Coast Guard<sup>f</sup></i>	Transportation Systems <sup>g</sup>
<i>Immigration and Customs Enforcement, Federal Protective Service</i>	Government Facilities <sup>h</sup>

Source: National Infrastructure Protection Plan, 2006

**Figure 6-4. Sector-specific agencies and critical infrastructure/key resources sector.**

The NIPP is also consistent with the Homeland Security Act of 2002 which assigns DHS the responsibility to develop a comprehensive national plan for securing the Critical Infrastructure (CI) and Key Resources (KR) of the United States. Each of the federal departments with responsibilities under the NIPP is a mandatory signatory to a Letters of Agreement that has committed their respective agencies to the following:

- Support NIPP concepts, frameworks, and processes, and carry out their assigned functional responsibilities as appropriate and consistent with their own agency-specific authorities, resources, and programs regarding the protection of CI/KR (Critical Infrastructure)/(Key Resources);
- Work with the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance CI/KR protection;

<b>Emergency Support Function #1 – Transportation Annex</b>
<p><b>Policies</b></p> <p>Primary responsibility for management of incidents involving transportation normally rests with State and local authorities and the private sector, which own and operate the majority of the Nation’s transportation resources. As such, a Federal response must acknowledge State and local transportation policies, authorities, and plans that manage transportation systems and prioritize the movement of relief personnel and supplies during emergencies.</p> <p>The Secretary of Transportation coordinates ESF #1, consistent with DOT’s statutory mission, to promote fast, safe, efficient, and convenient transportation in support of the national objectives of general welfare, economic growth and stability, and the security of the United States.</p> <p>DHS/Federal Emergency Management Agency (FEMA) is responsible for the provision of transportation assets and services (including contracts or other agreements for transportation assistance) for responders, equipment, and goods, consistent with the ESF #7 – Logistics Management and Resource Support Annex.</p> <p>The ability to sustain transportation services, mitigate adverse economic impacts, meet societal needs, and move emergency relief personnel and commodities will hinge on effective transportation decisions at all levels. Unnecessary reductions or restrictions to transportation will directly impact the effectiveness of all prevention, preparedness, response, recovery, and mitigation efforts.</p> <p>Department of Defense (DOD) transportation support will be provided in accordance with Defense Support of Civil Authorities, the memorandum of understanding between DOD and DOT concerning commercial aviation programs, and the memorandum of agreement between DOD and DOT concerning the National Defense Reserve Fleet and the Ready Reserve Force.</p> <p>DOT/Federal Aviation Administration (FAA) is responsible for the operation and regulation of the U.S. National Airspace System, including during emergencies.</p> <p>In cases where State, tribal, and local authorities are overwhelmed, Federal support for mass evacuations is addressed in the Mass Evacuation Incident Annex to the <i>National Response Framework (NRF)</i>. ESF #1 can provide any or all of the activities within the scope of this annex to support the Mass Evacuation Incident Annex.</p> <p>During mass evacuations, consistent with the Mass Evacuation Incident Annex, DHS/FEMA provides transport for persons, including individuals with special needs, provided they meet the following criteria:</p> <ul style="list-style-type: none"> <li>• Evacuees can be accommodated at both embarkation points and at destination general population shelters.</li> <li>• Evacuees can travel on commercial long-haul buses, aircraft or passenger trains, or lift-equipped buses.</li> <li>• Evacuees do not have medical needs indicating that they should be transported by ESF #8 – Public Health and Medical Services.</li> </ul> <p>Consistent with the Mass Evacuation Incident Annex and the Post-Katrina Emergency Management Reform Act, DHS/FEMA is responsible for evacuation of service and companion animals.</p>

**Figure 6-5. ESF #1 Annex Policies Section.**

- Provide annual reports, consistent with HSPD-7 requirements, to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors;
- Coordinate development of Sector-Specific Plans (SSPs) in collaboration with security partners and submit completed SSPs to the Department of Homeland Security within 180 days of final approval of the NIPP. Each SSP will align with the NIPP risk management framework



- and include a menu of sector-specific protective activities and a description of the sector's information sharing mechanisms and protocols;
- Undertake the initiatives and actions outlined in the NIPP Initial Implementation Initiatives and Actions matrix;
  - Develop or modify existing interagency and agency-specific CI/KR plans as appropriate, to facilitate compliance with the NIPP and SSPs;
  - Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations; and
  - Protect critical infrastructure information according to the Protected Critical Infrastructure Information Program or other appropriate guidelines, and share information relevant to CI/KR protection (e.g., actionable information on threats, incidents, and CI/KR status) as appropriate and consistent with their own agency-specific authorities. (NIPP page iii).

The NIPP establishes CI/KR protection roles for certain federal departments and agencies. Figure 6-4 illustrates the sector-specific agency assignments. Footnote 6 of the Table refers directly to the text of HSPD-7, “the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.” The text of the plan at Section 2.2.3 adds additional direction and responsibilities to DOT:

“. . . and is additionally responsible for operating the National Airspace System. DOT and DHS collaborate on regulating the transportation of hazardous materials by all modes (including pipelines).”

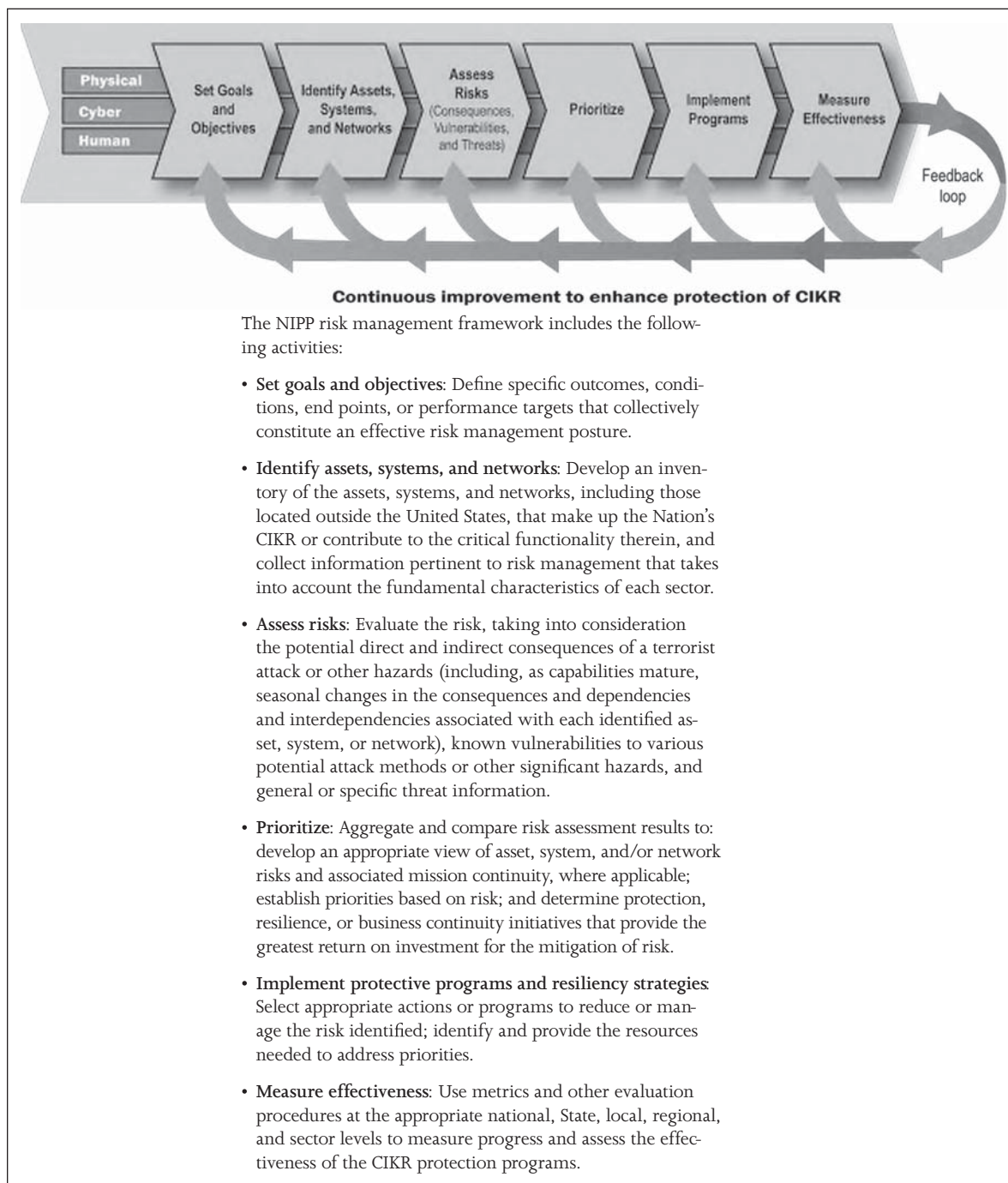
The NIPP also establishes the *NIPP Risk Management Framework* protection program strategy, described as the “cornerstone” of the plan. Figure 6-6 shows the three protection program areas—Physical, Cyber, and Human, as well as the six steps of the process shown as a continuous improvement feedback loop designed to enhance the protection of CI/KR.

## Transportation Systems CI/KR Sector-Specific Plan

Perhaps the most significant NPA component category area for purposes of transportation agency security is the Sector-Specific Plans component. It is known formally as the *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (TSSP)*, published by DHS in May 2007. The main body of the TSSP document contains significant detailed information about the transportation sector, including sector profile data; cross sector dependencies; identification of key federal, state, local, and private security partners; system data regarding assets, networks and functions; risk management and assessment information; security plan development recommendations; and performance measurement parameters for protection program implementation. This information is presented as a transportation sector continuation plan that builds on the content of the NIPP.

The most important planning tools associated with the TSSP exist in its Modal Annexes. Here DHS compartmentalizes federal government homeland security strategy into descriptive, usable elements, by mode at the operations level. There are six Modal Annexes to the TSSP—Aviation, Maritime, Mass Transit (including passenger rail), Highway Infrastructure and Motor Carrier, Freight Rail, and Pipeline.

Each annex contains comprehensive guidance on issues such as communications and information sharing through the Homeland Security Information Network (HSIN), obtaining grant funds for training employees using DHS-approved courses, identifying promising cooperative R&D initiatives for sponsorship, or simply learning about well-proven countermeasures being



Source: National Infrastructure Protection Plan, 2006

**Figure 6-6. Activities included in NIPP risk management framework.**

used in the sector to reduce vulnerabilities or mitigate risks. The subject matter content of each of the Modal Annexes is divided into five subcategories:

- Executive Summary
- Overview of Transportation Mode
  - Vision and Description
  - Coordinating Council Process and Structure

- Implementation Plan
  - Goals and Objectives
  - Programs and Processes
  - Industry Effective Practices
  - Security Guidelines
  - Security Standards and Requirements
  - Compliance and Assessment Processes
  - Grant Programs
  - The Way Forward
- Program Management
- Security Gaps

Figure 6-7, adapted from the Modal Annex for Highway Infrastructure and Motor Carriers:

		Transportation Systems Sector Goals and Objectives												
		Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.	Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.	Goal 1B: Increase the vigilance of travelers and transportation workers.	Goal 1C: Enhance information and intelligence sharing among transportation security partners.	Goal 2: Enhance the resiliency of the U.S. transportation system.	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.	Goal 3: Improve the cost-effective use of resources for transportation security.	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.	Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.	Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
<b>Highway and Motor Carrier Programs</b>	1. FHWA Bridge and Tunnel Vulnerability Workshops		✓	✓		✓	✓	✓						
	2. FHWA Statewide and Project-Specific Vulnerability Assessments		✓	✓		✓	✓	✓		✓				
	3. TSA Security Action Items (SAIs)		✓	✓	✓	✓	✓	✓		✓	✓	✓		
	4. TSA Intercity Bus Security Grant Program (IBSGP)										✓			
	5. TSA Truck Security Grant Program		✓	✓							✓			
	6. FHWA-Supported Security R&D Program		✓				✓							

**Figure 6-7. Information product and associated program, goals and objectives matrix contained in the modal annex for highway infrastructure and motor carriers.**

The chart shows the relationship of each project to the Transportation Systems Sector goals and objectives.

		Transportation Systems Sector Goals and Objectives												
		Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.	Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.	Goal 1B: Increase the vigilance of travelers and transportation workers.	Goal 1C: Enhance information and intelligence sharing among transportation security partners.	Goal 2: Enhance the resiliency of the U.S. transportation system.	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.	Goal 3: Improve the cost-effective use of resources for transportation security.	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.	Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.	Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
Highway and Motor Carrier Programs	7. National Cooperative Highway Research Program Project 20-59		✓				✓					✓		
	8. FMCSA and TSA Truck Tracking Security Pilots		✓				✓				✓			
	9. Hazardous Materials Research Involving Security Initiatives		✓								✓			
	10. TSA HAZMAT Driver Background Rulemaking		✓											
	11. FMCSA Hazardous Materials Safety Permit Program		✓				✓							
	12. Security Plans and Training		✓	✓			✓							
	13. FHWA Security Self-Assessment Tool		✓				✓	✓			✓			
	14. TSA Corporate Security Reviews (CSRs)			✓							✓			

Figure 6-7. Continued.

		Transportation Systems Sector Goals and Objectives										
<p>The chart shows the relationship of each project to the Transportation Systems Sector goals and objectives.</p>		<p><b>Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.</b></p> <p><b>Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.</b></p> <p><b>Goal 1B: Increase the vigilance of travelers and transportation workers.</b></p> <p><b>Goal 1C: Enhance information and intelligence sharing among transportation security partners.</b></p> <p><b>Goal 2: Enhance the resiliency of the U.S. transportation system.</b></p> <p><b>Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.</b></p> <p><b>Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.</b></p> <p><b>Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.</b></p> <p><b>Goal 3: Improve the cost-effective use of resources for transportation security.</b></p> <p><b>Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.</b></p> <p><b>Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.</b></p> <p><b>Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.</b></p> <p><b>Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.</b></p>										
		Highway and Motor Carrier Programs	15. TSA Missouri Pilot								✓	
			16. FMCSA Sensitive Security Visits (SSVs) and Security Contact Reviews (SCRs)		✓							✓
			17. FHWA Security and Emergency Management Professional Capacity Building Program			✓						
			18. TSA School Transportation Security Awareness (STSA)	✓	✓							✓

Source: Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan, 2007

Figure 6-7. Continued.

# Annotated Bibliography

## A. Risk Analysis and Asset Evaluation

### **A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection**

American Association of State Highway and Transportation Officials (AASHTO)  
NCHRP Project 20-07/Task 151B, May 2002  
Science Applications International Corporation (SAIC)  
[http://freight.transportation.org/doc/NCHRP\\_B.pdf](http://freight.transportation.org/doc/NCHRP_B.pdf)

This guideline provides state DOTs, including senior officials, mid-level managers, and front-line employees, with information about how to conduct a vulnerability assessment. Three major phases of the process—pre-assessment, assessment, and post-assessment—are identified. These phases are broken into six steps described by the authors as a “straightforward method for examining critical assets and identifying cost-effective countermeasures to guard against terrorism.” Information about the vulnerability assessment methods of both state and federal agencies is included along with illustrative examples.

### **A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection, Appendices A–F**

American Association of State Highway and Transportation Officials (AASHTO)  
NCHRP Project 20-07/Task 151B, May 2002  
Science Applications International Corporation (SAIC)  
[http://security.transportation.org/sites/security/docs/guide-VA\\_Appendices.pdf](http://security.transportation.org/sites/security/docs/guide-VA_Appendices.pdf)

This companion text to the above guideline contains worksheets reproduced from the main document covering: critical asset factors values and scoring, vulnerability factors and scoring, countermeasures identification, and countermeasures cost information. The appendices contain a bibliography that provides state-specific vulnerability assessment information about Arkansas, California, Illinois, Iowa, Maryland, New Mexico, New York, South Carolina, Texas, Virginia, Washington, Washington D.C., and Wisconsin. The appendices also present “illustrative practices” from Iowa, Maryland, New Mexico, Oregon, Texas, and Washington, as well as the FTA, FAA, and DOJ.

### **Bomb Threat Checklist**

Department of the Treasury, Bureau of Alcohol, Tobacco & Firearms  
ATF F 1613.1 (Formerly ATF F 1730.1, which still may be used) (6-97)  
[http://www.state.tn.us/homelandsecurity/bomb\\_checklist.pdf](http://www.state.tn.us/homelandsecurity/bomb_checklist.pdf)

This guidance document provides users with an information-gathering checklist designed to help collect as much information as possible about a threatened bomb detonation.

### **Dirty Bombs—Fact Sheet**

Department of Health and Human Services, Centers for Disease Control and Prevention (CDC)  
July 2003  
<http://www.cdc.gov>

This 3-page guideline describes what a dirty bomb is and the actions that should be taken by people in the event of a possible or actual radiological exposure. The pamphlet also contains reference information about radiation and emergency response and the medical response to radiation exposures.

### **Terrorist “Dirty Bombs”: A Brief Primer**

Jonathan Medalia, Specialist in National Defense Foreign Affairs, Defense, and Trade Division  
CRS Report for Congress, Order Code RS21528, April 1, 2004

This primer provides a concise overview of the technical aspects of radiological dispersion devices (RDDs). RDDs are described in brief, along with information about prevention and response.

### **The Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment Checklist**

Federal Bureau of Investigation (FBI)  
<http://www.cutr.usf.edu/security/reports.htm>

This vulnerability self-assessment checklist is intended to help the transportation organization determine its vulnerability to terrorism and to assist local law enforcement in assessing the overall vulnerability of the community. The checklist provides a worksheet that can be customized to the transportation-specific organization. The worksheet is intended to be a general guide.

### **Federal Bureau of Investigation (FBI) Guide to Concealable Weapons**

Federal Bureau of Investigation (FBI) 2003  
<http://www.cutr.usf.edu/security/reports.htm>

This reference document is a pictorial collection of easily concealable edged weapons collected by the Firearms and Toolmarks Unit of the FBI Laboratory.

### **A Guide to Printed and Electronic Resources for Developing a Cost-Effective Risk Mitigation Plan for New and Existing Constructed Facilities (NISTIR 7390)**

National Institute of Standards and Technology February 2007  
<http://www2.bfml.nist.gov/software/NISTIR7390>

This extensive reference text consists primarily of an annotated bibliography of risk management information. A URL is provided whenever a reference is available in electronic format. In most cases, references are available for free as downloads. In other cases, the URL provides information on how to purchase the reference.

Information headings in the text include the following: Risk Assessment Resources, Guidance Documents and Software, Hazards Data and Man-made Hazards, Risk Management Resources, Guidance Documents and Software Guidance Documents for Estimating Costs and Losses, Mitigation Costs, Event Related Losses, Economic Evaluation Guidance, Software for Estimating Costs and Losses, Economic Tools, Evaluation Methods, Industry Standards, Software for Implementing Industry Standards, Economic Modeling Resources and Analysis Strategies for Treating Uncertainty.

Appendix A provides a Three Step Protocol for Developing a Cost-Effective Risk Mitigation Plan. Appendix B presents a Clearinghouse and list of Web Portals. Appendix C presents an additional annotated bibliography of Policies, Research and Theory.

***NCHRP Report 525: Surface Transportation Security Volume 4—A Self-Study Course on Terrorism-Related Risk Management of Highway Infrastructure***

National Cooperative Highway Research Program 2005

[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rpt\\_525v4.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v4.pdf)

This guideline consists of a self-study course book designed to provide a general background in terrorism threat-related risk management for bridge, tunnel, and other highway infrastructure, contained on a CD-ROM. The materials are derived from the content of workshops developed by the AASHTO Task Force on Transportation Security. The methodology in this course book is based on an updated version of the approach published by AASHTO in the *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. (It is recommended that users of this course book have a copy of the AASHTO Guide and its appendix available as a reference).

The course covers the following topics: Concepts Of Risk Management, Identification Of Critical Asset Factors Through A Consideration Of Terrorism Event Consequences And Application Of These Factors To Assets To Determine The Most Critical Assets, Concepts Of Terrorist Threats And Related Weapons Of Mass Destruction, Identification Of Asset Vulnerability Factors And Application Of Vulnerability Factors To Determine The Relative Vulnerability Of Each Of The Critical Assets, Plotting The Criticality And Vulnerability Scores On A Matrix To Determine Assets With The Highest Priority For Countermeasure Consideration, Identifying The Range Of Potential Countermeasures And Their Applicability To Critical Assets, Identifying Countermeasure Costs, And Application Of Criticality And Vulnerability Assessment Processes To Bridges And Tunnels In Terms Of Program Development.

**Terrorism and Other Public Health Emergencies:  
A Reference Guide for Media**

Department of Health and Human Services September 2005

<http://www.hhs.gov/disasters/press/newsroom/mediaguide/HHSMediaReferenceGuideFinal.pdf>

Although designated primarily as a guide for the communications media, this reference document provides good information about public health-related terrorism risks, threats, and vulnerabilities and how to take countermeasure precautions. Information is included on Biological and Chemical Agents, Radiation Emergencies, Terrorism and the Food Supply, Environmental Testing and Safety, the Role of the Federal Government, Risk Communications during a Terrorist Attack or other Public Health Emergency, and a history of Biological, Chemical, and Radiation Emergencies. Also contained in the guide is a ready reference table depicting the National Response Plan Emergency Support Functions (ESF) 1-15.



## **B. Plans and Strategies**

### **Maintaining Strategic Direction for Protecting America's Transportation System**

American Association of State Highway and Transportation Officials (AASHTO) May 2006  
[https://bookstore.transportation.org/item\\_details.aspx?=377](https://bookstore.transportation.org/item_details.aspx?=377) (available)

This strategy guide defines two critical areas of homeland security for transportation agencies—Critical Transportation Infrastructure Protection and All Hazards Emergency Management Support.

### **National Needs Assessment for Ensuring Transportation Infrastructure Security**

American Association of State Highway and Transportation Officials (AASHTO)  
 NCHRP Project 20-59, Task 5, October 2002  
[www.transportation.org/sites/security/docs/NatlNeedsAssess.pdf](http://www.transportation.org/sites/security/docs/NatlNeedsAssess.pdf)

Three key security-related planning areas were examined in this study:

- Protecting critical mobility assets,
- Enhancing traffic management capabilities, and
- Improving state DOT (Department of Transportation) emergency response capabilities.

The study also addresses important non-security areas, including safety improvements to bridges and tunnels and operational capabilities of the surface transportation network. Security investment guidelines and estimates are provided by the authors.

### **A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents**

American Association of State Highway and Transportation Officials (AASHTO)  
 NCHRP Project 20-07/Task 151A, May 2002  
[http://freight.transportation.org/doc/NCHRP\\_A.pdf](http://freight.transportation.org/doc/NCHRP_A.pdf)

The guidelines contained in this report are designed to take advantage of the expertise of state DOTs at managing emergencies and applying time-tested practices and experiences to the handling of security-related incidents. Special emphasis is placed on the handling of WMD incidents. The guide “recommends building on the existing institutional relationships, roles, plans and procedures, using the all-hazards framework and modifying it when necessary to incorporate appropriate WMD responses, and working closely with the state emergency management agency and others to ensure coordinated responses.”

### **ASIS International Workplace Violence Prevention and Response Guideline**

American Society for Industrial Security 2005  
[www.asisonline.org/guidelines/inprogress\\_published.htm](http://www.asisonline.org/guidelines/inprogress_published.htm)

This guideline provides an overview of general policies, structures, and practices that can be used to prevent threatening misconduct and violence affecting the workplace. It contains definitions of workplace violence and the continuum of acts and behavior, from less severe to more severe, and a classification of workplace violence incidents. The guideline outlines prevention strategies and

procedures for detecting, investigating, managing, and following up on threats or violent incidents that occur in a workplace. The guideline covers the following topics: Workplace Violence—A Broad Concern for Employers; the Need for a Multidisciplinary Response; Preparedness and Prevention; Threat Response and Incident Management; Integrating the Issue of Domestic Violence into Workplace Violence Prevention Strategies; and the Role of Law Enforcement.

### **Handbook for Transit Safety and Security Certification**

Federal Transit Administration November 2002

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=21>

This Handbook provides step-by-step instructions for transit agencies (primary focus is on rail transit) to “self-certify” the safety and security of their systems. The material is organized into two chapters:

Chapter 1—The Basics: Introduces the basic concepts of certification for safety and security

Chapter 2—The Tools: Introduces three tools that support the safety and security certification process: (1) a well-defined project scope, (2) a safety and security certification plan (SSCP), and (3) a 10-step safety and security certification methodology.

Appendices offer additional information on key topics including project life cycle definitions, useful safety and security resources, a resource guide, and a sample design and construction specification form and direction.

### **TSA/FTA Security and Emergency Management Action Items for Transit Agencies**

Transportation Security Administration December 2006

[www.tsa.gov/assets/pdf/mass\\_transit\\_action\\_items.pdf](http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf)

An update to the FTA’s original Top 20 action items list, these action items cover all modes directly operated or contracted by a transit agency (e.g., bus, bus rapid transit, light rail, heavy rail, commuter rail, and paratransit). The 17 SAIs cover a range of areas, including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for Homeland Security Advisory System (HSAS) threat levels, physical security, personnel security, and information sharing.

### **Security and Emergency Management Technical Assistance for the Top 50 Transit Agencies (SEMTAP)**

Federal Transit Administration April 2007

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=540>

This report provides information and feedback regarding the FTA’s security-related technical assistance program conducted over a 4-year period (2002–2006) at the top 50 transit agencies in size in the United States. The scope and purposes of the program were as follows: (1) Review the transit agency’s environment for security and emergency management; (2) Review, analyze, and make recommendations on security documents; (3) Develop methods to enhance security and emergency management procedures and training; (4) Develop and refine counterterrorism tools; (5) Assess training needs and provide technical assistance for training; (6) Develop materials for security briefings and awareness; (7) Provide technical assistance for emergency tabletop exercises and planning for actual drills; and (8) Provide guidance on how to conduct threat and vulnerability assessments (TVAs). The report includes a program background and

summary, the methodology used, findings and results gathered during the technical assistance visits, and a description of the next-generation technical assistance program.

### **Standard Protocols for Managing Security Incidents Involving Surface Transit Vehicles**

Federal Transit Administration 2002

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=54>

This guideline consists of a three-part protocol mainly focused on transit vehicle operators. Part One (Prevention) involves the inspection of transit vehicles, as part of a routine maintenance measure, to prevent the placement of an explosive device or hazardous substance. Part Two (Unknown Substances and Suspicious Packages) addresses operator activities associated with the inspection of a transit vehicle for suspicious packages or devices. Part Three (Response) presents information about the measures to be taken when responding to a verified or highly suspicious event.

### **Implementation Guidelines for 49 CFR Part 659**

Federal Transit Administration March 2006

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=504>

From its authority to condition the receipt of grant funds (49 U.S.C. § 4324(c)), FTA also exercises regulatory authority, administering programs that place safety and security requirements on transit grantees and state agencies. Failure to comply with these requirements can result in the withholding of FTA funds.

In April 2005, FTA amended 49 CFR Part 659 revising the prior rule clarifying sections, and setting forth further specification concerning what the state (State Safety Oversight—SSO) must require to monitor safety and security of rail transit systems. (Appendix A provides a copy of FTA’s revised Rule.) These implementation guidelines have been prepared to assist states and rail transit agencies in developing compliant programs based on the revised FTA Rule.

The guidelines incorporate practices and recommendations from the complement of prior technical assistance tools previously developed for the SSO program, including templates, reports, training workshops, seminars, web-based resources, and previously published documents, such as FTA’s

Implementation Guidelines for State Safety Oversight of Rail Fixed Guideway Systems (1996);  
 Transit Security Handbook (1998);  
 Technical Advisory for the Notification and Investigation of Accidents and Unacceptable Hazardous Conditions (1999);  
 Critical Incident Management Guidelines (1999);  
 Compliance Guidelines for States with New Starts Projects (2000);  
 Hazard Analysis Guidelines for Transit Projects (2000);  
 Keeping Safety on Track brochure series (2000 and 2001);  
 Safety Certification Handbook (2002);  
 Public Transportation System Security and Emergency Preparedness Planning Guide (2003);  
 FTA’s Top 20 Security Action Items Website (2003 and 2004); and  
 Transit Security Design Considerations (2005).

### **FTA 49 CFR Part 659 Reference Guide, Rail Fixed Guideway Systems; State Safety Oversight**

Federal Transit Administration June 2005

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=602>

The *49 CFR Part 659 Reference Guide* has been prepared to support implementation of FTA's revised state safety oversight rule, published in the Federal Register on April 29, 2005. While this guide is targeted for states and oversight agencies, it can also support activities to be undertaken by rail transit agencies. The guide begins by presenting a flow chart that identifies the revised rule's process for program development and implementation. Then, each section of the revised rule is discussed, including requirements and recommendations from FTA.

## **Resource Toolkit for State Oversight Agencies Implementing 49 CFR Part 659**

Federal Transit Administration March 2006

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=642>

This Resource Toolkit is a companion document to FTA's *Implementation Guidelines for 49 CFR Part 659*. It contains a sample "oversight agency program standard and referenced procedures" document that can be tailored by each affected state oversight agency. It also includes sample program requirements that can be adopted by the state oversight agency to support the development of compliant System Safety Program Plans and System Security Plans at rail transit agencies. A sample "certification that the system safety program plan and the system security plan have been developed, reviewed, and approved" is also provided, as well as sample checklists for use by state oversight agencies in reviewing and approving the rail transit agency plans and other submissions.

The Resource Toolkit begins with the sample "Program Standard and Referenced Procedures," which has nine sections:

1. Introduction and Overview
2. System Safety Program Plan Standard
3. System Security Plan Standard
4. Rail Transit Agency Internal Safety and Security Audit Program
5. Hazard Management Process
6. Accident Notification, Investigation and Reporting
7. Three-Year On-site Safety and Security Review
8. Corrective Action Plans
9. Reporting to FTA

Additional references and procedures are provided as appendices:

Appendix A: Authority for the State Oversight Agency

Appendix B: 49 CFR Part 659 (April 29, 2005)

Appendix C: Organization Charts

Appendix D: Rail Transit Agency Safety and Security Points-of-Contact

Appendix E: Program Requirements for Development of a Rail Transit Agency System Safety Program Plan (SSPP)

Appendix F: State Oversight Agency SSPP Review Checklist

Appendix G: Program Requirements for Development of a Rail Transit Agency System Security and Emergency Preparedness Program Plan (SEPP)

Appendix H: State Oversight Agency System Security Program Plan Checklist

Appendix I: Checklist for Reviewing Rail Transit Agency Accident Investigation Reports and Supporting Documentation

Appendix J: Sample Three-Year Safety and Security Review Checklist

Appendix K: Sample Certification that Rail Transit Agency System Safety Program Plan and System Security Plan Have Been Developed, Reviewed, and Approved

## **The Public Transportation System Security and Emergency Preparedness Planning Guide**

Federal Transit Administration January 2003

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=53>

This document is cited in the FTA's *49 CFR Part 659 Reference Guide* as an aid to assist in compliance with mandatory rail transit safety and security requirements pursuant to the Code of Federal Regulations. The 659 Reference Guide states, "to identify the controls in place that address the personal security of passengers and employees, FTA has prepared the Public Transportation System Security and Emergency Preparedness Planning Guide. This guide addressed procedures, plans, training, technology, and a program for reporting and investigating unusual occurrences and incidents. It includes planning templates, and offers recommendations to address new threats in the rail transit environment."

## **Highway Transportation Sector Security Resource Aid and Highway Transportation System Security and Emergency Preparedness Plan (SSEPP) Template**

Highway ISAC and Highway Watch® Program American Trucking Associations, Inc

[www.highwaywatch.com](http://www.highwaywatch.com) (available to members)

This document was created under the auspices of the Highway Watch ISAC program of the American Trucking Association. It contains a "Security Plan Checklist" covering management and accountability, security problem identification, employees and training, audits and drills, document control, access control, and homeland security. The document also contains an "Employee Guide to System Security for Bus Operations." Preventive activities, suspicious activities, responding to and identifying suspicious persons, suspicious packages and devices, suspicious substances, threat and incident response, information gathering, reporting, interior and exterior vehicle inspection, a homeland security advisory system definition, and FTA-recommended HSAS measures are included in the guide. The final section is a stand-alone document "System Security and Emergency Preparedness Plan (SSEP) Template." It is a highway-specific template developed by the Ohio Department of Transportation and the FTA that is modeled directly after the FTA's SSEPP Guide.

## **Survey of United States Transit System Security Needs and Funding Priorities**

American Public Transportation Association (APTA) April 2004

[http://www.apta.com/services/security/documents/security\\_survey.pdf](http://www.apta.com/services/security/documents/security_survey.pdf)

This survey reports the results of information obtained from 120 transit systems regarding their efforts after the terrorist attacks of September 11, 2001, to implement new or enhanced security measures. It includes information about needs and funding priorities, categories of transit agency security personnel, transit agency security actions and expenditures, new and augmented transit agency security measures, security funding shortfalls, and transit agency security priorities for federal funding.

## **Crime Prevention Through Environmental Design Principles**

The Peel CPTED Advisory Committee 2006

<http://www.peelregion.ca/planning/cpted/CPTED-2006.pdf>

This document is composed of both a theoretical overview and a practical concept guide. It describes the underlying objective of CPTED, which is to help businesses and industry to improve security and reduce crime and losses through the use of design principles and strategies. The document discusses concepts of natural surveillance, natural access control, territorial reinforcement, space assessment and design, signage, grounds, and building interiors and exteriors. Special attention is given to parking structures, garages, elevator vestibules and stairwells, automated bank machines, and schools.

### **Crime Prevention Through Environmental Design (CPTED) Guidebook**

National Crime Prevention Council (NCPC) of Singapore October 2003  
<http://www.npc.gov.sg/pdf/CPTED%20Guidebook.pdf>

This guideline provides an overview of the four fundamental principles of CPTED, Natural Surveillance, Natural Access Control, Territorial Reinforcement, and Maintenance and Management. It describes the methodology for applying these principles through a “3-D approach of Designation, Definition and Design.” A design guide is presented in the form of a checklist that assists users to address the security aspects of a project. The questions contained in the checklist provide the basis for initial crime prevention through environmental design review. Special attention is given to car parks, open spaces and playgrounds, public washrooms, sidewalks and walkways, underpasses and pedestrian overhead bridges, bus shelters, taxi stands, and transit stations.

### **Immediate Actions (IAs) for Transit Agencies for Potential and Actual Life-Threatening Incidents**

Federal Transit Administration April 2004  
<http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/ImmediateActions/PDF/IAs.pdf>

The FTA’s “Immediate Actions” publication is designed “to assist operators and other transit agency personnel who may encounter potential or actual life-threatening events involving criminal activities or terrorism.” The guide contemplates that during emergency or heightened risk situations the transit employee may have only seconds to react to conditions. Immediate Actions (IAs) are identified as “clear procedures that may help prevent or mitigate a terrorist or violent criminal act.”

There are three types of IAs contained in the guideline:

1. Suspicious Activity IAs include suspicious activities or suspicious packages/substances.
2. Imminent Threat and Attack IAs include armed (personal deadly weapons such as firearms, knives, or clubs) threat and attack, explosives threat and attack, and chem/bio threat and attack.
3. Life Safety IAs include lockdown (shelter in place) and evacuation.

### ***NCHRP Report 525: Surface Transportation Security Volume 3—Incorporating Security into the Transportation Planning Process***

National Cooperative Highway Research Program 2005  
[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rpt\\_525v3.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v3.pdf)

The stated purpose of this research was “to assess whether and how traditional transportation planning processes at the state and local levels of government incorporate the potential for security threats and events.” The research team conducted a review of Transportation Improvement Programs of 10 major metropolitan areas and detailed case studies in New York, New York; Portland, Oregon; San Francisco, California; and Washington, DC.

## **Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment**

Federal Highway Administration (FHWA) March 2006  
<http://www.tfhrc.gov/structur/pubs/06072/06072.pdf>

This multi-year strategy report proposes an R&D program addressing highway bridge and tunnel security. It was developed by the FHWA Office of Infrastructure Research and Development (R&D). The report presents a plan to address the agency's objectives to "Support National Disaster Preparedness, and Response and Recovery Efforts" and to "Initiate and Facilitate Research and Technology Development in Support of a More Secure Highway System." The proposed FHWA program focuses on the following strategic area, "to reduce the threat of damage to the infrastructure so that there is minimal loss of life, the infrastructure can stay open for movement of people and goods, and there will be little or no impact on the economy." The recommended strategic focus areas for bridge and tunnel security R&D include Risk and Vulnerability Assessment; System Analysis and Design; Improved Materials, Prevention, Detection, and Surveillance; Post-Event Assessment; Repair and Restoration; and Evaluation and Training.

## **C. Physical Security Countermeasures**

### **Improvised Explosive Device (IED) Safe Standoff Distance Cheat Sheet**

Army National Ground Intelligence Center  
[www.ofm.gov.on.ca/english/Publications/communiques/2007/pdf/2007-26at3.pdf](http://www.ofm.gov.on.ca/english/Publications/communiques/2007/pdf/2007-26at3.pdf)

This table lists threat descriptions for types of high explosives and liquefied petroleum gas (LPG) both butane and propane. It provides building evacuation distances and outdoor evacuation distances based on explosive mass (TNT equivalent) and fireball diameter and safe distance based on LPG mass/volume.

### **Terrorist Bomb Threat Stand-Off Card (Pocket Guide)**

Technical Support Working Group (TSWG)  
[www.tswg.gov](http://www.tswg.gov) (restricted/available upon request)

This chart is intended as a guide for immediate evacuation response to a suspected explosive threat. It lists threat descriptions based on explosives capacity and provides data regarding lethal air blast range, mandatory evacuation distances, and desired evacuation distances.

### **Standard for Closed Circuit Television (CCTV) Inspection, Testing and Maintenance, Volume 6—Signals & Communications**

American Public Transportation Association (APTA)  
 RT-S-SC-012-03, Copyright © 2004

This standard provides procedures for inspecting, testing, and maintaining rail transit Closed-circuit television (CCTV) systems installed in stations or at other fixed locations. It is not applicable to vehicle-mounted CCTV systems.

### **Standard for Wayside Intrusion Detection System Inspection and Testing**

American Public Transportation Association (APTA)  
 RT-S-SC-044-03, Copyright © 2004

This standard provides procedures for inspecting and testing rail transit wayside intrusion detection systems at the time of placement in service, or when modified or repaired.

## **United States Army Physical Security Manual**

HQ TRADOC, Department of the Army

FM No. 3-19.30, January 2001

<http://www.globalsecurity.org/military/library/policy/army/fm/3-19-30/index.html>

This physical security operations manual contains information, standards, and guidelines designed to “minimize the loss of personnel, supplies, equipment, and material through both human and natural threats.” The manual supports the development of a systems approach to security through the use of integrated protective measures. The manual is organized into a series of chapters and appendices that contain mutually supporting information designed to prevent gaps or overlaps in responsibilities and performance. The Army Field Manual (FM) covers

- Physical protective measures, including barriers, lighting, and electronic security systems.
- Procedural security measures, including procedures in place before an incident and those employed in response to an incident. (These include procedures employed by asset owners and those applied by and governing the actions of guards.)
- Terrorism counteraction measures that protect assets against terrorist attacks.

## **Basic Security 101—Alarm Systems**

Digital Security Controls, Ltd/Tyco/Fire & Security

[www.dsc.com](http://www.dsc.com) <http://www.alarmsbc.com/pdf/basic%20security%20101.pdf>

This informative PowerPoint guide provides an overview of the basic components of an alarm system, the technology behind the equipment, and communications platforms, as well as a primer on fundamental industry terminology. The functionality of input devices such as door/window contacts, glassbreak detectors, gas detectors, hold-up buttons, passive infra-red detectors; and output devices such as indoor and outdoor sirens and multi-colored strobes are described in basic terms.

## **The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-Lines and Networks for Use in Transit Related CCTV Systems**

American Public Transportation Association (APTA)

IT-RP-001-07 V1.2, Copyright © 2007

[www.asis.online.org/guidelines/CCTV\\_TS\\_document\\_JULY07\\_%20IT\\_RP.v1.2.pdf](http://www.asis.online.org/guidelines/CCTV_TS_document_JULY07_%20IT_RP.v1.2.pdf)

This guideline consists of a “technical recommended practice” for the selection of both analog and digital cameras, digital recording, and digital high-speed train lines for use in transit. The document covers CCTV use in security systems in transit-related applications, such as rail cars, buses, depots, and stations. The basic principles and recommendations of this recommended practice are generally applicable to any system using CCTV cameras, digital video recorders, and recording hard drives.

## **Getting the Best Use Out of CCTV in the Railways New and Emerging CCTV Technologies**

Rail Safety and Standards Board, Kingston University, Mott MacDonald and Ipsotek Ltd

Project Reference: 07-T061 (Rserv265Y), July 2003

[www.rssb.co.uk](http://www.rssb.co.uk)

This guideline describes how new and emerging technologies for CCTV systems can assist in deterring, detecting, and prosecuting acts of vandalism on the UK rail network. The review covers automatic video detection and advanced surveillance systems. Technology assessments include



reviews of commercially available IP (Internet Protocol) cameras, wireless cameras, digital video recorders, remote viewing devices, and intelligent surveillance systems. The applicability of technologies to the railway environment is also discussed, and where appropriate “ideal” specifications for a system are included. A particular highlight of this report is the inclusion of “state-of-the-art research in intelligent visual surveillance with application to the railway sector.” Automated visual surveillance is described and the automatic interpretation of scenes based on the information acquired by sensors (CCTV cameras).

### **Handbook of Access Control Technologies**

Space and Naval Warfare Systems Center (SPAWARSYSCEN) Charleston

February 2005

<https://www.dhs-saver.info>

This handbook is a compendium of access control technologies. It provides basic information for any organization seeking to develop, configure, and build an access control system. The four main elements of a system: (1) access control barriers, (2) access control verification or identification equipment, (3) access control panels that control the barriers and (4) the communications structure that connects these elements and connects the system to the reaction elements are described. The handbook addresses access control considerations including operational requirements, performance characteristics, system architecture, and databases of authorized personnel, environmental considerations, alarm assessment, integration, communications, power supply, and costs. Categories of equipment discussed include physical control equipment, tokens and cipher systems, biometric systems, and assistive technologies.

### **Assessing the Impact of CCTV, Home Office Research Study 292**

Martin Gill and Angela Spriggs, Home Office Research, Development and Statistics Directorate

February 2005

<http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>

This exhaustive report evaluates 13 CCTV projects implemented in the UK in a range of contexts, including town centers, city centers, car parks, hospitals, and residential areas. The researchers used statistics to determine the impact of CCTV on the reduction of crime in “intervention areas,” both before and after the installation of CCTV systems and in comparable “control areas.”

### **Physical Security Concepts—Security PACE Book 2**

SimplexGrinnell LP

[www.simplexgrinnell.com/resorcecenter/documents/PACEBook2.pdf](http://www.simplexgrinnell.com/resorcecenter/documents/PACEBook2.pdf)

This coursebook provides a basic set of physical security learning objectives and accompanying course materials covering physical security controls, security design considerations, barriers as a means of access control, preventing interruption of operations, perception as protection, protection scheme guidelines, and lighting application issues.

### **NFPA 730 Guide for Premises Security 2006 Edition**

National Fire Protection Association August 2005

[www.nfpa.org/index.asp](http://www.nfpa.org/index.asp) (there is a charge for this publication)

This edition of NFPA 730 was approved as an American National Standard on August 18, 2005. It provides a detailed description of construction, protection, occupancy features, and practices intended to reduce security vulnerabilities to life and property. NFPA 730 has a companion text,

NFPA 731, “Standard for the Installation of Electronic Premises Security Systems, 2006 edition.” There are also references in the Guidebook to other NFPA standards, guidelines, and recommended practices, as well as ASTM, ANSI/BHMAA, ESNA, SDI, UL, and US ARMY Corps of Engineers standards and publications. The text addresses standards and guidelines related to the following areas: Security Vulnerability Assessment, Exterior Security Devices and Systems, Physical Security Devices, Interior Security Systems, Security Personnel, Security Planning, Educational Facilities, Health Care Facilities, One and Two Story Dwellings, Lodging Facilities, Apartment Buildings, Restaurants, Retail Stores, Office Buildings, Industrial Facilities, Parking Facilities and Special Events.

### **Transit Agency Security and Emergency Management Protective Measures**

Federal Transit Administration November 2006

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=439>

This document was developed by the FTA, in consultation with the Department of Homeland Security’s (DHS) Transportation Security Administration (TSA) and Office of Grants and Training (OGT). It is designed to provide an approach that can be used to integrate a transit agency’s security and emergency management programs with the DHS Homeland Security Advisory System (HSAS). In addition to protective measures responsive to the HSAS threat conditions, this document also provides protective measures to be implemented in the event of an attack or active incident (an actual emergency, which might include a terrorist attack, accident or natural disaster) and during the recovery phase following an incident.

### **Technical Support Working Group (TSWG) Physical Security Guidelines**

Technical Support Working Group

[www.tswg.gov](http://www.tswg.gov) (restricted/available upon request)

The mission of TSWG is to “identify, prioritize, and execute research and development, testing, evaluation, and commercialization efforts that satisfy interagency requirements for physical security technology to protect personnel, vital equipment, and facilities against terrorist attacks.” TSWG publications are “restricted use” mainly to government agencies at the federal, state and local level.

TSWG physical security guidelines include research information in the following areas: Blast Mitigation, Entry Point Screening, Electronic Security Systems, Infrastructure Protection, and Maritime Security. Some of the products developed through the research include: Damage and Injury Card Set, Window Vulnerability Assessment and Design Software, Personnel Screening Guide, Vehicle Inspection Guide (VIG), Advanced Vehicle/Driver Identification System, Railcar Inspection Guide (RIG), Tactical Video Surveillance System, Video Vehicle Surveillance Program, Radio Frequency Weapons Pocket Guide, Assessment of Critical Infrastructure Databases, and Securing SCADA (Supervisory Control and Data Acquisition) Systems.

TSWG conducts security research in a number of additional areas. They include: Blast Effects and Mitigation, Chemical, Biological, Radiological and Nuclear Countermeasures, Explosives Detection, Improvised Device Defeat, Investigative Support and Forensics, Surveillance, Collection and Operations Support, Tactical Operations Support, Training Technology Development, and VIP Protection.

### ***TCRP Report 86 Public Transportation Security: Volume 2—K9 Units in Public Transportation: A Guide for Decisionmakers***

Transit Cooperative Research Program 2002

<http://www.tcrponline.org/bin/publications.pl?category=18>

This Guide offers information about the potential deployment of K9 (canines), principally for explosives detection use in the public transportation environment. Data is reported regarding the survey of 14 transit systems that were either currently deploying K9 or had done so within the previous 5 years. The guide describes a step-by-step methodology for determining the pros and cons of a canine program.

***TCRP Report 86 Public Transportation Security: Volume 4—Intrusion Detection for Public Transportation Facilities Handbook***

Transit Cooperative Research Program 2003

<http://www.tcrponline.org/bin/publications.pl?category=18>

This stated objective of this research was to “develop a handbook for selecting and managing intrusion detection systems (IDS) in the public transportation environment.” It contains technology based information about the applicability of IDS to the full range of transportation facilities including tunnels, bridges, buildings, power stations, transfer stations, rail yards, bus yards, and parking lots, as well as transit vehicles. The Handbook provides comprehensive information on application and implementation of a wide range of Intrusion Detection Systems (IDS) technologies to include, Fencing Systems, Barrier Systems, Lighting Systems, Video Systems, Access Control Systems, Sensor Systems, Identification Systems, Data Fusion, Display and Control Systems, Crisis Management Software, and a number of other systems. Chapter 4 of the Handbook describes the steps in applying and implementing IDS. The text makes excellent use of tables to present comparative information.

***TCRP Report 86 Public Transportation Security: Volume 6—Applicability of Portable Explosive Detection Devices in Transit Environments***

Transit Cooperative Research Program 2004

<http://www.tcrponline.org/bin/publications.pl?category=18>

The stated objective of this research was to “demonstrate the capabilities of existing explosive detection devices (EDDs) in a transit environment, including subways and bus station platforms.” Demonstration teams conducted tests of various portable EDDs onsite at three transit agencies across the United States, evaluating the use of these devices to check suspicious packages.

This research report includes a review of the properties of explosives and the various technologies both in use and emerging that are suitable for portable instrumentation for explosives detection. The technologies discussed are Ion Mobility Spectrometry (IMS), Surface Acoustic Wave (SAW), Electron Capture Detectors, Thermo-Redox Detectors, Amplifying Fluorescent Polymer and Canines.

Test procedures and the results of the demonstrations are reported along with a set of conclusions and recommendations covering Transportability, Reliability of the Units, Throughput, Ease of Use and Training Requirements, Maintenance Costs, Consumables False Positive Alarms, and False Negative Alarms. The costs associated with the tested EDDs are included in the report along with estimated product life cycles.

***TCRP Report 86 Public Transportation Security: Volume 1—Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers***

Transit Cooperative Research Program 2007

<http://www.tcrponline.org/bin/publications.pl?category=18>

The stated objective of this research was to “provide guidance that a public transportation agency may use when considering whether, where, when, and how to introduce a passenger security

inspection program into its operations.” The report is a useful ready reference guide that identifies (1) the most promising types of screening technologies and methods currently in use or being tested, (2) the operational considerations for the deployment of these technologies in land-based systems, (3) the legal precedent that either applies or that should be contemplated in connection with passenger screening activities, and (4) a passenger security inspection policy decision-making model.

The report describes the potential deployment of the following inspections methods in terms of operational feasibility and based on Constitutional, Statutory and Tort Law requirements: Radiation Detection Pagers, Ticket Machine Scanners, Handheld Trace Detectors, Desktop Trace Detectors, Puffer Portals, Magnetometers, Backscatter X-ray Scanners, Z Backscatter Vans, Baggage Scanners, Explosives Detection Canines, Behavioral Assessments, and Visual/Physical Bag Inspections. The result of a survey of Public Transportation Agencies who either use or are contemplating use of passenger screening is also included in the research.

*Transit Cooperative Research Program Research Results Digest 58: Safety and Security Issues at All-Bus Systems in Small- to Medium-Sized Cities in Western Europe*

Transit Cooperative Research Program 2003  
[http://www.trb.org/news/blurp\\_detail.asp?id=1460](http://www.trb.org/news/blurp_detail.asp?id=1460)

This research was performed under the auspices of the International Transit Studies Program (ITSP). The program arranges for teams of public transportation professionals to visit exemplary transit operations in other countries. Each study mission focuses on a theme that encompasses issues of concern in public transportation. The purpose of the mission was to learn what other agencies are doing to ensure the safety of bus riders, agency employees, and the communities served—how they deal with security threats that include firebombs, riots, hijackings, kidnapping, vandalism, armed assaults, and bombings. Over a 2-week period, the study team members met with staff members from nine public agencies and operating companies in Belfast, Northern Ireland; Manchester, Liverpool, and Sheffield, England; and Lyon, Grenoble, Bordeaux, and Toulouse, France.

The mission focused on the four subject areas:

1. Prevention activities—what the agency does to reduce or eliminate threats.
2. Preparation activities—how the agency develops plans to respond to crises/incidents.
3. Response activities—what the agency would do, should a crisis occur, to save lives, protect property, and stabilize the situation.
4. Recovery activities—once a crisis has been stabilized, how the agency would return their system operations to normal.

### **Advanced Lighting Guidelines**

New Buildings Institute Incorporated 2003  
[http://www.newbuildings.org/downloads/ALG\\_2003.pdf](http://www.newbuildings.org/downloads/ALG_2003.pdf)

This comprehensive 445-page guideline is an A–Z manual that addresses all aspects of lighting. The text is divided into seven broad categories covering Lighting and Human Performance, Lighting Impacts and Policies, Lighting Design Considerations, Applications, Light Sources and Ballast Systems, Luminaries and Light Distribution, and Lighting Controls. The guidelines are intended for use by architects, design build contractors, lighting designers, electrical engineers, electrical designers, lighting educators, students, utility program managers, energy service project managers, government policy analysts, facilities managers, building owners, building financiers, code enforcement officers, and others who make decisions about lighting.

## **D. Personnel**

### **ASIS International Pre-Employment Background Screening Guideline**

American Society For Industrial Security 2006  
[www.asisonline.org/guidelines/inprogress\\_published.htm](http://www.asisonline.org/guidelines/inprogress_published.htm)

This guideline provides employers with an understanding of the fundamental concepts, methodologies and related legal issues associated with the preemployment background screening of job applicants. It contains practical information concerning the value of screening, the importance of the application form, important legal issues and considerations such as the Fair Credit Reporting Act, privacy issues, as well as state laws, rules, and regulations. There is an appendix depicting a sample preemployment background screening flow chart. Additional preemployment background screening resources are listed in a References/Bibliography section of the document.

### **ASIS International Private Security Officer Selection and Training Guideline**

American Society For Industrial Security 2004  
[www.asisonline.org/guidelines/inprogress\\_published.htm](http://www.asisonline.org/guidelines/inprogress_published.htm)

This guideline lists its purpose as “to provide regulating bodies in the United States with consistent minimum qualifications in order to improve the performance of private security officers and the quality of security services.” The Private Security Officer (PSO) Selection and Training Guideline is an in-depth research effort of the American Society for Industrial Security that recommends minimum criteria for the selection and training of all private security officers. It includes definitions of terms and a reference/bibliography. As a part of the study, requirements for private security officers were identified for the following states: Arizona, California, Florida, New York, Oregon, Utah, Virginia, and North Dakota. These states were selected using ratings provided by the Services Employees International Union (SEIU). The Pinkerton’s, “Internal Analysis of all State Regulations for Private Security Officers,” and Westcott Communications Inc.’s, “Private Security Television Network (PSTN) Catalog of Security Officer Training Programs” were also reviewed.

### **Employee Guide to System Security, Observe and Report—Bus Operations**

National Transit Institute (NTI)  
<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, suspicious activity, suspicious packages and devices, suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to System Security, Observe and Report—Bus Maintenance**

National Transit Institute (NTI)  
<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, security sweeps, suspicious activity, suspicious packages and devices,

suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to System Security, Observe and Report—Commuter Bus**

National Transit Institute (NTI)

<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, security sweeps, suspicious activity, suspicious packages and devices, suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to System Security, Observe and Report—Commuter Rail**

National Transit Institute (NTI)

<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, security sweeps, suspicious activity, suspicious packages and devices, suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to System Security, Observe and Report—Heavy Rail**

National Transit Institute (NTI)

<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, security sweeps, suspicious activity, suspicious packages and devices, suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to System Security, Observe and Report—Light Rail**

National Transit Institute (NTI)

<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a pictorial guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with the reporting of an incident, security sweeps, suspicious activity, suspicious packages and devices, suspicious substances, threat and incident response, information gathering and prevention. The guide is produced through funding and support from the FTA.

### **Employee Guide to Preventing Workplace Violence**

National Transit Institute (NTI)

<http://www.safety@nti.rutgers.edu> [www.ntionline.com](http://www.ntionline.com)

This 2-page pocket brochure consists of a guideline and text for transportation employees covering security-related topics. Information is provided to assist employees with reporting workplace violence, recognizing warning signs, dealing with people, dealing with difficult people, dealing with dangerous people, effects of workplace violence, and the recovery process.

### **Sheltering in Place During a Radiation Emergency—Fact Sheet**

Department of Health and Human Services, Centers for Disease Control and Prevention (CDC)  
June 2003  
<http://www.cdc.gov>

This 3-page guideline describes the actions that should be taken by people in the event it is necessary for them to take shelter during a radiological emergency. The pamphlet describes the process of sheltering at home and lists the types of provisions and emergency supplies that should be stored within the designated shelter area.

### **Biological Attack Human Pathogens, Biotoxins, and Agricultural Threats**

National Academy of Sciences 2005  
[www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)

This fact sheet and summary contains a definition for biological attack and provides a concise description of bio-threat agents as listed by the Centers for Disease Control and Prevention (CDC). A table is included in the summary that identifies the “Onset, Health Impacts and Treatments” for bio-threat agents with categories describing “Disease, Incubation Period, Symptoms, Spread, Lethality if Untreated, Persistence of Organism, Vaccine Status and Medical Treatment.” Basic instructions are presented for what people should do to protect themselves during a declared biological emergency.

### **Chemical Attack Warfare Agents, Industrial Chemicals and Toxins**

National Academy of Sciences 2004  
[www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)

This fact sheet and summary contains a definition for chemical attack. A table is included that identifies the four categories of chemical weapons developed for military use, “nerve agents, blister agents, blood agents, and choking agents.” Sarin, VX, Mustard, Lewisite, Hydrogen Cyanide, Cyanogen Chloride and Chlorine Phosgene are described in terms of “odor, persistency, rate of action, signs and symptoms, first aid and decontamination.” Examples of the toxicity levels for both chemical weapons Sarin and Hydrogen Cyanide, and some industrial chemicals including Chlorine, Hydrogen Chloride, Carbon Monoxide, Ammonia, Chloroform and Vinyl Chloride are listed by lethal concentration in parts per million (PPM). Basic instructions are presented for what people should do to protect themselves if indoors or outdoors during a chemical emergency.

### **Radiological Attack Dirty Bombs and Other Devices**

National Academy of Sciences 2004  
[www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)

This fact sheet and summary references Radiological Dispersion Devices (RDD’s aka dirty bombs). It defines “ionizing radiation” including Gamma and X-Rays, Beta Radiation and Alpha Radiation. A chart is contained in the summary that compares radiation exposures (in rems) with doses known to produce near-term health effects. Some of the common radioactive

materials used in society are listed including Cobalt-60, Cesium-137, Iridium-192, Strontium-90, Plutonium-238 and Americium-241. Basic instructions are presented for what people should do to protect themselves in the event of a radiological explosion.

## **Nuclear Attack**

National Academy of Sciences 2004

[www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument](http://www.nae.edu/nae/pubundcom.nsf/weblinks/CGOZ-642P3W?OpenDocument)

This fact sheet and summary contains a definition for nuclear attack and describes the characteristics of a nuclear explosion. The comparative size of explosion in terms of kiloton or megaton yield (explosive energy) is discussed along with a representation of the general patterns of damage; shockwave, thermal (heat) energy, initial radiation zone and lethality, assuming a 10 Kiloton (KT) blast. Basic instructions are presented for what people should do to protect themselves during a nuclear emergency.

## **Cops, Cameras, and Enclosures: A Synthesis of the Effectiveness of Methods to Provide Enhanced Security for Bus Operators**

National Center for Transit Research, University of South Florida

<http://www.nctr.usf.edu/publications.htm>

This synthesis survey reports the results of information obtained from transit agencies describing a variety of techniques used to minimize the possibilities of assault against bus operators and passengers. The survey addressed security countermeasures including the use of panic buttons, automatic vehicle locator (AVL) systems, on-board video surveillance, two-way communications, operator training, cab enclosures, transit crime reporting and police or security officers on-board.

## ***NCHRP Report 525: Surface Transportation Security Volume 1—Responding to Threats: A Field Personnel Manual***

National Cooperative Highway Research Program 2004

[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rpt\\_525v1.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v1.pdf)

This manual consists of a series of draft templates that can be used by a transportation organization to improve security awareness. According to the “Instructions Page” the manual was “inspired by the training material, System Security Awareness for Transportation Employees and Security Incident Management for Transportation Supervisors—Instructor Package, developed by the National Transit Institute (NTI).” The following sections are included in the text: How Terrorists/Criminals Select a Target or a Victim, Potential Targets, What the Terrorist Criminal Needs to Know, Where to Look, What to Look for, How and What to Report, When to Intervene, Potential Actions to Further Improve Security, Sample Reports, and Contact Lists.

## ***NCHRP Report 525: Surface Transportation Security Volume 7—System Security Awareness for Transportation Employees***

National Cooperative Highway Research Program 2005

<http://www.ntionline.com> (CD-ROM available upon request)

This research product consists of a computer-based training (CBT) Program for Transportation Employees that takes approximately two hours to complete. The course materials address employee security awareness activities; define system security, threat, vulnerability and risk; provide the FBI’s definition of Terrorism; identify types of terrorists and the type of terrorist weapons deployed; provide information about the HSAS advisory system; and describe critical transportation assets at risk. The training also includes a six-step process for approaching a



person exhibiting signs of suspicious behavior and guidelines for handling suspicious telephone calls, persons, packages or vehicles on transportation property A “DECIDE Model” for reacting to a potential threat or incident and “Life Safety Don’ts” are used to reinforce the training objectives.

There are six Modules to the training:

1. What Is System Security?
2. What Is Your Role In Reducing Vulnerability?
3. What Is Suspicious Activity?
4. What Is A Suspicious Object?
5. What Is Your Top Priority?
6. What Are You Doing To Prepare?

## **E. Communications and Information Management**

### **Standard for Emergency Signage for Egress/Access of Passenger Rail Equipment**

American Public Transportation Association (APTA)  
SS-PS-002-98, Rev. 2, Copyright © 2002

This standard contains minimum requirements for the physical characteristics, informational content, and placement of emergency signs and markings for passenger rail car egress/access points on both the interior and exterior of said equipment.

### **Standard for Passenger Railroad Emergency Communications**

American Public Transportation Association (APTA)  
SS-PS-001-98, Copyright © 1998

This standard establishes the minimum criteria for the provision and use of on-board communications systems for railroad operating personnel with particular focus on communications in the event of an emergency.

### **ASIS International Information Asset Protection Guideline**

American Society For Industrial Security 2007  
[www.asisonline.org/guidelines/inprogress\\_published.htm](http://www.asisonline.org/guidelines/inprogress_published.htm)

This guideline provides information about developing and implementing a comprehensive risk-based strategy for information assets protection. Topics covered include (1) classifying and labeling information, (2) handling protocols to specify use, distribution, storage, security expectations, declassification, return, and destruction/disposal methodology, (3) training, (4) incident reporting and investigation, and (5) audit/compliance processes and special needs (disaster recovery). The Guideline is applicable to all sizes of organizations and all industry sectors to include non-profits, educational institutions, and government agencies. Appendices to the guide present users with a framework and principles for developing policy including an actual sample IAP policy. There is also a Quick Reference Guide and a sample flow chart for assessing information protection needs.

### ***TCRP Report 86 Public Transportation Security: Volume 5—Security-Related Customer Communications and Training for Public Transportation Providers***

Transit Cooperative Research Program 2004  
<http://www.tcrponline.org/bin/publications.pl?category=18>

Along with the research text, this guideline consists of a “Security Training and Communications Video” and “Templates of Communications Devices” contained on a CD-ROM computer disk. The materials are designed to assist transportation agencies to communicate effectively about security concerns and other emergencies with three main sets of stakeholders—their passengers, their employees, and other groups. The report is organized into seven sections. Three of these are conceptual. The remaining four chapters provide examples of actual communications methods and devices that public transportation systems of all sizes will find useful in developing or organizing security related communication and/or training.

*NCHRP Report 525: Surface Transportation Security Volume 5—Guidance for Transportation Agencies on Managing Sensitive Information*

National Cooperative Highway Research Program 2005

[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rpt\\_525v5.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v5.pdf)

This guideline provides basic information to assist DO’s in the management of sensitive information. Two elements of the process—Identifying What Kinds of Sensitive Information Needs to Be Protected and Controlling Access—are highlighted in the research. A set of key questions are provided along with a five-step methodology for developing an Information Protection Policy.

## **F. Infrastructure Protection**

### **Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks**

Department of Health and Human Services

Centers for Disease Control and Prevention

National Institute for Occupational Safety and Health, May 2002

DHHS (NIOSH) Publication No. 2002-139

[www.cdc.gov/niosh](http://www.cdc.gov/niosh)

This guideline presents building owners and managers with a list of action steps that can be used to enhance occupant protection from an airborne chemical, biological, or radiological (CBR) attack. The intended audience includes building owners, managers, and maintenance personnel of public, private, and governmental buildings, including offices, laboratories, hospitals, retail facilities, schools, transportation terminals, and other public venues. Higher risk facilities including subway systems are identified as beyond the scope of the guide.

### **Standard Guide for Developing a Cost-Effective Risk Mitigation Plan for New and Existing Constructed Facilities: E 2506—06**

ASTM Committee on Standards, Copyright © 2006 ASTM International

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

This guide describes a generic framework for developing a cost-effective risk mitigation plan for new and existing constructed facilities—buildings, industrial facilities, and other critical infrastructure. This guide provides owners and managers of constructed facilities, architects, engineers, constructors, other providers of professional services for constructed facilities, and researchers an approach for formulating and evaluating combinations of risk mitigation strategies. This guide is under the jurisdiction of ASTM Committee E06 on Performance of Buildings and is the direct responsibility of Subcommittee E06.81 on Building Economics.

## **Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings FEMA 426**

Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)  
December 2003

<http://www.fema.gov/plan/prevent/rms/rmsp426>

This 420-page manual is a “how to” guide for protecting high-occupancy buildings and the people who occupy them from terrorist attacks. It is intended to provide an understanding of risk, threat, vulnerability and hazard assessment methodologies and security design considerations for the protection of new and existing buildings. The manual provides guidance to the “building science community of architects and engineers” to reduce physical damage to buildings and related infrastructure.

## **Recommendations for Bridge and Tunnel Security**

AASHTO Blue Ribbon Panel on Bridge and Tunnel Security September 2003

[www.fhwa.dot.gov/bridge/security/brp.pdf](http://www.fhwa.dot.gov/bridge/security/brp.pdf)

This report consists of guidelines, tables, charts, figures and recommendations developed by a Blue Ribbon Panel (BRP) of bridge and tunnel experts from professional practice, academia, federal and state agencies, and toll authorities. It contains strategies and practices for deterring, disrupting, and mitigating potential terrorist attacks against bridges or tunnels. The intent of the report is to recommend policies and actions to “reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and socio-political damage.”

The BRP makes overarching recommendations:

- Institutional Recommendations
- Interagency Coordination
- Outreach and Communication
- Clarification of Legal Issues
- Fiscal Recommendations
- New Funding Sources for Bridge/Tunnel Security
- Funding Eligibility Determination
- Technical Recommendations
- Technical Expertise
- Research, Development, and Implementation

## **National Institute of Standards and Technology Final Report on the Collapse of the World Trade Center Towers**

NIST NCSTAR 1. Gaithersburg, MD: NIST, September 2005.

<http://wtc.nist.gov/NISTNCSTAR1CollapseofTowers.pdf>

This is the final report on the National Institute of Standards and Technology investigation of the collapse of the World Trade Center on September 11, 2001. This report describes how the aircraft impacts and subsequent fires led to the collapse of the towers. “The report concludes with a list of 30 recommendations for actions in the areas of increased structural integrity, enhanced fire endurance of structures, new methods for fire resistant design of structures, enhanced fire protection, improved building evacuation, improved emergency response, improved procedures and practices, and evaluation and training.”

## **Best Practices for Safe Mail Handling**

DHS Interagency Security Committee September 2006

This Interagency Security Committee (ISC) document contains suggested information on government mail center operations. It provides a series of security recommendations for low, moderate, and high risk facilities, establishes mail center personnel security procedures and lists protective measures for safe handling of suspicious letters and parcels. The document also contains a quick reference guide for handling bomb, radiological, biological or chemical threats.

## **GSA Facilities Standards for the Public Buildings Service**

General Services Administration March 2005

<http://www.gsa.gov> (available)

The GSA webpage states “The Facilities Standards for the Public Buildings Service establishes design standards and criteria for new buildings, major and minor alterations, and work in historic structures for the Public Buildings Service (PBS) of the General Services Administration (GSA). This document contains policy and technical criteria to be used in the programming, design, and documentation of GSA buildings. The Facilities Standards is a building standard: it is not a guideline, textbook, handbook, training manual or substitute for the technical competence expected of a design or construction professional.”

Chapter 8 of the 365-page document is entitled “Security Design.” It includes sections addressing Planning and Cost, Architecture and Interior Design, Commissioning, New Construction, Existing Construction Modernization, Historic Buildings, Structural Engineering, Mechanical Engineering, Fire Protection Engineering, Electronic Security, and Parking Security.

## **DoD Minimum Antiterrorism Standards for Buildings (Unified Facilities Criteria UFC 4-010-01)**

Department of Defense October 2003

[www.wbdg.org/ccb/DOD/UFC/ufc\\_4\\_010\\_01.pdf](http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf)

This document is issued under the authority of DoD Instruction Number 2000.16, DoD Antiterrorism Standards which requires DoD Components to adopt and adhere to common criteria and minimum construction standards to mitigate antiterrorism vulnerabilities and terrorist threats. This document is mandatory for use by all DoD Components. The stated intent of the standards is “to minimize the possibility of mass casualties in buildings or portions of buildings owned, leased, privatized, or otherwise occupied, managed or controlled by or for DoD. These standards provide appropriate, implementable, and enforceable measures to establish a level of protection against terrorist attacks for all inhabited DoD buildings where no known threat of terrorist activity currently exists.”

Subjects contained in the manual address security issues such as Maximize Standoff Distance, Prevent Building Collapse, Minimize Hazardous Flying Debris, Limit Airborne Contamination, Provide Mass Notification, Controlled Perimeter, Government Vehicle Parking, Levels of Protection, Minimum Standoff Distance, Enhanced Fire Safety and Training. Appendix B, DoD Antiterrorism Standards for New and Existing Buildings contains the actual standards. Appendix C contains additional measures that are not mandatory.

### **DoD Security Engineering Facilities Planning Manual (Draft) UFC 4-020-01**

Department of Defense March 2006

[www.wbdg.org/ndbm/DesignGuid/pdf/Final%20Draft\\_UFC\\_4-020-01.pdf](http://www.wbdg.org/ndbm/DesignGuid/pdf/Final%20Draft_UFC_4-020-01.pdf)

This comprehensive 321 page document is a follow-on draft companion text for use with the DoD Minimum Antiterrorism Standards for Buildings. The stated purpose of the Manual is “to support planning of projects that include requirements for security and antiterrorism. Projects include new construction, existing construction or expeditionary and temporary construction.” The intended users of this manual are “engineering planners responsible for project development and planning teams responsible for developing design criteria for projects.”

### **Designing and Operating Safe and Secure Transit Systems: Assessing Current Practices in the United States and Abroad**

Mineta Transportation Institute College of Business San José State University November 2005

<http://transweb.sjsu.edu/mtportal/research/publications/summary/0405.html>

The abstract filed with this comprehensive study states, “This study contributes to our understanding of transit security by (1) reviewing and synthesizing nearly all previously published research on transit terrorism; (2) conducting detailed case studies of transit systems in London, Madrid, New York, Paris, Tokyo, and Washington, D.C.; (3) interviewing federal officials here in the United States responsible for overseeing transit security and transit industry representatives both here and abroad to learn about efforts to coordinate and finance transit security planning; and (4) surveying 113 of the largest transit operators in the United States. Our major findings include: (1) the threat of transit terrorism is probably not universal—most major attacks in the developed world have been on the largest systems in the largest cities; (2) this asymmetry of risk does not square with fiscal politics that seek to spread security funding among many jurisdictions; (3) transit managers are struggling to balance the costs and (uncertain) benefits of increased security against the costs and (certain) benefits of attracting passengers; (4) coordination and cooperation between security and transit agencies is improving, but far from complete; (5) enlisting passengers in surveillance has benefits, but fearful passengers may stop using public transit; (6) the role of crime prevention through environmental design in security planning is waxing; and (7) given the uncertain effectiveness of transit antiterrorism efforts, the most tangible benefits of increased attention to and spending on transit security may be a reduction in transit-related person and property crimes.”

### **Identification of Cost-Effective Methods to Improve Security at Transit Operating/Maintenance Facilities and Passenger Stations (FTA-FL-26-71054-03)**

Center for Urban Transportation Research, University of South Florida July 2006

[www.cutr.usf.edu/security/documents/UCITSS/UCITSS%20Safety%20Security.pdf](http://www.cutr.usf.edu/security/documents/UCITSS/UCITSS%20Safety%20Security.pdf)

This report provides information regarding the conduct of Asset and Vulnerability Assessment, Threat Assessment, Physical Security Review and Incident Planning and Response. Case studies of “best practices” are included for the Denver Regional Transit District, Washington Metropolitan Area Transit Authority, Charlotte Area Transit System, Massachusetts Bay Transportation Authority, Central Florida Regional Transportation Authority and Bay Area Rapid Transit. Each case study provides an overview of the transit system, a statement of the problem identification and need for innovative security measures, a description of the transit system’s

previous attempts to address the problem, an outline of the proposed solution, a cost-benefit analysis, performance indicators, and lessons learned.

## **Transit Security Design Considerations**

Federal Transit Administration 2004

<http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=356>

This comprehensive 341 page report contains security design guidance for bus vehicles, rail vehicles, and transit infrastructure. The executive summary describes the document as a “compendium of actionable steps from which transit agency staff can select when creating a security strategy.” This document consists of nine chapters and several appendices. The first three chapters are introductory, presenting an overview of considerations associated with securing the transit environment. Chapter 4 details a process for “Developing a Security Strategy” that considers options, evaluates countermeasures, and establishes an implementable security strategy based on the criticality of the agency’s vulnerabilities. The remaining chapters address Access Management, Infrastructure Protection, Transit Vehicles, Communications, and Systems Integration.

Appendices include a (A) Chronology of Terrorist Attacks against Public Transit, (B) Case Studies of Transit Security Initiatives, and (G) Lessons Learned from Transit Communications Emergencies. Appendices also address (C) Performance Measures, (D/E) Vehicle Barriers, and (F) Codes and Standards.

## ***NCHRP Report 525: Surface Transportation Security Volume 12—Making Transportation Tunnels Safe and Secure***

Transit Cooperative Research Program 86/National Cooperative Highway Research Program 525 2006

[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rpt\\_525v12.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v12.pdf)

The stated objective of this research was “to provide safety and security guidelines for owners and operators of transportation tunnels to use in identifying (1) principal vulnerabilities of tunnels to various hazards and threats; (2) potential physical countermeasures; (3) potential operational countermeasures; and (4) deployable, integrated systems for emergency-related command, control, communications, and information.”

As discussed in the preface to the text, there are seven chapters contained in this comprehensive 184-page guideline:

- Chapter 1, “Introduction,” introduces the problems that the project has attempted to solve and the environment of the work.
- Chapter 2, “Hazards and Threats,” describes hazards and threats according to the areas or elements of the tunnel that might be affected, how the hazards and threats might be introduced, the operational and physical vulnerabilities to those hazards and threats, and the damage potential of the hazards and threats.
- Chapter 3, “Case Studies,” provides a chronology of past tunnel disasters that were studied for the project.
- Chapter 4, “Tunnel Elements and Vulnerabilities,” gives basic descriptions of various tunnel types, both by mode of transportation and by construction methodology. The chapter then outlines specific vulnerabilities by describing how and why failures can occur under given safety- and security-related hazards and threats based on characteristics of the tunnel’s structure, as well as the surrounding earth. The chapter also rates the damage potential for road, transit, and rail tunnels in conjunction with a given explosion or fire event.

- Chapter 5, “Countermeasures,” presents tunnel owners or operators with structural and system hazard and threat directories in the form of tables. The user is instructed how to apply these directories to his or her own facility. These tables then reference a list of 50 potential physical and/or operational countermeasures that can be used to improve structural and/or system elements.
- Chapter 6, “System Integration,” provides information on current and proposed integrated systems that may be used to increase the safety and security of a transportation tunnel.
- Chapter 7, “Future Research,” provides recommendations for areas requiring further study and approximate funding costs. The report concludes with a list of references that were cited in the text, a list of additional sources, and a list of abbreviations.

## **G. Homeland Security**

### **Homeland Security Advisory System (HSAS)**

Department of Homeland Security 2002

[www.dhs.gov/xinfo/share/programs/Copy\\_of\\_press\\_release\\_0046.shtm](http://www.dhs.gov/xinfo/share/programs/Copy_of_press_release_0046.shtm)

The Homeland Security Advisory System (HSAS) was created pursuant to Executive Order—Homeland Security Presidential Directive (HSPD) 3. The most well known aspect of the system is: (1) the Color-coded Threat Level System used to communicate with public safety officials and the public at-large. The HSAS Color-coded system is made up of five graduated threat conditions: Severe—Red, High—Orange, Elevated—Yellow, Guarded—Blue, and Low—Green. There are two other parts of HSAS: (2) Homeland Security Threat Advisories that contain actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, state, and local governments, private sector organizations, and international partners; and (3) Homeland Security Information Bulletins that communicate information of interest to the nation’s critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, state, and local governments, private sector organizations, and international partners.

### **The 9-11 Commission Report**

**Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition**

<http://www.gpoaccess.gov/911/pdf/fullreport.pdf>

The Commission’s Final Report provides a full and complete account of the circumstances surrounding the September 11th, 2001, terrorist attacks, including preparedness for and the immediate response to the attacks. It also includes recommendations designed to guard against future attacks.

### **National Infrastructure Protection Plan—Sector Specific Plan Transportation Systems (NIPP)**

Department of Homeland Security May 2007

<http://www.dhs.gov/xlibrary/assets/nipp-sp-transportation.pdf>

The NIPP Sector Specific Plan for Transportation contains a homeland security strategy for the entire transportation network. The plan discusses a “Systems-Based Risk Management (SBRM)” approach to improve the sector’s risk management posture. The strategy focuses upon implementing multiple layers of security. A “Vision Statement for the Transportation Sector—Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties” and “Mission Statement—Continuously improve the risk posture of the Nation’s transportation system” are highlighted in the plan. Annexes are included covering Aviation, Maritime, Mass Transit and Passenger Rail, Highway Infrastructure and Motor Carrier, and Freight Rail.

## **H. Security Technology**

### **The Use of Technology in Preparing Subway Systems for Chemical/Biological Terrorism**

Anthony J. Policastro & Susanna P. Gordon APTA 1999 Rapid Transit Conference Proceedings Paper

<http://www.apta.com/research/info/briefings/documents/policastro.pdf>

Describes technologies that can be put into place in a subway system in an attempt to save lives in case of an incident of biological or chemical terrorism.

### **Biometric Technology and Standards Reference**

National Science and Technology Council (NTSC)

Subcommittee on Biometrics and Identity Management 2007

<http://www.biometrics.gov/Documents/biofoundationdocs.pdf>

This comprehensive 167 page reference document is an introductory on-line downloadable text designed to improve knowledge and understanding of biometric technologies. The document includes the following information: Biometrics FAQ, Biometrics Glossary, Biometrics Overview, Biometrics History, Palm Print Recognition, Fingerprint Recognition, Hand Geometry, Dynamic Signature, Vascular Pattern Recognition, Iris Recognition, Face Recognition, Speaker Recognition, Cross-Cutting Topics, Biometrics Standards, and Biometrics Testing and Statistics. There is an accompanying “Biometrics Technology and Standards Overview” that summarizes the information contained in the reference document.

### **Vulnerability Assessment of the Transportation Infrastructure Relying on Global Positioning System Final Report**

John A. Volpe National Transportation Systems Center, August 2001

<http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-v4.6.pdf>

This document assesses the ways users might be affected by a short- or long-term GPS outage. It recommends steps the user community might take to minimize the impact of such outages.





## APPENDIX B

# Additional Sources of Information

### **A. Risk Analysis and Asset Evaluation**

1. **Vulnerability Assessment of Federal Facilities**, DOJ 1995
2. **FEMA 429, Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings**, DHS December 2003
3. **All Hazards Risk Management Systems Draft Best Practices Standard**, ASIS 2007
4. **Strategic Sector Assessment: (U//FOUO) Potential Terrorist Threat to U.S. Mass Transit Systems**, DHS March 2006
5. **Dirty Bombs Fact Sheet**, United States Nuclear Regulatory Commission March 2003
6. **RAMCAP Framework: Risk Analysis and Management for Critical Asset Protection**, ASME Innovative Technologies Institute May 2006
7. **Suicide Bombing Awareness Guide**, DHS
8. **Homeland Security Mapping Standard Point Symbology for Emergencies Management**, Federal Emergency Management Agency, ANSI INCITS 415-2006
9. **Terrorist Tactics, when Broken Down Vehicles go Boom**, Bureau of Diplomatic Security, Department of State, 2005
10. **Assessment of Highway Mode Security: Corporate Security Review Results**, Transportation Sector Network Management Office, Highway & Motor Carrier Division, Transportation Security Administration May 2006

### **B. Plans and Strategies**

11. **Crime Prevention Through Environmental Design and Community Policing**, National Institute of Justice August 1996
12. **Control of Public Space**, Peter Whent Presentation 1999
13. **Improving Transit Security**, Transportation Research Board 1997
14. **Transit Security Handbook**, FTA May 1998
15. **Critical Incident Management Guidelines**, FTA July 1998
16. **ASIS International Disaster Preparedness Guide**, American Society For Industrial Security, 2003
17. **ASIS International Business Continuity Guideline**, American Society For Industrial Security, 2005
18. **Model Annex for Preparedness and Response to a Radiological Transportation Incident**, Department of Energy Office of Transportation and Emergency Management August 2002
19. **FEMA Emergency Management Guide for Business and Industry**, DHS
20. **FTA Top 20 Security Program Action Items for Transit Agencies: Self-Assessment Checklist**, FTA November 2003

21. **Recommended Emergency Preparedness Guidelines for Urban, Rural, and Specialized Transit Systems**, Urban Mass Transit Administration February 1995 Reprint
22. **Transportation Equity and Emergency Preparedness: A Review of the Practices of State Departments of Transportation, Metropolitan Planning Organizations, and Transit Agencies in 20 Metropolitan Areas**, FTA May 2007
23. **Concept of Operations Plan (CONOPS) for Public Health and Medical Emergencies**, Department of Health and Human Services March 2004
24. **Protecting Passenger Transport Systems from the Threat of Terrorism**, Public Transport International January 2006
25. **Terrorism and the Security of Public Surface Transportation**, Brian Michael Jenkins RAND Corporation April 2004
26. **Terrorism and Rail Security**, Jack Riley RAND Corporation March 2004
27. **NCHRP Report 525: Surface Transportation Security Volume 6—Guide for Emergency Transportation Operations: Resource Guide**, National Cooperative Highway Research Program 2005
28. **NCHRP Report 525: Surface Transportation Security Volume 8—Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies**, Transit Cooperative Research Program 86/National Cooperative Highway Research Program 525 2005
29. **NCHRP Report 525: Surface Transportation Security Volume 10—A Guide to Transportation's Role in Public Health Disasters**, National Cooperative Highway Research Program 2006
30. **NCHRP Report 525: Surface Transportation Security Volume 11—Disruption Impact Estimating Tool—Transportation (DIETT): A Tool For Prioritizing High-Value Transportation Choke Points**, National Cooperative Highway Research Program 2006
31. **TCRP Report 86 Public Transportation Security: Volume 7 Public Transportation Emergency Mobilization and Emergency Operations Guide**, Transit Cooperative Research Program 2005
32. **TCRP Report 54 Management Toolkit for Rural and Small Urban Transportation Systems**, Transit Cooperative Research Program 1999
33. **Legal Research Digest 22 The Case for Searches on Public Transportation**, Transit Cooperative Research Program 2005
34. **Transit Cooperative Research Program Research Results Digest No. 59 A Guide to Public Transportation Security Resources**, Transit Cooperative Research Program 2003
35. **TCRP Synthesis 21 Improving Transit Security**, Transit Cooperative Research Program 1997
36. **TCRP Synthesis 27 Emergency Preparedness for Transit Terrorism**, Transit Cooperative Research Program 1997
37. **CDC Fact Sheet: Chemical Agents: Facts about Sheltering in Place**, Centers for Disease Control & Prevention August 2006
38. **Regional Transportation Operations Collaboration and Coordination, A Primer for Working Together to Improve Transportation Safety, Reliability and Security**, Federal Highway Administration, FHWA-OP-03-008

### **C. Physical Security Countermeasures**

39. **SAVER Summary—Handbook of Access Control Technologies**, Space and Naval Warfare Systems Center (SPAWARSYSCEN) February 2005
40. **SAVER Highlight—Automated Video Surveillance**, Space and Naval Warfare Systems Center (SPAWARSYSCEN) February 2005
41. **Video Surveillance of Public Places, (Problem-Oriented Guides for Police Response Guides Series, Guide No. 4)**, U.S. Department of Justice Office of Community Oriented Policing Services February 2006

42. **Operational Guidelines for the Use of Changeable Message Signs**, North Carolina Department of Transportation July 1995
43. **Selective Screening of Rail Passengers**, Mineta Transportation Institute February 2007
44. **Terrorism Protective Measures Resource Guide**, Office of Preparedness and Homeland Security State of Colorado October 2005
45. **Handbook of Intrusion Detection Sensors—SAVER Summary**, DHS September 2004
46. **Automated Video Surveillance Assessment and Validation Report—SAVER Summary**, DHS March 2007
47. **CCTV Technology—SAVER Highlight**, DHS February 2005
48. **Closed Circuit Television Technology Handbook—SAVER Summary**, DHS June 2006
49. **TCRP Report 86 Public Transportation Security: Volume 3 Robotic Devices: A Guide for the Transit Environment**, Transit Cooperative Research Program 2003
50. **TCRP Report 86 Public Transportation Security: Volume 11 Security Measures for Ferry Systems**, Transit Cooperative Research Program 2006
51. **Security Measures in the Commercial Trucking & Bus Industries, A Synthesis of Security Practice**, Commercial Truck & Bus Safety Synthesis Program, Transportation Research Board 2003
52. **Physical Security Handbook 440-2-H**, Office of Administration Policy & Services, US Geological Survey August 2005
53. **Perimeter Security Sensor Technologies Handbook**, Defense Advanced Research Protection Agency 1997
54. **Physical Security Systems, Inspectors Guide**, Office of Safeguards and Security Evaluations, Department of Energy September 2000

#### **D. Personnel**

55. **Security Awareness and Alertness Training in States' Departments of Transportation**, TRB Annual Meeting CD-ROM, Chen, Nof, Partridge, Varkonyi and Nakanishi January 2006
56. **Guide for the Selection of Biological Agent Detection Equipment for Emergency First Responders Guide 101–04 Volume I and II**, DHS March 2005
57. **Incident Indications and First Responder Concerns—Biological, Chemical Radiological/ Nuclear**, FTA
58. **Guidance for Planning, Conducting and Evaluating Transportation Emergency Preparedness Tabletop Drills and Exercises**, Department of Energy Office of Transportation and Emergency Management August 2002
59. **FEMA Building Design for Homeland Security Instructor Guide (E155)**, DHS January 2004
60. **FEMA Building Design for Homeland Security Student Manual (E155)**, DHS January 2004
61. **Guide on the Special Needs of People with Disabilities for Emergency Managers, Planners and Responders**, National Organization on Disability 2002
62. **49 CFR Parts 1570 and 1572 Security Threat Assessment for Individuals Applying for a Hazardous Materials Endorsement for a Commercial Drivers License; Final Rule**, Transportation Security Administration May 2003
63. **Police Traffic Services in the 21st Century**, National Highway Traffic Safety Administration September 1996
64. **NIMS ICS-100 Fact Sheet**, FEMA March 2007
65. **NIMS ICS-200 Fact Sheet**, FEMA March 2007
66. **NIMS ICS-700 Fact Sheet**, FEMA March 2007
67. **NIMS (National Incident Management System) FEMA 501 DRAFT**, FEMA August 2007
68. **NIMS (National Incident Management System)—National Standard Curriculum Training Development Guidance—FY07**, FEMA March 2007

69. **Worker Training in a New Era: Responding to New Threats**, Department of Health and Human Services NIOSH October 2002
70. **Preparedness Training Assessment Methodologies**, TRB Conference Ernest Ron Frazier Countermeasures Assessment & Security Experts January 22, 2006
71. **What You Should Do To Prepare For and Respond to Chemical, Radiological, Nuclear and Biological Terrorist Attacks**, RAND Corporation 2003
72. **NCHRP Report 525: Surface Transportation Security Volume 9—Guidelines for Transportation Emergency Training Exercises**, Transit Cooperative Research Program 86/ National Cooperative Highway Research Program 525 2006
73. **TCRP Report 86 Public Transportation Security: Volume 10 Hazard and Security Plan Workshop: Instructor Guide**, Transit Cooperative Research Program 2006
74. **FBI Workplace Violence, Issues in Response**, National Center for the Analysis of Violent Crimes, FBI Academy 2004
75. **FBI Advisory, What you Should Do If you Receive a Suspicious Letter or Package**, Department of Justice 2000
76. **Worker Training in a New Era: Responding to New Threats**, National Institute for Occupational Safety and Health, 2007
77. **Table Top Exercise Instructions for Planned Events & Unplanned Incident/Emergencies**, Federal Highway Administration 2007
78. **Intermodal Transportation Safety and Security Issues: Training Against Terrorism**, Journal of Public Transportation, Vol. 8, No. 4, University of Central Florida, 2005
79. **United for a Stronger America, a Safe Workplace is Everyone's Business**, National Crime Prevention Council September 2002
80. **Homeland Security Exercise & Evaluation Program (HSEEP) Vol. 1-3**, Department of Homeland Security February 2007

## **E. Communications and Information Management**

81. **Bus Incident Reporting, Tracking and Analysis System**, National Center for Transit Research, Center for Urban Transportation Research (CUTR) August 2006
82. **Convergence of Enterprise Security Organizations**, The Alliance for Enterprise Security Risk Management (ASIS/ISACA/ISSA) November 2005
83. **Information Technology Security Training Requirements: A Role- and Performance-Based Model (NIST Special Publication 800-16)**, NIST April 1998
84. **Computer Security: Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50)**, U.S. Department of Commerce October 2003
85. **Information Security: Biometric Data Specification for Personal Identity Verification (NIST Special Publication 800-76)**, U.S. Department of Commerce January 2005
86. **Freedom and Information Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security**, Eric Landree RAND Corporation April 2007
87. **Threat of Radio Frequency Weapons to Critical Infrastructure Facilities**, Technical Support Working Group (TSWG) August 2005
88. **Safeguarding Classified and Sensitive But Unclassified Information Reference Booklet for State, Local, Tribal and Private Sector Programs**, DHS May 2005
89. **NCHRP Report 525: Surface Transportation Security Volume 2—Information Sharing and Analysis Centers: Overview and Supporting Software Features**, National Cooperative Highway Research Program 2004
90. **TCRP Report 86 Public Transportation Security: Volume 1 Communication of Threats: A Guide**, Transit Cooperative Research Program 2002

91. **Transit Cooperative Research Program Research Results Digest No. 5 Electronic On-Vehicle Passenger Information Displays (Visual and Audible)**, Transit Cooperative Research Program 1995
92. **Transit Cooperative Research Program Research Results Digest No. 41 Guidelines for Collecting, Analyzing and Reporting Transit Crime Data**, Transit Cooperative Research Program 2001
93. **Fusion Center Guidelines, Developing & Sharing Information and Intelligence in a New Era**, Department of Homeland Security and Department of Justice August 2006

## **F. Infrastructure Protection**

94. **Railcar Inspection Guide**, Technical Support Working Group 2004
95. **A Performance Based Design Methodology for Designing Perimeter Vehicle Barriers using ISC Security Design Criteria**, Applied Research Associates, Inc.
96. **ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects**, ISC May 2001
97. **GSA Protective Design and Security Implementation Guidelines**, General Services Administration
98. **ISC Security Standards for Leased Space**, ISC 2004
99. **GSA Lease Security Standards**, GSA November 2005
100. **FEMA 426 Plan of Instruction Course E155, Building Design for Homeland Security**, DHS March 2004
101. **FEMA 452 Risk Assessment A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings**, DHS January 2005
102. **FEMA 427 Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks**, DHS December 2003
103. **NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition**, National Fire Protection Association 2004
104. **Study On the Feasibility of Organising a Network of Secured Parking Areas for Road Transport Operators On the Trans European Road Network**, European Commission Directorate-General Energy and Transport January 2007
105. **Rail Emergencies Special Report USFA-TR-094**, U.S. Fire Administration and FEMA February 2003
106. **Safe Spaces: Designing for Security and Civic Values (ABSTRACT)**, American Society of Landscape Architects July 2004
107. **Transit Cooperative Research Program Research Results Digest No. 9 Responding to Vandalism of Transit Bus and Rail Vehicle Passenger Windows**, Transit Cooperative Research Program 1996
108. **Measuring the Effects of Built Environment on Bus Stop Crime**, UCLA School of Public Policy & Social Research

## **G. Homeland Security**

109. **FY2007 Homeland Security Grant Program**, Office of Grants & Training
110. **FY2007 Infrastructure Protection Program: Transit Security**, Office of Grants & Training, Department of Homeland Security
111. **FY2007 Infrastructure Protection Program: Transit Security Supplemental Funding**, Office of Grants & Training, Department of Homeland Security
112. **Universal Task List**, Office of State and Local Government Coordination & Preparedness, Department of Homeland Security 2005

113. **C-TPAT Highway Carrier Security Criteria**, Minimum-Security Criteria, Customs & Border Protection, Department of Homeland Security 2006
114. **C-TPAT Rail Carrier Security Criteria**, Minimum-Security Criteria, Customs & Border Protection, Department of Homeland Security 2006
115. **National Strategy for Homeland Security**, Homeland Security Council October 2007
116. **National Strategy for Information Sharing, Successes & Challenges in Improving Terrorism—Related Information Sharing**, Homeland Security Council October 2007
117. **National Response Framework**, FEMA January 2008
118. **National Infrastructure Protection Plan (NIPP)** Department of Homeland Security May 2007

## **H. Security Technology**

119. **A First Responders Guide to Purchasing Personal Radiation Detectors for Homeland Security Purposes**, Environmental Measurements Laboratory DHS November 2004
120. **TCRP Synthesis 38 Electronic Surveillance Technology on Transit Vehicles: A Synthesis of Transit Practice**, Transit Cooperative Research Program 2001
121. **NSTC Policy for Enabling the Development, Adoption & Use of Biometric Standards**, National Science and Technology Council, Subcommittee on Biometrics & Identity Management September 2007



## APPENDIX C

# Acronyms, Abbreviations, and Initialisms

<b>AACE</b>	Association for the Advancement of Cost Engineering
<b>AMA</b>	American Management Association
<b>AAR</b>	After Action Reports
<b>AASHO</b>	American Association of State Highway Officials
<b>AASHTO</b>	American Association of State Highway and Transportation Officials
<b>ABA</b>	American Bus Association
<b>ACE</b>	Automated Commercial Environment
<b>ACE</b>	Assessment of Catastrophic Events Center
<b>ACI</b>	American Concrete Institute
<b>ACLU</b>	American Civil Liberties Union
<b>ADA</b>	Americans with Disabilities Act
<b>ADT</b>	Average Daily Traffic
<b>AED</b>	Automated External Defibrillator
<b>AEL</b>	Authorized Equipment List
<b>AEO</b>	Annual Energy Outlook
<b>AFCESA</b>	Air Force Civil Engineering Support Agency
<b>AFG</b>	Assistance to Firefighters Grant
<b>AFMAN</b>	Air Force Manual
<b>AG</b>	Automated Guideway
<b>AHP</b>	Analytical Hierarchy Process
<b>AHRQ</b>	Agency for Healthcare Research and Quality (part of HHS)
<b>AHU</b>	Air-handling unit
<b>AIA</b>	American Institute of Architects
<b>AIR</b>	Annual Interest Rate
<b>AIS</b>	Automatic Information System
<b>AISC</b>	American Institute of Steel Construction
<b>AL</b>	Argonne National Laboratory
<b>ALFRED</b>	Archival Federal Reserve Economic Database
<b>ALOFT-FT</b>	A Large Outdoor Fire plume Trajectory model - Flat Terrain
<b>ALOHA</b>	Aerial Locations of Hazardous Atmospheres
<b>ALS</b>	Advanced Life Support
<b>AM</b>	Amplitude modulation
<b>AMMTIAC</b>	Advanced Materials, Manufacturing, and Testing Information Analysis Center
<b>AMPTIAC</b>	Advanced Materials and Processes Technology Information Analysis Center
<b>AMS</b>	Committee Area Maritime Security Committee
<b>Amtrak</b>	National Railroad Passenger Corporation
<b>AN</b>	Ammonium Nitrate
<b>ANFO</b>	Ammonium Nitrate and Fuel Oil
<b>ANSI</b>	American National Standards Institute
<b>ANSS</b>	Advanced National Seismic System
<b>AOA</b>	Administration on Aging (part of HHS)
<b>AOC</b>	Architect of the Capitol
<b>AOR</b>	Area of Responsibility
<b>AOR</b>	Authorized Organization Representative
<b>AORA</b>	Areas of Response Assistance

<b>APHIS</b>	Animal and Plant Health Inspection Services
<b>APHL</b>	Association of Public Health Laboratories
<b>API</b>	American Press Institute
<b>APIS</b>	Advanced Passenger Information System
<b>APR</b>	Air Purifying Respirator
<b>APTA</b>	American Public Transportation Association
<b>ARC</b>	American Red Cross
<b>AREMA</b>	American Railway and Engineering and Maintenance-of-Way Association
<b>AREMA</b>	American Railway Engineering and Maintenance Association
<b>AS&amp;E</b>	American Science and Engineering, Inc.
<b>ASCE</b>	American Society of Civil Engineers
<b>ASCOS</b>	Analysis of Smoke Control Systems
<b>ASF</b>	Anti-shatter film
<b>ASHRAE</b>	American Society of Heating, Refrigerating and Air-Conditioning Engineers
<b>ASIS</b>	American Society for Industrial Security
<b>ASME</b>	American Society of Mechanical Engineers
<b>ASOS</b>	Automated Surface Observing System
<b>ASP</b>	Alternative Security Program
<b>ASPR</b>	Assistant Secretary for Preparedness Response (Part of HHS)
<b>ASSE</b>	American Society of Safety Engineers
<b>ASTHO</b>	Association of State and Territorial Health Officials
<b>ASTM</b>	American Society for Testing and Materials
<b>AT/FP</b>	Anti Terrorism Force/Protection Directorate
<b>ATA</b>	American Trucking Associations
<b>ATAP</b>	Anti-terrorism action plan
<b>ATC</b>	Automatic train control
<b>ATF</b>	Bureau of Alcohol, Tobacco, Firearms, and Explosives
<b>ATM</b>	Asynchronous Transfer Mode
<b>ATSA</b>	Aviation and Transportation Security Act
<b>ATSDR</b>	Agency for Toxic Substances and Disease Registry (part of CDC)
<b>ATV</b>	All-terrain vehicle
<b>AUA</b>	American Underground Construction Association
<b>AVL</b>	Automatic Vehicle Locator
<b>AWS</b>	American Welding Society
<b>BART</b>	Bay Area Rapid Transit
<b>BASS</b>	Behavioral Assessment Screening System
<b>BAWS</b>	Biological Aerosol Warning System
<b>BCC</b>	Backup Control Center
<b>BCR</b>	Benefit-to-Cost Ratio
<b>BDG</b>	Bi-Diffractive Grating
<b>BEA</b>	Bureau of Economic Analysis
<b>BEES</b>	Building for Environmental and Economic Sustainability
<b>BFRL</b>	Building and Fire Research Laboratory
<b>BIOAPI</b>	Biometric Application Programming Interface
<b>BJA</b>	Bureau of Justice Assistance
<b>BJS</b>	Bureau of Justice Statistics
<b>BLCC</b>	Building Life-Cycle Cost
<b>BLS</b>	Basic Life Support
<b>BLS</b>	Bureau of Labor Statistics
<b>BMSP</b>	Blast Mitigation Structures Program
<b>B-NICE</b>	Biological, Nuclear, Incendiary, Chemical, and Explosive
<b>BNL</b>	Brookhaven National Laboratory
<b>BOLO</b>	Be On the Look Out
<b>BOMA</b>	Building Owners and Manager's Association
<b>BRT</b>	Bus Rapid Transit
<b>BSIR</b>	Biannual Strategy Implementation Report
<b>BSK</b>	Biological Sampling Kit
<b>BSL</b>	Biosafety Level
<b>BTP</b>	British Transport Police
<b>BTS</b>	Bureau of Transportation Statistics



<b>BW</b>	Biological Warfare
<b>BWIC</b>	Biological Warfare and Incident Characterization System
<b>BZPP</b>	Buffer Zone Protection Program
<b>C/B/R</b>	Chemical/Biological/Radiological
<b>C/E</b>	Controller/Evaluator
<b>c/s</b>	cycle per second
<b>C4</b>	Military explosive mixture of RDX and plasticizer
<b>CA</b>	Chemical Agent
<b>CAD</b>	Computer-aided Design
<b>CAM</b>	Chemical Agent Monitor
<b>CAP</b>	Corrective Action Plan
<b>CAPR</b>	Categorical Assistance Progress Reports
<b>CapWIN</b>	Capital Wireless Integrated Network
<b>CARES</b>	Capital Asset Realignment for Enhanced Services
<b>CARVER</b>	Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability
<b>CATV</b>	Cable television
<b>CBD</b>	Central business district
<b>CBECS</b>	Commercial Buildings Energy Consumption Survey
<b>CBEFF</b>	Common Biometric Exchange Formats Framework
<b>CBMS</b>	Chemical Biological Mass Spectrometer
<b>CBP</b>	Capabilities-Based Planning
<b>CBP</b>	U.S. Customs and Border Protection
<b>CBR</b>	Chemical, Biological, or Radiological
<b>CBRN</b>	Chemical, Biological, Radiological and Nuclear
<b>CBRNE</b>	Chemical, Biological, Radiologic, Nuclear and Explosive
<b>CBRNIAC</b>	Chemical, Biological, Radiological & Nuclear Defense Information Analysis Center
<b>CBS</b>	Central Broadcasting System
<b>CBWNP</b>	Chemical and Biological Weapons Nonproliferation Program
<b>CC</b>	Cable car
<b>CCA</b>	Contamination Control Area
<b>CCB</b>	Construction Criteria Base
<b>CCE</b>	Certified Cost Engineer
<b>CCP</b>	Casualty Collection Point
<b>CCRF</b>	Commissioned Corps Readiness Force (part of PHS)
<b>CCTV</b>	Closed Circuit Television
<b>CCV</b>	Characteristics and Common Vulnerabilities
<b>CCVE</b>	Closed-Circuit Video Equipment
<b>CDC</b>	Centers for Disease Control and Prevention (part of HHS)
<b>CDISS</b>	Centre for Defense and International Security Studies
<b>CDL</b>	Commercial Drivers License
<b>CDLIS</b>	Commercial Driver's License Information System
<b>CDP</b>	Center For Domestic Preparedness
<b>CDRG</b>	Catastrophic Disaster Response Group
<b>CEMP</b>	Certified Emergency Management Plan
<b>CEO</b>	Chief Executive Officer
<b>CEQ</b>	Council on Environmental Quality
<b>CERC</b>	Crisis and Emergency Risk Communications
<b>CESB</b>	Council of Engineering and Scientific Specialty Boards
<b>CFDA</b>	Catalog of Federal Domestic Assistance
<b>CFR</b>	Code of Federal Regulations
<b>CFSAN</b>	Center for Food Safety and Applied Nutrition (part of FDA)
<b>CG</b>	Phosgene
<b>CI/KR</b>	Critical Infrastructure/Key Resource
<b>CIA</b>	Central Intelligence Agency
<b>CIAO</b>	Critical Infrastructure Assurance Office
<b>CIBADS</b>	Canadian Integrated Biological Agent Detection System
<b>CIP</b>	Critical Infrastructure Protection
<b>Cipro</b>	Ciprofloxacin Hydrochloride
<b>CM</b>	Countermeasure
<b>CMC</b>	Crisis Management Center

<b>CMS</b>	Center for Medicare & Medicaid Services (part of HHS)
<b>CMU</b>	Concrete masonry unit
<b>CMV</b>	Commercial motor vehicle
<b>CNG</b>	Compressed Natural Gas
<b>CNS</b>	Center for Nonproliferation Studies
<b>COA</b>	Course of action
<b>COG</b>	Continuity of Government
<b>Comms</b>	Communications
<b>ConOps</b>	Concept of Operations
<b>CONTAM</b>	Contaminant Multizone Modeling Software
<b>CONUS</b>	Continental U.S.
<b>COOP</b>	Continuity of operations
<b>COOP</b>	Continuity of Operations Plan
<b>COPS</b>	Office of Community Oriented Policing Services (DOJ)
<b>COR/COS</b>	Carrier Operated Relay/Carrier Operated Squelch
<b>COSIN</b>	Control Staff Instructions
<b>COSUF</b>	Committee on Operational Safety of Underground Facilities
<b>COTP</b>	Captain of the Port
<b>COTPER</b>	Coordinating Office for Terrorism Preparedness and Emergency Response (Part of CDC)
<b>COTS</b>	Commercial Off The Shelf
<b>CP</b>	Command post
<b>CP</b>	Collective protection
<b>CP</b>	Chemically pure
<b>CPP</b>	Certified Protection Professional
<b>CPR</b>	Cardiopulmonary Resuscitation
<b>CPSC</b>	Consumer Product Safety Commission
<b>CPT</b>	Cone Penetration Test
<b>CPTED</b>	Crime Prevention Through Environmental Design
<b>CPX</b>	Command Post Exercise
<b>CRASAR</b>	Center for Robotic-Assisted Search and Rescue
<b>CREATE</b>	Center for Risk and Economic Analysis of Terrorism Events
<b>CRWG</b>	Comprehensive Review Working Group
<b>CSB</b>	Chemical Safety Board
<b>CSEPP</b>	Chemical Stockpile Emergency Preparedness Program
<b>CSI</b>	Construction Specifications Institute
<b>CSI</b>	Container Security Initiative
<b>CSID</b>	Centralized Scheduling and Information Desk
<b>CSO</b>	Company Security Officer
<b>CSS</b>	Crime and Safety Surveys
<b>CST</b>	Civil Support Team
<b>CTA</b>	Chicago Transit Authority
<b>CTAA</b>	Community Transportation Association of America
<b>CTBSSP</b>	Commercial Truck and Bus Safety Synthesis Program
<b>C-TPAT</b>	Customs-Trade Partnership Against Terrorism
<b>CVSA</b>	Commercial Vehicle Safety Alliance
<b>CW</b>	Chemical Warfare
<b>CWA</b>	Chemical warfare agent
<b>DARP</b>	Damage Assessment and Restoration Program
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>DART</b>	Dallas Area Rapid Transit
<b>DARTS</b>	Durable and Reliable Tunnel Structures
<b>DBT</b>	design basis threat
<b>DCS</b>	Distributed Control Systems
<b>DCS</b>	Deputy Chief of Staff
<b>DCSINT</b>	Deputy Chief of Staff for Intelligence
<b>DCT</b>	Data Collection Tool
<b>DERA</b>	Disaster Preparedness and Emergency Response Association
<b>DFO</b>	Disaster Field Office
<b>DHS</b>	Department of Homeland Security
<b>DI</b>	Directorate of Intelligence

<b>DLA</b>	Defense Logistics Agency
<b>DMAT</b>	Disaster Medical Assistance Team (part of NDMS)
<b>DMORT</b>	Disaster Mortuary Operational Response Team (part of NDMS)
<b>DMZ</b>	Demilitarized Zone (computing)
<b>DNDO</b>	Domestic Nuclear Detection Office
<b>DNI</b>	Director of National Intelligence
<b>DNSC</b>	Defense National Stockpile Center
<b>DNT</b>	Dinitrotoluene A byproduct in TNT product.
<b>DOC</b>	Department of Commerce
<b>DOC</b>	Department Operations Center
<b>DoD</b>	Department of Defense
<b>DoD BSK</b>	Department of Defense Biological Sampling Kit
<b>DOE</b>	Department of Energy
<b>DOI</b>	Department of Interior
<b>DOJ</b>	Department of Justice
<b>DOL</b>	Department of Labor
<b>DOS</b>	Department of State
<b>DOT</b>	Department of Transportation
<b>DP</b>	Damage Potential
<b>DPS</b>	Department of Public Safety
<b>DQ</b>	Division of Global Migration and Quarantine (part of CDC)
<b>DS</b>	Diplomatic Security
<b>DTRA</b>	Defense Threat Reduction Agency
<b>DWG</b>	Drawing
<b>DWI</b>	Disaster Welfare Information
<b>E day</b>	Day an Exercise Begins
<b>E&amp;DCP</b>	Evaluation and Data Collection Plan
<b>EA</b>	Environmental Assessment
<b>EAP</b>	Employee Assistance Program
<b>EAS</b>	Emergency Alert Status or Emergency Alert System
<b>ECBC</b>	Edgewood Chemical Biological Center
<b>ECES</b>	Environmental Cost Element Structure
<b>ECG</b>	Exercise Control Group
<b>ECHOS</b>	Environmental Cost Handling Options and Solutions
<b>ED</b>	Emergency Director
<b>EDCS</b>	Emergency Decontamination Corridor System
<b>EDD</b>	Explosive detection device
<b>EDU</b>	Explosives disposal unit
<b>EER</b>	Exercise Evaluation Report
<b>EERC</b>	Energy Escalation Rate Calculator
<b>EERE</b>	Energy Efficiency and Renewable Energy
<b>EFTS / F</b>	Electronic Fingerprint Transmission Specification (Appendix F)
<b>EGDN</b>	Ethylene glycol dinitrate, taggant for explosives
<b>EIA</b>	Energy Information Administration
<b>EIA</b>	Electronics Industries Association
<b>EIS</b>	Epidemic Intelligence Services (part of CDC)
<b>EIS</b>	Environmental Impact Statement
<b>EM</b>	Emergency manager
<b>EMAC</b>	Emergency Management Assistance Compacts
<b>emf</b>	Electromotive force
<b>EMG</b>	Emergency Management Group
<b>EMI</b>	Electro-Magnetic Interference
<b>EMI</b>	Emergency Management Institute
<b>EMS</b>	Emergency Medical Service
<b>EMT</b>	Emergency Medical Technician
<b>EMT</b>	Emergency Management Team
<b>ENR</b>	Engineering News Record
<b>EO</b>	Executive Order
<b>EOC</b>	Emergency Operations Center
<b>EOC</b>	Emergency Operator Coordinator

<b>EOD</b>	Explosive Ordinance Disposal
<b>EOG</b>	Emergency Operations Group
<b>EOO</b>	Electro Optics Organization, Inc.
<b>EOP</b>	Emergency Operations Plans
<b>EOP</b>	Emergency Operating Procedure
<b>EP&amp;R</b>	Emergency Preparedness and Response Directorate (DHS)
<b>EPA</b>	Environmental Protection Agency
<b>EPCRA</b>	Emergency Planning and Community Right-To-Know Act
<b>Epi-X</b>	Epidemic Information Exchange (part of CDC)
<b>EPM</b>	Exercise Program Manager
<b>EPPC</b>	Emergency Preparedness and Prevention Council
<b>EPRI</b>	Electric Power Research Institute
<b>EPT</b>	Exercise Planning Team
<b>ERDA</b>	Energy Research and Development Administration
<b>ERDEC</b>	Edgewood Research, Development, and Engineering Center (U.S. Army)
<b>ERG</b>	Emergency Response Guidebook
<b>ERP</b>	Emergency Response Plan
<b>ERS</b>	Emergency Response System
<b>ERT-JA</b>	Emergency Response to Terrorism: Job Aid
<b>ESF</b>	Emergency Support Functions
<b>ESI</b>	Estimating Systems Incorporated
<b>EST</b>	Emergency Support Team
<b>ETD</b>	Explosives trace detection
<b>Ethernet</b>	Communication protocol for computing devices
<b>ETL</b>	Engineering Technical Letter
<b>EVALPLAN</b>	Evaluation Plan
<b>EXPLAN</b>	Exercise Plan
<b>FAA</b>	Federal Aviation Administration
<b>FAH</b>	Foreign Affairs Handbook
<b>FAR</b>	Federal Acquisition Regulations
<b>FAS</b>	Freight Assessment System
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communication Commission
<b>FCO</b>	Federal Coordinating Officer
<b>FDA</b>	Food and Drug Administration (part of HHS)
<b>FDEM</b>	Florida Department of Emergency Management
<b>FEMA</b>	Federal Emergency Management Agency
<b>FEMP</b>	Federal Energy Management Program
<b>FERP</b>	Facility Emergency Response Plan
<b>FF</b>	Firefighter
<b>FHWA</b>	Federal Highway Administration
<b>FIC</b>	Field Incident Commander
<b>FICC</b>	Federal Interagency Coordination Council
<b>FIPS</b>	Federal Information Processing Standard
<b>FIRP</b>	Facility Incidence Response Plan
<b>FIT</b>	Fire in Tunnels
<b>FITM</b>	Freeway Incident Traffic Management
<b>FM</b>	Field manual
<b>FMC</b>	Federal Mobilization Center
<b>FMCSA</b>	Federal Motor Carrier Safety Administration
<b>FMFM</b>	Fleet Marine Force Manual
<b>FOIA</b>	Freedom of Information Act
<b>FoodNet</b>	Foodborne Diseases Active Surveillance Network part of CDC)
<b>FOUO</b>	For official use only
<b>FPS</b>	Federal Protective Service
<b>FPS</b>	Frames per second
<b>FRA</b>	Federal Railroad Administration
<b>FRAWG</b>	Federal Risk Assessment Working Group
<b>FRC</b>	Federal Resources Coordinator
<b>FRERP</b>	Federal Radiological Emergency Response Plan

<b>FRF</b>	Fragment retention film
<b>FRP</b>	Facility Response Plan
<b>FRP</b>	Federal Response Plan
<b>FRP</b>	Fiber-reinforced polymer
<b>FRT</b>	Facility Response Team
<b>FS&amp;L</b>	Federal, State, and local
<b>FSA</b>	Facility Security Assessment
<b>FSE</b>	Full-scale exercise
<b>FSIS</b>	Food Safety and Inspection Service (part of USDA)
<b>FSO</b>	Facility Security Officer
<b>FSP</b>	Facility Security Plan
<b>FSR</b>	Financial Status Report
<b>FSRM</b>	Federal Security Risk Management
<b>FTA</b>	Federal Transit Administration
<b>FTE</b>	Full-time employees
<b>FTIR</b>	Fourier Transform Infrared
<b>FY</b>	Fiscal year
<b>G&amp;T</b>	Preparedness Directorate Office of Grants and Training
<b>GAN</b>	Grant Adjustment Notice
<b>GAO</b>	Government Accountability Office
<b>GATT</b>	General Agreement on Tariffs and Trade
<b>GATX</b>	General American Transportation
<b>GB</b>	Sarin
<b>GCC</b>	Government Coordinating Council
<b>GD</b>	Soman
<b>GETS</b>	Government Emergency Telecommunications Service
<b>GFE</b>	Government-furnished equipment
<b>GHz</b>	Gigahertz
<b>GIA</b>	Groupe Islamique Arm (armed Islamic group)
<b>GIS</b>	Geographic Information Systems
<b>GMS</b>	Grants Management System
<b>GPO</b>	Government Printing Office
<b>GPS</b>	Global Positioning System
<b>GSA</b>	General Services Administration
<b>HAN</b>	Health Alert Network (part of CDC)
<b>HAR</b>	Highway Advisory Radio
<b>HAZMAT</b>	Hazardous material
<b>HAZUS</b>	Hazards U.S.
<b>HAZUS-MH</b>	HAZUS Multi-Hazard
<b>HBRRP</b>	Highway Bridge Replacement and Rehabilitation Program
<b>HDER</b>	Homeland Defense Equipment Reuse
<b>HEICS</b>	Hospital Emergency Incident Command System
<b>HEMP</b>	High-Altitude Electromagnetic Pulse
<b>HEPA</b>	High-efficiency particulate air
<b>HEU</b>	Highly enriched uranium
<b>HFC-4310</b>	Decafluoropentane
<b>HHA</b>	Hand-Held Immunochromatographic Assay
<b>HHS</b>	Department of Health and Human Services
<b>H-ISAC</b>	Highway Information Sharing and Analysis Center
<b>HLS</b>	Homeland Security
<b>HMR</b>	Hazardous Material Regulations
<b>HMRT</b>	Hazardous Materials Response Team
<b>HMX</b>	A plastic explosive, also known as octahydro-1,3,5,7-tetranitro-1,3,5,7-tetrazocine
<b>HOV</b>	High-occupancy vehicle
<b>HPAC</b>	Hazard Prediction and Assessment Capability
<b>HPLC-UV</b>	High Performance Liquid Chromatography-Ultraviolet
<b>HPM</b>	High-power microwave
<b>HPPL</b>	High-performance photoluminescent material
<b>HPS</b>	Health Physics Society
<b>HQ</b>	Headquarters

<b>HQUSACE</b>	Headquarters, U.S. Army Corps of Engineers
<b>HRSA</b>	Health Resources and Services Administration part of HHS)
<b>HSA</b>	Homeland Security Act
<b>HSAC</b>	Homeland Security Advisory Council (DHS)
<b>HSAS</b>	Homeland Security Advisory System
<b>HSC</b>	Homeland Security Council (White House)
<b>HSDL</b>	Homeland Security Digital Library
<b>HSEEP</b>	Homeland Security Exercise and Evaluation Program
<b>HSGP</b>	Homeland Security Grant Program
<b>HSIN</b>	Homeland Security Information Network
<b>HSO</b>	Homeland Security Office
<b>HSOC</b>	Homeland Security Operations Center
<b>HSPD</b>	Homeland Security Presidential Directives
<b>HSPTAP</b>	Homeland Security Preparedness Technical Assistance Program
<b>HUMINT</b>	Human intelligence
<b>HUS</b>	Hemolytic uremic syndrome
<b>HV/HR</b>	High-Value/High-Risk
<b>HVAC</b>	Heating, ventilation, and air conditioning
<b>HWP</b>	Highway Watch Program
<b>IA</b>	Information Analysis Division (DHS)
<b>IA/IP</b>	Information Analysis and Infrastructure Protection
<b>IAB</b>	Interagency Board
<b>IACP</b>	International Association of Chiefs of Police
<b>IAEA</b>	International Atomic Energy Agency
<b>IAEM</b>	International Association of Emergency Managers
<b>IAIP</b>	Information Analysis and Infrastructure Protection Directorate (DHS)
<b>IANA</b>	Intermodal Association of North America
<b>IAP</b>	Incident Action Plan
<b>IAs</b>	Immediate actions
<b>IBADS</b>	Interim Biological Agent Detector System
<b>IBC</b>	International Building Code
<b>IBHS</b>	Institute for Business & Home Safety
<b>IBTTA</b>	International Bridge, Tunnel and Turnpike Association
<b>IC</b>	Incident Commander
<b>ICBO</b>	International Conference of Building Officials
<b>ICC</b>	International Code Council
<b>ICE</b>	Integrated Computer Engineering
<b>ICE</b>	Immigration and Customs Enforcement
<b>ICP</b>	Incident Command Post
<b>ICS</b>	Incident Command System
<b>ICT</b>	International Policy Institute for Counter-Terrorism
<b>ICTAP</b>	Interoperable Communications Technical Assistance Program
<b>ID</b>	Identification
<b>ID</b>	Identity
<b>IDS</b>	Intrusion Detection System
<b>IEC</b>	International Electrotechnical Commission
<b>IED</b>	Improvised explosive device
<b>IEDDA</b>	International Explosive Detection Dog Association
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IEMA</b>	Illinois Emergency Management Agency
<b>IESNA</b>	Illuminating Engineering Society of North America
<b>IEST</b>	Institute of Environmental Sciences and Technology
<b>IETF</b>	Internet Engineering Task Force
<b>IFJ</b>	International Federation of Journalists
<b>IG</b>	Inspector General
<b>IHS</b>	Indian Health Service (part of HHS)
<b>IID</b>	Improvised incendiary device
<b>IIMG</b>	Interagency Incident Management Group
<b>IIMS</b>	Integrated Incident Management System
<b>IM</b>	Incident management task

<b>IMC</b>	International Mechanical Code
<b>IME</b>	Institute for Makers of Explosives
<b>IMO</b>	International Maritime Organization
<b>IMS</b>	Ionization/Ion Mobility Spectrometry
<b>IMS</b>	Incident management system
<b>IMT</b>	Incident Management Team
<b>INCITS</b>	InterNational Committee for Information Technology Standards
<b>IND</b>	Investigational New Drug
<b>IND</b>	Improvised Nuclear Device
<b>INS</b>	Immigration and Naturalization Service
<b>Interpol</b>	International Criminal Police Organization
<b>IOC</b>	Intergovernmental Oceanographic Commission
<b>IP</b>	Infrastructure Protection Division (DHS)
<b>IP</b>	Improvement plan
<b>IP/TCP</b>	Internet Protocol/Transmission Control Protocol
<b>IPC</b>	Initial Planning Conference
<b>IPE</b>	Individual protective equipment
<b>IPP</b>	Infrastructure Protection Program
<b>IPR</b>	Incident Prevention and Response Task
<b>IR</b>	Infrared
<b>IRA</b>	Irish Republican Army
<b>IRP</b>	Incidence response plan
<b>IRT</b>	Incidence response team
<b>ISAC</b>	Information Sharing & Analysis Center
<b>ISAO</b>	Information Sharing and Analysis Organization
<b>ISBE</b>	Infrastructure Security for the Built Environment
<b>ISC</b>	Interagency Security Committee
<b>ISDR</b>	International Strategy for Disaster Reduction
<b>ISIP</b>	Initial Strategy Implementation Plan
<b>ISO</b>	International Standards Organization
<b>ISP</b>	Internet service provider
<b>ISPS</b>	International Ship and Port Security
<b>ISTEA</b>	Intermodal Surface Transportation Efficiency Act of 1991
<b>IT</b>	Information technology
<b>ITA</b>	International Tunnelling Association
<b>ITA</b>	International Trade Administration
<b>ITDS</b>	International Trade Data System
<b>ITE</b>	Institute of Transportation Engineers
<b>ITI</b>	Innovative Technologies Institute
<b>ITS</b>	Intelligent Transportation Systems
<b>ITSA</b>	Intelligent Transportation Society of America
<b>IV</b>	Intravenous
<b>IVA</b>	Integrated Vulnerability Assessment
<b>IWN</b>	Integrated Wireless Network
<b>J</b>	Joule
<b>JAUGS</b>	Joint Architecture for Unmanned Ground Systems
<b>JFO</b>	Joint Field Office
<b>JIC</b>	Joint Information Center
<b>JIS</b>	Joint Information System
<b>JOC</b>	Joint bus-rail operations center
<b>JOC</b>	Joint Operations Center
<b>JPM</b>	Joint Program for Collective Protection
<b>JRIES</b>	Joint Regional Information Exchange Systems
<b>JSLSCAD</b>	Joint Service Lightweight Standoff Chemical Agent Detector
<b>JTTF</b>	Joint Terrorism Task Force
<b>K-9</b>	Canine team
<b>KHz</b>	Kilohertz (one thousand cycles per second)
<b>KI</b>	Potassium Iodide
<b>km</b>	Kilometer
<b>L</b>	Lambert

L	Liter
L	Lewisite
LA/LB	Port of Los Angeles/Long Beach
LAN	Local area network
LANL	Los Alamos National Laboratory
LAW	Light antitank weapon
LAX	Los Angeles International Airport
LCC	Life Cycle Cost
LD50	Lethal Dose for 50% of Population
LDS	Ladder Pipe Decontamination System
LED	Light-emitting diode
LEPC	Local Emergency Planning Committee
LESLP	London Emergency Services Liaison Panel
LETPP	Law Enforcement Terrorism Prevention Program
LIDAR	Light Detection and Ranging
LIRR	Long Island Rail Road
LLIS	Lessons Learned Information Sharing System
LLNL	Lawrence Livermore National Laboratory
LMR	Land Mobile Radio
LNM	Local Notice to Mariners
LO/LO	Load-On/Load-Off
LOINC	Logical Observation Identifiers Names and Codes
LOP	Level of protection
LPG	Liquefied petroleum gas
LRN	Laboratory Response Network (part of CDC)
LRV	Light rail vehicle
LTL	Less-Than-Truck Load
LVA	Low-Volatility Agent
LVB	Large Vehicle Bomb
M&A	Management and Administrative
MAA	Mutual Aid Agreement
MAC	Multiagency Coordination
MACS	Multi-Agency Coordinating System
MADA	Multi-Attribute Decision Analysis
MANPADS	Man-portable air defense system
MARC	Maryland Area Rail Commuter
MARSEC	Maritime Security
MARTA	Metropolitan Atlanta Rapid Transit Authority
MASINT	Measurement and Signatures Intelligence
MBTA	Massachusetts Bay Transportation Authority
MCC	Master Control Cell
MCC	Movement Coordination Center
MCI	Mass casualty incidents
MCWP	Marine Corps Warfighting Publication
MDOT	Maryland Department of Transportation
MDSHA	Maryland State Highway Administration
MDT	Mobile data terminals
MDTA	Maryland Transportation Authority
MERV	Minimum efficiency reporting value
MHz	Megahertz (one million cycles per second)
MIL-PRF	Military Performance Specification
MIL-STD	Military Standard
MIPT	Memorial Institute for the Prevention of Terrorism
MMW	Millimeter wave
MO	Monorail
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MOW	Maintenance-of-way
MPC	Mid-Term Planning Conference
MPO	Metropolitan planning organization



<b>MRA</b>	Mutual Response Agreement
<b>MRC</b>	Medical Reserve Corps (part of HHS)
<b>MSEL</b>	Master Scenario Events List
<b>MSIS Database</b>	Marine Safety Information System Database
<b>MT/HSAP</b>	Mass Transit Homeland Security Assistance Program
<b>MTA</b>	New York City Metropolitan Transportation Authority
<b>MTA</b>	Maryland Transit Administration
<b>MTBF</b>	Mean time between failure
<b>MTFVTP</b>	Memorial Tunnel Fire Ventilation Test Program
<b>MTI</b>	Mineta Transportation Institute
<b>MTMC</b>	Military Traffic Management Command
<b>MTRS</b>	Man Transportable Robotic System (a NAVSEA program)
<b>MTSA</b>	Maritime Transportation Security Act
<b>MTTR</b>	Mean time to repair
<b>MVR</b>	Motor Vehicle Record
<b>NACCHO</b>	National Association of County and City Health Officials
<b>NADB</b>	National Asset Database
<b>NAPA</b>	National Academy of Public Administration
<b>NAS</b>	National Academy of Sciences
<b>NASA</b>	National Aeronautics and Space Administration
<b>NASAR</b>	National Association for Search and Rescue
<b>NAVFAC</b>	Naval Facilities Engineering Command
<b>NAVSEA</b>	Naval Sea Systems Command
<b>NBC</b>	Nuclear, biological, and chemical
<b>NBER</b>	National Bureau of Economic Research
<b>NBI</b>	National Bridge Inventory
<b>NBS</b>	National Bureau of Standards
<b>NBSCAB</b>	National Bomb Squad Commanders Advisory Board
<b>NCDC</b>	National Climatic Data Center
<b>NCHRP</b>	National Cooperative Highway Research Program
<b>NCIC</b>	National Crime Information Center
<b>NCJA</b>	National Criminal Justice Association
<b>NCR</b>	National Capital Region
<b>NCTC</b>	National Counterterrorism Center
<b>NCTRP</b>	National Cooperative Transit Research and Development Program
<b>NDMS</b>	National Disaster Medical System (part of DHS)
<b>NDR</b>	National Driver Register
<b>NDS</b>	National Design Specifications
<b>NEC</b>	Northeast Corridor
<b>NECC</b>	National Emergency Coordination Center (part of FEMA)
<b>NEDSS</b>	National Electronic Disease Surveillance System (part of CDC)
<b>NEMA</b>	National Electrical Manufacturers Association
<b>NEMA</b>	National Emergency Management Association
<b>NEPA</b>	National Environmental Policy Act
<b>NESDIS</b>	National Environmental Satellite, Data, and Information Service
<b>NFIP</b>	National Flood Insurance Program
<b>NFIQ</b>	NIST Fingerprint Image Quality
<b>NFIRS</b>	National Fire Incident Reporting System
<b>NFPA</b>	National Fire Protection Association
<b>NG</b>	Nitroglycerin A liquid explosive.
<b>NGA</b>	National Governors Association
<b>NGO</b>	Non-governmental organization
<b>NGVC</b>	Natural Gas Vehicle Coalition
<b>NHS</b>	National Highway System
<b>NHTSA</b>	National Highway Traffic Safety Administration
<b>NIAC</b>	National Infrastructure Advisory Council
<b>NIAID</b>	National Institute of Allergy and Infectious Diseases (Part of NIH)
<b>NIBS</b>	National Institute of Building Sciences
<b>NIC</b>	NIMS Integration Center
<b>NICC</b>	National Infrastructure Coordinating Center

<b>NICS</b>	National Institute for Chemical Studies
<b>NIEHS</b>	National Institute of Environmental Health Sciences
<b>NIH</b>	National Institutes of Health (part of HHS)
<b>NIJ</b>	National Institute of Justice
<b>NIMA</b>	National Imaging and Mapping Agency
<b>NIMCAST</b>	NIMS Capability Assessment Support Tool
<b>NIMH</b>	National Institute of Mental Health (part of NIH)
<b>NIMS</b>	National Incident Management System
<b>NIOSH</b>	National Institute for Occupational Safety and Health (part of CDC)
<b>NIPC</b>	National Infrastructure Protection Center
<b>NIPP</b>	National Infrastructure Protection Plan
<b>NIST</b>	National Institute of Standards and Technology
<b>NJTTF</b>	National Joint Terrorism Task Force
<b>NMRT</b>	National Medical Response Team (part of NDMS)
<b>NMRT-WMD</b>	National Medical Response Team-Weapons of Mass Destruction
<b>NO<sub>3</sub></b>	Nitrous oxide
<b>NOAA</b>	National Oceanic and Atmospheric Association
<b>NODC</b>	National Oceanographic Data Center
<b>NPCA</b>	National Police Canine Association
<b>NPG</b>	National Preparedness Guidance
<b>NPHIC</b>	National Public Health Information Coalition
<b>NPHPP</b>	National Bioterrorism Hospital Preparedness Program (part of HRSA)
<b>NPRT</b>	National Pharmacy Response Team (part of NDMS)
<b>NPS</b>	National Park Service
<b>NRC</b>	National Research Council
<b>NRC</b>	U.S. Nuclear Regulatory Commission
<b>NRCC</b>	National Response Coordination Center
<b>NRCC</b>	National Research Council of Canada
<b>NRF</b>	National Response Framework
<b>NRL</b>	The Naval Research Laboratory
<b>NRP</b>	National Response Plan
<b>NRT</b>	National Response Team
<b>NS</b>	National Strategic Task
<b>NSA</b>	National Security Agency
<b>NSC</b>	National Security Council
<b>NSF</b>	National Science Foundation
<b>NSHS</b>	National Strategy for Homeland Security
<b>NSN</b>	National Stock Number
<b>NSSE</b>	National Security Special Events
<b>NSTAC</b>	National Security Telecommunications Advisory Council
<b>NSTS</b>	National Strategy for Transportation Security
<b>NTD</b>	National Transit Database
<b>NTI</b>	National Transit Institute
<b>NTRC</b>	National Transportation Research Center
<b>NTSB</b>	National Transportation Safety Board
<b>NTTC</b>	National Tank Truck Carriers
<b>NTTP</b>	Navy Tactics, Techniques, and Procedures
<b>NVIC</b>	Navigation and Vessel Inspection Circular
<b>NVPO</b>	National Vaccine Program Office (part of HHS)
<b>NVPZ</b>	Naval Vessel Protection Zone
<b>NWS</b>	National Weather Service
<b>NYCT</b>	New York City Transit
<b>NYCTA</b>	New York City Transit Authority
<b>NYPD</b>	New York Police Department
<b>O&amp;M</b>	Operations and Maintenance
<b>OAE</b>	Office of Applied Economics
<b>OASIS</b>	Operation Area Satellite System
<b>OC</b>	Office of the Comptroller
<b>OCC</b>	Operations Control Center
<b>OCMI</b>	Officer in Charge of Marine Inspection

<b>OCS</b>	Operator control station
<b>ODP</b>	Office for Domestic Preparedness (DHS)
<b>OEM</b>	Office of Emergency Management
<b>OEM</b>	Original equipment manufacturer
<b>OES</b>	Office of Emergency Services
<b>OGC</b>	Office of General Counsel
<b>OGO</b>	Office of Grant Operations
<b>OGT</b>	Office of Grants and Training
<b>OHS</b>	Office of Homeland Security
<b>OIC</b>	Office for Interoperability and Compatibility
<b>OIS</b>	Office of Intelligence and Security
<b>OJP</b>	Office of Justice Programs (DOJ)
<b>OLES</b>	Office of Law Enforcement Standards
<b>OMB</b>	Office of Management and Budget
<b>ONP</b>	Office of National Preparedness
<b>OPNAV</b>	Office of the Chief of Naval Operations
<b>OPS</b>	Office of Pipeline Safety
<b>ORNL</b>	Oak Ridge National Laboratory
<b>OSC</b>	Office for Security Coordination
<b>OSHA</b>	Occupational Safety and Health Administration (part of DOL)
<b>OSTP</b>	Office of Science and Technology Policy (White House)
<b>OTR</b>	Over the road
<b>OTS</b>	Off-the-shelf
<b>OV</b>	Operational Vulnerability
<b>P.L.</b>	Public Law
<b>PA</b>	Public address system
<b>PAC</b>	Protective action coordinator
<b>PAG</b>	Protective Action Guidance
<b>PART</b>	Program Assessment and Rating Tool
<b>PATH</b>	Port Authority Trans-Hudson Corporation
<b>PBS</b>	Public Buildings Service
<b>PCB</b>	Polychlorinated Biphenyl
<b>PCC</b>	Policy Coordinating Committee
<b>PCI</b>	Professional Certified Investigator
<b>PCII</b>	Protected Critical Infrastructure Information
<b>PCS</b>	Planning, Coordination and Support Task
<b>PD</b>	Probability of detection
<b>PDA</b>	Personal digital assistant
<b>PDC</b>	Pacific Disaster Center
<b>PDD</b>	Presidential Decision Directive
<b>PEMS</b>	Postal Emergency Management System
<b>PERI</b>	Public Entity Risk Institute
<b>PETN</b>	Pentaerythritol tetranitrate
<b>PFD</b>	Personal flotation device
<b>PFNA</b>	Pulsed fast neutron analysis
<b>PFO</b>	Principal Federal Official
<b>PHMSA</b>	Pipeline and Hazardous Materials Administration
<b>PHS</b>	Public Health Service (part of HHS)
<b>PIDS</b>	Perimeter Intrusion Detection System
<b>PIN</b>	Personnel identification number
<b>PIO</b>	Public Information Officer
<b>PIV</b>	Personal identity verification
<b>PIVA</b>	Port Integrated Vulnerability Assessment
<b>PL</b>	Photoluminescent
<b>PM</b>	Protective Measure
<b>PML</b>	Probable Maximum Loss
<b>p-MNT</b>	Para-mononitrotoluene an explosive taggant
<b>PMTL</b>	Protective Measures Target List
<b>POC</b>	Point of contact
<b>POETE</b>	Planning, Organization, Equipment, Training, and Exercises

<b>PORR</b>	Program Observation and Recommendation Report
<b>ppb</b>	Parts per billion
<b>PPE</b>	Personal protective equipment
<b>ppm</b>	Parts per million
<b>ppt</b>	Parts per trillion
<b>PRA</b>	Paperwork Reduction Act
<b>PRD</b>	Personal radiation detector
<b>PROTECT</b>	Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism
<b>PSA</b>	Patient Staging Area
<b>PSGP</b>	Port Security Grant Program
<b>PSI</b>	Pounds per square inch
<b>PSP</b>	Physical security professionals
<b>PSTN</b>	Public Switched Telephone Network
<b>PTII</b>	Public Transportation Information Infrastructure
<b>PTSD</b>	Post-traumatic Stress Disorder
<b>PTT</b>	Push-to-Talk
<b>PUC</b>	Public Utility Commission
<b>PV</b>	Physical vulnerability
<b>PVA</b>	Passenger Vessel Association
<b>PY-GC-IMS</b>	Pyrolysis-Gas Chromatography-Ion Mobility Spectrometer
<b>R&amp;D</b>	Research and Development
<b>RAD/NUC</b>	Radiological/Nuclear
<b>RAM</b>	Risk Assessment Methodology
<b>RAMCAP</b>	Risk Analysis and Management for Critical Asset Protection
<b>RAMPART</b>	Risk Assessment Method Property Analysis and Ranking Tool
<b>RAP</b>	Radiological Assistance Program
<b>RAPID-T</b>	Recognition, protection, decontamination, triage, treatment
<b>RB-HS</b>	Homeland Security Response Boat
<b>RDD</b>	Radiation Dispersal Device
<b>RDT&amp;E</b>	Research, development, test and evaluation
<b>RDX</b>	Research Department
<b>RED</b>	Radiation-emitting device
<b>RERP</b>	Regional Emergency Response Plan
<b>RF</b>	Radio frequency
<b>RFP</b>	Reinforced Fiber Protection
<b>RIIDs</b>	Radiation isotope identifier devices
<b>RKB</b>	Responder Knowledge Base
<b>RMS</b>	Risk management solutions
<b>RO/RO</b>	Roll-On/Roll-Off
<b>ROC</b>	Regional Operations Center
<b>ROI</b>	Return on investment
<b>ROW</b>	Right-of-way
<b>RPM</b>	Radiation portal monitor
<b>RRCC</b>	Regional Response Coordination Center
<b>RRR</b>	Rapid Response Registry (part of ATSDR)
<b>RS232</b>	Wiring protocol for electronics communication
<b>RSCAAL</b>	Remote Sensing Chemical Agent Alarm
<b>RSPA</b>	Research and Special Programs Administration
<b>RTS</b>	Rail transit system
<b>RTSS</b>	Regional Transit Security Strategy
<b>RTSWG</b>	Regional Transit Security Work Group
<b>S&amp;T</b>	Science and Technology Directorate (DHS)
<b>SAA</b>	State Administrative Agency
<b>SAE</b>	Society of Automotive Engineers
<b>SAFECOM</b>	Safety Interoperable Communications Program
<b>SAFETEA-LU</b>	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
<b>SAMHSA</b>	Substance Abuse and Mental Health Services Administration (part of HHS)
<b>SAP</b>	Select Agent Program (part of CDC)
<b>SAP</b>	State Assistance Plan

<b>SAR</b>	Search and rescue
<b>SAW</b>	Surface acoustic wave
<b>SBCCI</b>	Southern Building Code Congress International, Inc.
<b>SBCCOM</b>	Soldier, Biological, and Chemical Command
<b>SBU</b>	Sensitive-but-Unclassified
<b>SC</b>	Security Coordinator
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SCBA</b>	Self-Contained Breathing Apparatus
<b>SCC</b>	Sector Coordinating Council
<b>SCIP</b>	Statewide Communications Interoperability Planning
<b>SCP</b>	Situational crime prevention
<b>SD</b>	Security Directive
<b>SDO</b>	Standards Development Organization
<b>SEA</b>	Safe Explosives Act
<b>SEL</b>	Standardized Equipment List
<b>SEM</b>	Sequential Excavation Method
<b>SEP</b>	State emergency plan
<b>SEPP</b>	Security and Emergency Preparedness Plan
<b>SEPTA</b>	Southeastern Pennsylvania Transportation Authority
<b>SERC</b>	State Emergency Response Commission
<b>SERT</b>	Secretary's Emergency Response Team (part of HHS)
<b>SESI</b>	Science and Engineering Services, Inc.
<b>SFPE</b>	Society of Fire Protection Engineers
<b>SHSAS</b>	State Homeland Security Assessment and Strategy
<b>SHSGP</b>	State Homeland Security Grant Program
<b>SHSS</b>	State Homeland Security Strategy
<b>SIA</b>	Specific intensity per unit area
<b>SIDA</b>	Secure Identification Display Area
<b>SIOC</b>	Strategic Information and Operations Center (FBI HQ)
<b>SITMAN</b>	Situation Manual
<b>SL</b>	Scenario Loss
<b>SLG</b>	State and Local Guide
<b>SLGCP</b>	Office of State and Local Government Coordination and Preparedness (DHS)
<b>SMART</b>	Simple, Measurable, Achievable, Realistic, Task Oriented
<b>SME</b>	Subject matter expert
<b>SNL</b>	Sandia National Laboratories
<b>SNOMED</b>	Systematized Nomenclature of Medicine
<b>SNS</b>	Strategic National Stockpile (part of CDC)
<b>SOC</b>	Strategic Operations Center
<b>SONET</b>	Synchronous Optical Network
<b>SOP</b>	Standard operating procedure
<b>SPOT</b>	Screening of Passengers by Observation Technique
<b>SPT</b>	Standard Penetration Test
<b>SRA</b>	Safe Refuge Area
<b>SRI</b>	Stanford Research Institute
<b>SRWF</b>	Shatter-resistant window film
<b>SSA</b>	Sector-Specific Agency
<b>SSAPP</b>	System safety program plan
<b>SSC</b>	Scientific Support Coordinator
<b>SSI</b>	Sensitive Security Information
<b>SSP</b>	Sector-Specific Plan
<b>SSPP</b>	System security program plan
<b>START</b>	Study of Terrorism and Responses to Terrorism
<b>START</b>	Simple triage and rapid treatment/transport
<b>STB</b>	Surface Transportation Board
<b>STD</b>	Standard
<b>ST-ISAC</b>	Surface Transportation Information Sharing & Analysis Center
<b>STP</b>	Surface Transportation Program
<b>STRAHNET</b>	Strategic Highway Network
<b>STSI</b>	Surface Transportation Security Inspection

<b>SVA</b>	Security Vulnerability/Risk Assessment
<b>SVP</b>	Safety verification plan
<b>SWAT</b>	Special weapons and tactics
<b>TA</b>	Technical Assistance
<b>TATP</b>	Triacetone Triperoxide. An unstable explosive used in IEDs.
<b>TBM</b>	Tunnel-boring machine
<b>TCIP</b>	Transit Communications Interface Protocols
<b>TCO</b>	Total Cost of Ownership
<b>TCRP</b>	Transit Cooperative Research Program
<b>TEA</b>	Thermal Energy Analysis
<b>TEA-21</b>	Transportation Equity Act for the 21st Century
<b>TEDA</b>	triethylenediamine
<b>TEOC</b>	Transportation Emergency Operations Center
<b>Tetryl</b>	Trinitrophenylmethylnitramine
<b>TEW</b>	Terrorism Early Warning (Group)
<b>TFA</b>	Toxic-free area
<b>TIA</b>	Terrorism Incident Annex
<b>TIC</b>	Transit incident commander
<b>TIC</b>	Toxic industrial compound
<b>TIFs</b>	Threat Information Forums
<b>TII</b>	Transportation Information Infrastructure
<b>TIMs</b>	Toxic industrial materials
<b>TIOC</b>	Transportation Information Operations Center
<b>TISD</b>	Transportation Infrastructure Security Division
<b>TISP</b>	The Infrastructure Security Partnership
<b>TL</b>	Truck Load
<b>TM</b>	Technical Manual
<b>TM</b>	Transverse Magnetic
<b>TMA</b>	Transportation management association
<b>TMC</b>	Transportation Management Center
<b>TMP</b>	SMX Trimethoprim/Sulfamethoxazole
<b>TMS</b>	Tunnel Management System
<b>TMS</b>	The Masonry Society
<b>TNT</b>	Trinitrotoluene
<b>TOPOFF</b>	Top Officials (Exercise)
<b>TOSIC</b>	Transit on-site incident commander
<b>TR</b>	Technical Report
<b>TRACEM</b>	Thermal, radiological, asphyxiation, chemical, etiological, and mechanical
<b>TRANSCOM</b>	Transportation Operations Coordinating Committee
<b>Transit EOC</b>	Joint Transit Bus and Rail Emergency Operations Center
<b>TRB</b>	Transportation Research Board
<b>TRC</b>	Tone Remote Control
<b>TRI</b>	Toxic Release Inventory
<b>TrucksISAC</b>	Trucking Information Sharing and Analysis Center
<b>TSA</b>	Transportation Security Administration
<b>TSC</b>	Transit Standards Consortium
<b>TSC</b>	Terrorist Screening Center
<b>TSGP</b>	Transit Security Grant Program
<b>TSI</b>	Transportation Security Incident
<b>TSI</b>	Transportation Safety Institute
<b>TSOC</b>	Transportation Security Operations Center
<b>TSWG</b>	Technical Support Working Group
<b>TTIC</b>	Terrorist Threat Integration Center
<b>TTP</b>	Thrombocytopenic purpura
<b>TTPs</b>	Tactics, Techniques, & Procedures
<b>TTX</b>	Tabletop Exercise
<b>TUGs</b>	Threat User Groups
<b>TVA</b>	Threat and Vulnerability Assessment
<b>TWIC</b>	Transportation Worker Identification Credentialing
<b>TWIC</b>	Transportation Worker Identification Card

<b>UA</b>	Universal Adversary
<b>UASI</b>	Urban Areas Security Initiative
<b>UAV</b>	Unmanned Aerial Vehicle
<b>UAWG</b>	Urban Areas Working Group
<b>UBC</b>	Universal Building Code
<b>UC</b>	Unified Command
<b>UCRL</b>	University of California Radiation Laboratory
<b>UCS</b>	Unified Command System
<b>UFC</b>	Unified Facilities Criteria
<b>UFGS</b>	Unified Facilities Guide Specification
<b>UFOV</b>	Useful field of view
<b>UHF</b>	Ultra High Frequency
<b>UICC</b>	Unified incident command center
<b>UL</b>	Underwriters' Laboratories
<b>UPS</b>	Uninterruptible power supply
<b>URM</b>	Unreinforced masonry
<b>US&amp;R</b>	Urban Search and Rescue
<b>USACE</b>	United States Army Corps of Engineers
<b>USAMRIID</b>	U.S. Army Medical Research Institute for Infectious Diseases (part of DOD)
<b>USB</b>	Universal serial bus
<b>USC</b>	United States Code
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USCG</b>	U.S. Coast Guard
<b>USD (AT&amp;L)</b>	Under Secretary of Defense for Acquisition, Technology, and Logistics
<b>USDA</b>	United States Department of Agriculture
<b>USFA</b>	United States Fire Administration
<b>USGS</b>	United States Geological Survey
<b>USMS</b>	United States Marshals Service
<b>USPCA</b>	United States Police Canine Association
<b>USPHS</b>	United States Public Health Service
<b>USPS</b>	U.S. Postal Service
<b>UTL</b>	Universal Task List
<b>UV</b>	Ultraviolet
<b>UVGI</b>	Ultraviolet germicidal irradiation
<b>VA</b>	Department of Veterans Affairs
<b>VA</b>	Value Analysis
<b>VACIS</b>	Vehicle and Cargo Inspection System
<b>VAPO</b>	Vulnerability Assessment and Protection Option
<b>VBIED</b>	Vehicle-borne improvised explosive devices
<b>VDOT</b>	Virginia Department of Transportation
<b>VDOT STC</b>	VDOT Smart Traffic Center
<b>VHF</b>	Very-high frequency
<b>VMAT</b>	Veterinary Medical Assistance Team (part of NDMS)
<b>VMRS</b>	Vessel Movement Reporting System
<b>VMS</b>	Variable message sign
<b>VOAD</b>	Volunteer Organizations Active in Disasters
<b>VoIP</b>	Voice-over-Internet Protocol
<b>VOIS</b>	Virginia Operational Information System
<b>VOX</b>	Voice-Operated Transmit
<b>VRE</b>	Virginia Railway Express
<b>VSO</b>	Vessel Security Officer
<b>VSP</b>	Vessel Security Plan
<b>VTS</b>	Vessel Traffic Service
<b>VX</b>	V Agent
<b>WAN</b>	wide area network
<b>WiFi</b>	Wireless Fidelity
<b>WMATA</b>	Washington Metropolitan Area Transit Authority
<b>WMD</b>	Weapons of Mass Destruction

# Glossary

<b>Aberration</b>	Any inherent deficiency of a lens or optical system. Aberrations are responsible for imperfections in shape or sharpness of the image.
<b>Abnormal user</b>	Persons whom you do not desire to be in a certain space.
<b>Absolute risk</b>	The proportion of a population expected to get a disease over a specified time period. See also risk, relative risk.
<b>Absorbed dose</b>	The amount of energy deposited by ionizing radiation in a unit mass of tissue. It is expressed in units of joule per kilogram (J/kg), and called “gray” (Gy).
<b>Acceptable risk</b>	The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific system.
<b>Access control</b>	Any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.
<b>Access control methods and technologies</b>	Used to identify and control access to a defined area. Used in conjunction with intrusion detection systems to control nuisance alarms.
<b>Access control point (ACP)</b>	A station at an entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.
<b>Access control system (ACS)</b>	Also referred to as an Electronic Entry Control System, an electronic system that controls entry and egress from a building or area.
<b>Access control system elements</b>	Detection measures used to control vehicle or personnel entry into a protected area. Access Control System elements include locks, Electronic Entry Control Systems, and guards.
<b>Access controls</b>	Procedures and controls that limit or detect access to minimum essential infrastructure resource elements (e.g., people, technology, applications, data, and/or facilities), thereby protecting these resources against loss of integrity, confidentiality, accountability, and/or availability.
<b>Access group</b>	A software configuration of an Access Control System that groups together access points or authorized users for easier arrangement and maintenance of the system.
<b>Access road</b>	Any roadway such as a maintenance, delivery, service, emergency, or other special limited use road that is necessary for the operation of a building or structure.
<b>Accessibility</b>	The quality of being assessable; that which may be approached or entered.
<b>Accessible</b>	Having the legally required features and/or qualities that ensure easy entrance, participation, and usability of places, programs, services, and activities by individuals with a wide variety of disabilities.
<b>Accident notification threshold</b>	The oversight agency must require the rail transit agency to notify the oversight agency within two (2) hours of any incident involving a rail transit vehicle or taking place on rail transit-controlled property where one or more of the



following occurs: 1. A fatality at the scene; or where an individual is confirmed dead within thirty (30) days of a rail transit-related incident; 2. Injuries requiring immediate medical attention away from the scene for two or more individuals; 3. Property damage to rail transit vehicles, non-rail transit vehicles, other rail transit property or facilities and non-transit property that equals or exceeds \$25,000; 4. An evacuation due to life safety reasons; 5. A collision at a grade crossing; 6. A main-line derailment; 7. A collision with an individual on a rail right of way; or 8. A collision between a rail transit vehicle and a second rail transit vehicle, or a rail transit non-revenue vehicle.

<b>Accountability</b>	The explicit assignment of responsibilities for oversight of areas of control to executives, managers, staff, owners, providers, and users of minimum essential infrastructure resource elements.
<b>Acoustic eavesdropping</b>	The use of listening devices to monitor voice communications or other audibly transmitted information with the objective to compromise information.
<b>Acquisition procedures</b>	Used to obtain resources to support operational requirements.
<b>Active detector</b>	An active detector is, in general, a device that generates and emits energy for illuminating the portal region of the detector. For the walk-through metal detector, the emitted energy is in the form of a magnetic field. The interaction of the emitted magnetic field with certain types of objects in the portal region of the detector and the ability to detect this interaction is the basis of operation for walk-through metal detectors.
<b>Active illumination</b>	Illumination that is generated by electrical energy.
<b>Active incident</b>	Synonymous with an attack, something has in fact happened and lives and property are at risk.
<b>Active vehicle barrier</b>	An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.
<b>Activity (radioactivity)</b>	The rate of decay of radioactive material expressed as the number of atoms breaking down per second measured in units called becquerels or curies.
<b>Acute exposure</b>	An exposure to radiation that occurred in a matter of minutes rather than in longer, continuing exposure over a period of time. See also chronic exposure, exposure, fractionated exposure.
<b>Acute radiation syndrome (ARS)</b>	A serious illness caused by receiving a dose greater than 50 rads of penetrating radiation to the body in a short time (usually minutes). The earliest symptoms are nausea, fatigue, vomiting, and diarrhea. Hair loss, bleeding, swelling of the mouth and throat, and general loss of energy may follow. If the exposure has been approximately 1,000 rads or more, death may occur within 2 – 4 weeks.
<b>Adversary</b>	Any individual, group, organization or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets.
<b>Aerosol</b>	Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).
<b>After action report</b>	A report covering response actions, application of emergency management, modifications to plans and procedures, training needs, and recovery activities. After Action Reports are required under emergency management plans after any incident which requires a declaration of an emergency. Reports are required within 90 days.
<b>Agency (Incident Command Systems)</b>	A division of government with a specific function offering a particular kind of assistance. In ICS, agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating.
<b>Agency administrator/executive</b>	The official responsible for administering policy for an agency or jurisdiction, having full authority for making decisions and providing direction to the management organization for an incident.
<b>Agency dispatch</b>	The agency or jurisdictional facility from which resources are sent to incidents.

<b>Agency representative</b>	A person assigned by a primary, assisting, or cooperating Federal, State, tribal, or local government agency or private organization that has been delegated authority to make decisions affecting that agency's or organization's participation in incident management activities following appropriate consultation with the leadership of that agency.
<b>Aggressor</b>	Any person seeking to compromise a function or structure.
<b>Air burst</b>	A nuclear weapon explosion that is high enough in the air to keep the fireball from touching the ground. Because the fireball does not reach the ground and does not pick up any surface material, the radioactivity in the fallout from an air burst is relatively insignificant compared with a surface burst.
<b>Airborne contamination</b>	Chemical or biological agents introduced into and fouling the source of supply of breathing or conditioning air.
<b>Airlock</b>	A building entry configuration with which airflow from the outside can be prevented from entering a toxic-free area. An airlock uses two doors, only one of which can be opened at a time, and a blower system to maintain positive air pressures and purge contaminated air from the airlock before the second door is opened.
<b>Alarm assessment</b>	Verification and evaluation of an alarm alert through the use of closed circuit television or human observation. Systems used for alarm assessment are designed to respond rapidly, automatically, and predictably to the receipt of alarms at the security center.
<b>Alarm indication</b>	A signal to warn of the detection of a metal object. The indication can be visual and/or auditory.
<b>Alarm indicator</b>	The device used to generate the alarm indication. For a visual indication, the alarm generating device can be a light bulb, lamp, light emitting diode, etc. For an auditory indication, the alarm generating device can be a horn, siren, buzzer, etc.
<b>Alarm printers</b>	Alarm printers provide a hard-copy of all alarm events and system activity, as well as limited backup in case the visual display fails.
<b>Alarm priority</b>	A hierarchy of alarms by order of importance. This is often used in larger systems to give priority to alarms with greater importance.
<b>All-hazards</b>	Any incident, natural or manmade, that warrants action to protect life, property, environment, public health or safety, and minimize disruptions of government, social, or economic activities.
<b>All-hazards preparedness</b>	Refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies. (HSPD-8)
<b>Allocated resources</b>	Resources dispatched to an incident.
<b>Alpha particle</b>	The nucleus of a helium atom, made up of two neutrons and two protons with a charge of +2. Certain radioactive nuclei emit alpha particles. Alpha particles generally carry more energy than gamma or beta particles, and deposit that energy very quickly while passing through tissue. Alpha particles can be stopped by a thin layer of light material, such as a sheet of paper, and cannot penetrate the outer, dead layer of skin. Therefore, they do not damage living tissue when outside the body. When alpha-emitting atoms are inhaled or swallowed, however, they are especially damaging because they transfer relatively large amounts of ionizing energy to living cells. See also beta particle, gamma ray, neutron, x-ray.
<b>Alternate worksite</b>	A work location, other than the primary location, to be used when the primary location is not accessible.
<b>Alternative security program</b>	A third-party- or industrial-organization-developed standard that the commandant has determined provides an equivalent level of security to that established by current federal and U.S. Coast Guard regulations.
<b>Ambient air</b>	The air that surrounds us.

<b>Americium (Am)</b>	A silvery metal; it is a man-made element whose isotopes Am-237 through Am-246 are all radioactive. Am-241 is formed spontaneously by the beta decay of plutonium-241. Trace quantities of americium are widely used in smoke detectors, and as neutron sources in neutron moisture gauges.
<b>Analytical risk management (ARM)</b>	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.
<b>Annunciation</b>	A visual, audible, or other indication by a security system of a condition.
<b>Antiterrorism (AT)</b>	Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts.
<b>Applied police research</b>	Research that results in findings that have a practical application for a police agency.
<b>Approved</b>	Acceptable to the authority having jurisdiction.
<b>Area command</b>	An organization established to oversee the management of multiple incidents that are each being handled by a separate ICS organization or to oversee the management of a very large or evolving incident that has multiple incident management teams engaged. An agency administrator/executive or other public official with jurisdictional responsibility for the incident usually makes the decision to establish an Area Command. An Area Command is activated only if necessary, depending on the complexity of the incident and incident management span-of-control.
<b>Area command (Unified area command)</b>	An organization established (1) to oversee the management of multiple incidents that are each being handled by an ICS organization or (2) to oversee the management of large or multiple incidents to which several Incident Management Teams have been assigned. Area Command has the responsibility to set overall strategy and priorities, allocate critical resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multijurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident command post.
<b>Area lighting</b>	Lighting that illuminates a large exterior area.
<b>Area Maritime Security Committee</b>	The committee established to assist and advise in the development, review, and update of the area maritime security plan for its Captain of the Port zone.
<b>Area of responsibility</b>	A Coast Guard area, district, marine inspection zone, or Captain of the Port zone.
<b>Area sensor</b>	Used to monitor a physical surface area such as a floor, outdoor ground area, etc. Ranging from as simple as a pressure mat, to as complex as a buried field sensor. Distinction between Area and Volume sensors is sometimes limited.
<b>Areas of potential compromise</b>	Categories where losses can occur that will impact either a department's or an agency's minimum essential infrastructure and its ability to conduct core functions and activities.
<b>Areas of rescue</b>	Assistance or areas of refuge spaces where persons unable to use stairs can call for and await evacuation assistance from emergency personnel assets, mission-essential equipment, and facilities.
<b>Armed</b>	As used in this guideline, armed refers to a private security officer who is equipped with a weapon (firearm), such as a pistol or rifle, from which a shot is discharged.
<b>Armed threat or attack</b>	Refers to an individual(s) having, threatening, or using a personal deadly weapon such as a firearm, knife, baseball bat, or other personal weapon that can be carried or concealed by a person.
<b>Armored car company</b>	A company which, for itself or under contract with another, transports currency, securities, valuables, jewelry, food stamps, or any other item that requires secured and insured delivery from one place to another with armed personnel.

<b>Armored car personnel</b>	An armed employee of an armored car company who is engaged exclusively by that company and is liable for the safe transportation, care, and custody of valuables.
<b>Arrest</b>	The taking or keeping of a person in custody by legal authority, especially in response to a criminal charge; specifically, the apprehension of someone for the purpose of securing the administration of the law, especially of bringing that person before a court.
<b>Assess</b>	Refers to the action of a transit agency employee determining if an observed situation constitutes criminal or terrorist preliminary activities, or poses potential or real danger to the transit agency's facilities, themselves, passengers/patrons, and anyone else in the vicinity.
<b>Assessment</b>	The evaluation and interpretation of measurements and other information to provide a basis for decision-making.
<b>Assessment system elements</b>	Detection measures used to assist guards in visual verification of Intrusion Detection System Alarms and Access Control System functions and to assist in visual detection by guards. Assessment System elements include closed circuit television and protective lighting.
<b>Asset<sup>1</sup></b>	An asset is any person, facility, material, information, or activity that has a positive value to the Transportation Systems Sector. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways, including people, information, equipment, facilities, and activities or operations.
<b>Asset<sup>2</sup></b>	A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's information and reputation).
<b>Asset protection</b>	Security program designed to protect personnel, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, and personal protective services, and supported by intelligence, counter-intelligence, and other security.
<b>Asset value</b>	The degree of debilitating impact that would be caused by the incapacity or destruction of an asset.
<b>Assets</b>	People, information, and property for which the public transportation system is responsible as legal owner, employer, or service provider.
<b>Assets (Critical)</b>	A sub-category of assets whose loss has the greatest consequences for people and the ability of the system to sustain service. These assets may require higher or special protection.
<b>Assigned resources</b>	Resources checked in and assigned work tasks on an incident.
<b>Assignments</b>	Tasks given to resources to perform within a given operational period that are based on operational objectives defined in the Incident Action Plan (IAP).
<b>Assistant</b>	Title for subordinates of principal Command Staff positions. The title indicates a level of technical capability, qualifications, and responsibility subordinate to the primary positions. Assistants may also be assigned to unit leaders.
<b>Assisting agency</b>	An agency or organization providing personnel, services, or other resources to the agency with direct responsibility for incident management. See Supporting Agency.
<b>Assurance</b>	The confidence that may be held in the security provided by a system, product or process (envoy)
<b>Attack<sup>1</sup></b>	A hostile action resulting in the destruction, injury, or death to the civilian population, or damage or destruction to public and private property.
<b>Attack<sup>2</sup></b>	Sabotage or the use of bombs, chemical or biological agents, nuclear or radiological materials, or armed assault with firearms or other weapons by a terrorist

	or quasi-terrorist actor that cause or may cause substantial damage or injury to persons or property in any manner.
<b>Attack</b> <sup>3</sup>	A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.
<b>Audible alarm device</b>	An alarm device that produces an audible announcement (e.g., bell, horn, siren, etc.) of an alarm condition.
<b>Audit</b> <sup>1</sup>	An evaluation of a security assessment or security plan—performed by the owner or operator, the owner or operator’s designee, or an approved third party—intended to identify deficiencies, non-conformities, and/or inadequacies that would render the assessment or plan insufficient.
<b>Audit</b> <sup>2</sup>	The process of reviewing and evaluating compliance with applicable directives and regulations and/or the examination of records or accounts to check their accuracy.
<b>Authority having jurisdiction (AHJ)</b>	An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.
<b>Auto equivalent units (AEUs)</b>	A commonly used measurement to determine auto-deck capacity to keep the vessel balanced. The measurement is based on the space that a boarding vehicle occupies compared with the space of a standard vehicle to determine weight constraints for vehicle ferries.
<b>Auto-Iris Lens</b>	A lens with an electronically controlled iris. This allows the lens to maintain one light level throughout varying light conditions.
<b>Automatic identification system (AIS)</b>	A shipboard broadcast system that acts like a transponder, operates in the VHF maritime band, is capable of handling thousands of reports per minute, and updates as often as every 2 seconds.
<b>Availability</b>	The ability to have access to mission essential infrastructure resource elements when required by the mission and core supporting processes.
<b>Available resources</b>	Resources assigned to an incident, checked in, and available for a mission assignment, normally located in a Staging Area.
<b>Background radiation</b>	Ionizing radiation from natural sources, such as terrestrial radiation due to radionuclides in the soil or cosmic radiation originating in outer space.
<b>Background screening</b>	An inquiry into the history and behaviors of an individual under consideration for employment, credit, access to sensitive assets (such as national defense information), and other reasons.
<b>Background verification/check</b>	The process of checking an individual’s character, general reputation, personal characteristics, or mode of living for consideration of employment, promotion, access to sensitive assets (such as national information), or for continued employment. Elements of a background verification/check can vary widely, and may include information from credit bureaus, courts records repositories, departments of motor vehicles, past or present employers and educational institutions, governmental occupational licensing or registration entities, business or personal references, and any other source required to verify information that was voluntarily supplied.
<b>Badging</b>	Based on credentialing and resource ordering, provides incident-specific credentials and can be used to limit access to various incident sites.
<b>Balance pressure switch</b>	An IDS sensor that alarms when subjected to a pressure differential.
<b>Balance Magnetic Switch (BMS)</b>	A set of contacts and magnets used to annunciate the opening / closing of door, window, or other device. Replaces magnetic position switches that are easily defeated and bypassed.
<b>Balanced magnetic switch (BMS)</b>	A door position switch utilizing a reed switch held in a balanced or center position by interacting magnetic fields when not in alarm condition.

<b>Ballistics attack</b>	An attack in which small arms (e.g., pistols, submachine guns, shotguns, and rifles) are fired from a distance and rely on the flight of the projectile to damage the target.
<b>Barbed tape or concertina</b>	A coiled tape or coil of wires with wire barbs or blades deployed as an obstacle to human trespass or entry into an area.
<b>Barbed wire</b>	A double strand of wire with four-point barbs equally spaced along the wire deployed as an obstacle to human trespass or entry into an area.
<b>Barcode</b>	A black bar printed on white paper or tape that can be easily read with an optical scanner.
<b>Barrier Sensors Sensors</b>	Used to monitor a physical barrier - fence, wall, roof, window, etc.
<b>Base</b>	The location at which primary Logistics functions for an incident are coordinated and administered. There is only one Base per incident. (Incident name or other designator will be added to the term Base.) The Incident Command Post may be co-located with the Base.
<b>Base Measure</b>	See Baseline.
<b>Baseline</b>	A starting point used in research and identified prior to experimentation as a point of comparison with data after experimental variables are introduced.
<b>Becquerel (Bq)</b>	The amount of a radioactive material that will undergo one decay (disintegration) per second.
<b>Benefit</b>	Amount of risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities (ARM).
<b>Beta particles</b>	Electrons ejected from the nucleus of a decaying atom. Although they can be stopped by a thin sheet of aluminum, beta particles can penetrate the dead skin layer, potentially causing burns. They can pose a serious direct or external radiation threat and can be lethal depending on the amount received. They also pose a serious internal radiation threat if beta-emitting atoms are ingested or inhaled. See also alpha particle, gamma ray, neutron, x-ray.
<b>Binary sensor</b>	An IDS sensing device that has only 2 states - open or closed, which is used to announce alarms. Example = BMS
<b>Bioassay</b>	An assessment of radioactive materials that may be present inside a person's body through analysis of the person's blood, urine, feces, or sweat.
<b>Biological agents</b>	Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.
<b>Biological effects of ionizing radiation (BEIR) reports</b>	Reports of the National Research Council's committee on the Biological Effects of Ionizing Radiation.
<b>Biometric</b>	The utilization of a personal biometric trait to identify a user to ACS and IDS systems. Examples are fingerprints, iris scans, retinal scans, hand geometry.
<b>Biometric reader</b>	A device that gathers and analyzes biometric features.
<b>Biometrics</b>	The use of physical characteristics of the human body as a unique identification method.
<b>Blast curtains</b>	Heavy curtains made of blast-resistant materials that could protect the occupants of a room from flying debris.
<b>Blast vulnerability envelope</b>	The geographical area in which an explosive device will cause damage to assets.
<b>Blast-resistant glazing</b>	Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.
<b>Blower door assembly</b>	A calibrated device that measures the airflow rate into the facility during pressurization and out of the facility during depressurization.

<b>Bollard</b>	A vehicle barrier consisting of a cylinder, usually made of steel and sometimes filled with concrete, placed on end in the ground and spaced about 3 feet apart to prevent vehicles from passing, but allowing entrance of pedestrians and bicycles.
<b>Bomb</b>	A device capable of producing damage to material and injury or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary.
<b>Bomb incident</b>	Involves any occurrence concerning the detonation/ignition of a bomb, the discovery of a bomb, or execution of a bomb threat.
<b>Bomb threat</b>	A message delivered by any means and the message may or may not: Specify location of the bomb, Include the time for detonation/ignition, Contain an ultimatum related to the detonation/igniter or concealment of the bomb.
<b>Boundary penetration sensor</b>	An interior intrusion detection sensor that detects attempts by individuals to penetrate or enter a building.
<b>Branch</b>	The organizational level having functional or geographical responsibility for major aspects of incident operations. A Branch is organizationally situated between the Section Chief and the Division or Group in the Operations Section, and between the Section and Units in the Logistics Section. Branches are identified by the use of roman numerals or by functional area.
<b>Breach of security</b>	An incident that has not resulted in a transportation security incident because security measures have been circumvented, eluded, or violated.
<b>Breakwire</b>	An IDS sensor that alarms an IDS when a wire or other cable is broken.
<b>Building hardening<sup>1</sup></b>	Enhanced conventional construction that mitigates threat hazards where stand-off distance is limited. Building hardening may also be considered to include the prohibition of certain building materials and construction techniques.
<b>Building hardening<sup>2</sup></b>	Enhanced construction that reduces vulnerability to external blast and ballistic attacks.
<b>Building separation</b>	The distance between closest points on the exterior walls of adjacent buildings or structures.
<b>Building/facility elements</b>	One of the three cost types that define the building/facility component of the detailed cost-accounting framework: building/facility elements; building/facility site work; non-elemental. The building/facility elements cost type is associated with the elemental classification UNIFORMAT II.
<b>Business continuity</b>	A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.
<b>Business continuity program (BCP)</b>	An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity services through personnel training, plan testing, and maintenance.
<b>Business impact analysis (BIA)</b>	A management level financial analysis that identifies the impacts of losing an organization's resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide reliable data upon which to base decisions on mitigation, recovery, and business continuity strategies.
<b>C2</b>	Command & Control
<b>C3</b>	Command, Control, & Communications
<b>C4</b>	Command, Control, Communications, Computers & Integration - Military term to define an integrated system for overall control and operation of a complex operation
<b>Cable barrier</b>	Cable or wire rope anchored to and suspended off the ground or attached to chain-link fence to act as a barrier to moving vehicles.
<b>Cache</b>	A predetermined complement of tools, equipment, and/or supplies stored in a designated location, available for incident use.

<b>Camera Format</b>	The approximate size of a camera image pickup device. This measurement is derived from the diagonal line of a chip or the diameter of the tube.
<b>Capabilities assessment</b>	A formal evaluation, conducted by the public transportation system, to identify the status of its security and emergency preparedness activities. This activity enables the system to determine its existing capacity to (1) Reduce the threat of crime and other intentional acts; (2) Recognize, mitigate, and resolve incidents that occur in service and on system property; (3) Reduce the threat of crime and other intentional acts; (4) Protect passengers, employees, emergency responders, and the environment during emergency operations; and (5) Support community response to a major event.
<b>Capability</b>	The ability of a suitably organized, trained, and equipped entity to address, penetrate, or alter systems and/or to disrupt, deny or destroy all or part of a critical infrastructure (CIAO). A measure of the degree to which a system is able to satisfy its performance objectives.
<b>Capacitance</b>	An IDS sensor technology that measures the disturbance of a capacitive field set up to protect fixed objects.
<b>Capacitance sensor</b>	A device that detects an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.
<b>Captain of the Port (COTP)</b>	The local officer exercising authority for the Captain of the Port zones. The COTP is the maritime security coordinator and the port facility security officer.
<b>Carcinogen</b>	A cancer-causing substance.
<b>Card reader</b>	A device that gathers or reads information when a card is presented as an identification method.
<b>Cat5</b>	Category 5 cable includes four twisted pairs in a single cable jacket. This use of balanced lines helps preserve a high signal-to-noise ratio despite interference from both external sources and other pairs (this latter form of interference is called crosstalk). It is most commonly used for 100 Mbit/s networks, such as 100BASE-TX Ethernet.
<b>Catamaran</b>	A vessel with twin hulls and usually a deck or superstructure connecting the hulls.
<b>Categorizing resources</b>	Resources are organized by category, kind, and type, including size, capacity, capability, skill, and other characteristics. This makes the resource ordering and dispatch process within and across organizations and agencies, and between governmental and nongovernmental entities, more efficient, and ensures that the resources received are appropriate to their needs.
<b>CATS</b>	Consequence Assessment Tool Set
<b>Causation</b>	The ability of one event to create or control another event.
<b>CBR event</b>	An airborne release involving a CBR agent and caused by an industrial accident or an intentional release either external or internal to the facility
<b>CCTV pan-tilt-zoom camera (PTZ)</b>	A CCTV camera that can move side to side, up and down, and zoom in or out.
<b>CCTV pan-tilt-zoom control</b>	The method of controlling the PTZ functions of a camera.
<b>CCTV pan-tilt-zoom controller</b>	The operator interface for performing PTZ control.
<b>CCTV switcher</b>	A piece of equipment capable of presenting multiple video images to various monitors, recorders, etc.
<b>Certified K9</b>	A K9 team meeting the performance standards of the police department, contracting agency, or recognized professional association, as evaluated by a qualified service dog expert.
<b>Certifying personnel</b>	Personnel certification entails authoritatively attesting that individuals meet professional standards for the training, experience, and performance required for key incident management functions.



<b>Chain of Command 1</b>	A series of command and control (in hierarchical order of authority) executive, or management positions.
<b>Chain of Command 2</b>	The orderly line of authority within the ranks of the incident management organization.
<b>Chain reaction</b>	A process that initiates its own repetition. In a fission chain reaction, a fissile nucleus absorbs a neutron and fissions (splits) spontaneously, releasing additional neutrons. These, in turn, can be absorbed by other fissile nuclei, releasing still more neutrons. A fission chain reaction is self-sustaining when the number of neutrons released in a given time equals or exceeds the number of neutrons lost by absorption in non-fissile material or by escape from the system.
<b>Check-In 1</b>	All responders, regardless of agency affiliation, must report in to receive an assignment in accordance with the procedures established by the IC.
<b>Check-In 2</b>	The process through which resources first report to an incident. Check-in locations include the incident command post, Resources Unit, incident base, camps, staging areas, or directly on the site.
<b>Chemical agent</b>	A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect (e.g., lethal, blister, and incapacitating).
<b>Chief</b>	The ICS title for individuals responsible for management of functional sections: Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established as a separate section).
<b>Chimney effect</b>	Air movement in a building between floors caused by differential air temperature (differences in density), between the air inside and outside the building. It occurs in vertical shafts, such as elevators, stairwells, and conduit/wiring/piping chases. Hotter air inside the building will rise and be replaced by infiltration with colder outside air through the lower portions of the building. Conversely, reversing the temperature will reverse the flow (down the chimney). Also known as stack effect.
<b>Chronic exposure</b>	Exposure to a substance over a long period of time, possibly resulting in adverse health effects. See also acute exposure, fractionated exposure.
<b>Circulator service</b>	A ferry service on a fixed route without a fixed schedule.
<b>Clear zone</b>	An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.
<b>Closed circuit television (CCTV)</b>	An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.
<b>Coastal</b>	Pertaining to services providing intercity and interisland trips on saltwater and large freshwater lakes. Travel times range from 1 hour to 1 day. Service frequency often ranges from daily to weekly.
<b>Cobalt (Co)</b>	Gray, hard, magnetic, and somewhat malleable metal. Cobalt is relatively rare and generally obtained as a byproduct of other metals, such as copper. Its most common radioisotope, cobalt-60 (Co-60), is used in radiography and medical applications. Cobalt-60 emits beta particles and gamma rays during radioactive decay.
<b>Codec</b>	A device or program capable of performing encoding and decoding on a digital data stream or signal. The word codec may be a combination of any of the following: ‘Compressor-De-compressor’, ‘Coder-Decoder’, or ‘Compression/Decompression algorithm’.
<b>Coding</b>	Assigning numbers to types of data so that they can be readily tabulated.
<b>Collateral damage</b>	Injury to personnel or damage to buildings that are not the primary target of an attack.
<b>Collaterally protected construction</b>	Construction that provides protection against near-miss detonations of large general purpose military bombs.

<b>Collective dose</b>	The estimated dose for an area or region multiplied by the estimated population in that area or region.
<b>Collective protection</b>	Provision of a contaminant-free area where personnel can function without individual protective equipment such as a mask and protective garments
<b>Combating terrorism</b>	The full range of federal programs and activities applied against terrorism, domestically and abroad, regardless of the source or motive.
<b>Command</b>	The act of directing, and/or controlling resources at an incident by virtue of explicit legal, agency, or delegated authority. May also refer to the Incident Commander.
<b>Command post</b>	(See Incident Command Post)
<b>Command staff</b>	In an incident management organization, the Command Staff consists of the Incident Command and the special staff positions of Public Information Officer, Safety Officer, Liaison Officer, and other positions as required, who report directly to the Incident Commander. They may have an assistant or assistants, as needed.
<b>Commandant</b>	Head of the U.S. Coast Guard.
<b>Committed dose</b>	A dose that accounts for continuing exposures expected to be received over a long period of time (such as 30, 50, or 70 years) from radioactive materials that were deposited inside the body.
<b>Common operating picture<sup>1</sup></b>	A broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence.
<b>Common operating picture<sup>2</sup></b>	Offers an overview of an incident thereby providing incident information enabling the IC/UC and any supporting agencies and organizations to make effective, consistent, and timely decisions.
<b>Common terminology</b>	Normally used words and phrases—avoids the use of different words/phrases for same concepts, consistency, to allow diverse incident management and support organizations to work together across a wide variety of incident management functions and hazard scenarios.
<b>Communications</b>	Process of transmission of information through verbal, written, or symbolic means.
<b>Communications unit</b>	An organizational unit in the Logistics Section responsible for providing communication services at an incident or an EOC. A Communications Unit may also be a facility (e.g., a trailer or mobile van) used to support an Incident Communications Center.
<b>Communications/dispatch center</b>	Agency or interagency dispatcher centers, 911 call centers, emergency control or command dispatch centers, or any naming convention given to the facility and staff that handles emergency calls from the public and communication with emergency management/response personnel. Center can serve as a primary coordination and support element of the MACS for an incident until other elements of MACS are formally established.
<b>Community</b>	A political entity that has the authority to adopt and enforce laws and ordinances for the area under its jurisdiction. In most cases, the community is an incorporated town, city, township, village, or unincorporated area of a county; however, each state defines its own political subdivisions and forms of government.
<b>Commuter rail urban</b>	Passenger train service for short-distance travel between a central city and adjacent suburbs. Commuter rail does not include heavy-rail or light-rail service.
<b>Components and cladding</b>	Elements of the building envelope that do not qualify as part of the main wind-force resisting system.
<b>Computer-based training</b>	Any training that uses a computer as the focal point of instructional delivery. Training is provided through the use of computer hardware and software that guides the learner through an interactive learning program.

<b>Concentration</b>	The ratio of the amount of a specific substance in a given volume or mass of solution to the mass or volume of solvent.
<b>Concurrent Validity</b>	A statistical form of validity that compares two or more sets of data that have been gathered simultaneously.
<b>Conference of Radiation Control Program Directors (CRCPD)</b>	An organization whose members represent state radiation protection programs.
<b>Confidentiality</b>	Secrecy, the state of having the dissemination of certain information restricted.
<b>Consequence</b>	The negative effect, or effects, that can be expected if an asset or system is damaged, destroyed, or disrupted.
<b>Consequence Management <sup>1</sup></b>	Measures to alleviate the damage, loss, hardship or suffering caused by emergencies. These include measures to restore essential government services, protect public health and safety, and provide emergency relief to afflicted entities. Consequence management response is under the primary jurisdiction of the affected state and local governments. Federal agencies support local efforts under the coordination of the Federal Emergency Management Agency (FEMA).
<b>Consequence Management <sup>2</sup></b>	Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise the primary authority to respond to the consequences of terrorism.
<b>Consequences</b>	The severity of impact and probability of loss for a given threat scenario. Consequences may be measured in qualitative or quantitative terms.
<b>Construction (CON)</b>	Begins with the development, fabrication, or construction of the engineered design for the selected alternative and concludes with the delivery of the completed project. This phase include the inspection, review, and checkout of the delivered project and concludes with the determination that the delivered project meets the engineering specification.
<b>Contact List</b>	A list of team members and key players in a crisis. The list should include home phone numbers, pager numbers, cell phone numbers, etc.
<b>Container structures</b>	Structures built using shipping containers that are designed to withstand structural loadings associated with shipping, including Container Express (CONEX) and International Organization for Standardization (ISO) containers. Testing has shown that these structures behave similarly to buildings for the purposes of these standards.
<b>Containment protection mode</b>	Mode that consists of compartmentalizing the fire zones by closing the fire doors and, if the building is so equipped, the smoke dampers.
<b>Contamination</b>	The undesirable deposition of a chemical, biological, or radiological material on the surface of structures, areas, objects, or people.
<b>Contamination (radioactive)</b>	The deposition of unwanted radioactive material on the surfaces of structures, areas, objects, or people where it may be external or internal. See also decontamination.
<b>Contamination control area</b>	An area where personnel can safely remove contaminated IPE, put on clean IPE, and bring items into or out of a protected area in a proper air flow environment using the appropriate contamination control procedures.
<b>Contingency plan</b>	Plan maintained for emergency response, backup operations and post-disaster recovery for a system (or an entity) to ensure availability of critical resources and facilitate the continuity of operations in an emergency.
<b>Continuity of core business function</b>	Strategies to mitigate risks and alternative methods for ensuring the continuation of the entity's business functions, e.g., financial management, information technology, operations support, critical training and the primary reason(s) for being for the entity.

<b>Continuity of government (COG)</b>	Activities that address the continuance of constitutional governance. COG planning aims to preserve and/or reconstitute the institution of government and ensure that a department or agency's constitutional, legislative, and/or administrative responsibility are maintained. This is accomplished through succession of leadership, the predelegation of emergency authority, and active command and control during response and recovery operations.
<b>Continuity of operations</b>	Those plans and/or processes designed to ensure a viable capability exists to continue essential functions across a wide range of potential emergencies. The focus of this type of planning is to ensure the survivability of critical department/agency/entity functions (FEMA).
<b>Continuity of operations plans (COOP)</b>	Planning should be instituted (including all levels of government) across the private sector and nongovernmental organizations (NGOs), as appropriate, to ensure the continued performance of core capabilities and/or critical government operations during any potential incident.
<b>Continuity of services and operations</b>	Controls to ensure that, when unexpected events occur, departmental/agency minimum essential infrastructure services and operations, including computer operations, continue without interruption or are promptly resumed, and that critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.
<b>Contract security service</b>	Protective services provided by one entity, specializing in such services, to another entity on a compensated basis.
<b>Contractor</b>	Means an entity that performs tasks required on behalf of the oversight or rail transit agency. The rail transit agency may not be a contractor for the oversight agency.
<b>Control center</b>	A centrally located room or facility staffed by personnel charged with the oversight of specific situations and/or equipment.
<b>Control Group</b>	Subjects in an experiment who are not exposed to changes in the independent variables.
<b>Controlled area</b>	An area into which access is controlled or limited. It is that portion of a restricted area usually near or surrounding a limited or exclusion area. Correlates with exclusion zone.
<b>Controlled perimeter</b>	A physical boundary at which vehicle and personnel access is controlled at the perimeter of a site. Access control at a controlled perimeter should demonstrate the capability to search individuals and vehicles.
<b>Conventional construction</b>	Building construction that is not specifically designed to resist weapons or explosives effects. Conventional construction is designed only to resist common loadings and environmental effects such as wind, seismic, and snow loads.
<b>Conventional construction standoff distance</b>	The standoff distance at which conventional construction may be used for buildings without a specific analysis of blast effects, except as otherwise required in these standards.
<b>Conviction</b>	The act or process of judicially finding someone guilty of a crime; the state of having been proved guilty.
<b>Cooperating agency</b>	An agency supplying assistance other than direct operational or support functions or resources to the incident management effort.
<b>Coordinate</b>	To advance systematically an analysis and exchange of information among principals who have or may have a need to know certain information to carry out specific incident management responsibilities.
<b>Corrective action plan</b>	A plan developed by the rail transit agency that describes the actions the rail transit agency will take to minimize, control, correct, or eliminate hazards, and the schedule for implementing those actions.
<b>Corrective actions</b>	Implementing procedures that are based on lessons learned from actual incidents or from training and exercises.

<b>Correlation</b>	A measure of the degree of relationship between two variables.
<b>Cosmic radiation</b>	Radiation produced in outer space when heavy particles from other galaxies (nuclei of all known natural elements) bombard the earth. See also background radiation, terrestrial radiation.
<b>Cost</b>	Tangible items, such as money, equipment and operational expenses; and, intangibles such as lost productivity, morale, etc. A result of a specific action that constitutes a <i>decrease</i> in the production possibilities or welfare level of society.
<b>Counterintelligence</b>	Information gathered and activities conducted to protect against: espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.
<b>Countermeasure</b>	A countermeasure is an action intended to induce institutional, process, and physical changes that reduce risks to systems and assets. The countermeasure may address a vulnerability, threat, consequence, or overall system performance.
<b>Countermeasures</b>	Those activities taken to reduce the likelihood that a specific threat will result in harm. Countermeasures typically include the deployment and training of personnel, the implementation of procedures, the design or retrofit of facilities and vehicles; the use of specialized equipment, the installation of alarms/warning devices and supporting monitoring systems; and communications systems and protocols.
<b>Counterterrorism (CT)</b>	Offensive measures taken to prevent, deter, and respond to terrorism.
<b>Covert entry</b>	Attempts to enter a facility by using false credentials or stealth.
<b>Crash bar</b>	A mechanical egress device located on the interior side of a door that unlocks the door when pressure is applied in the direction of egress.
<b>Credentialing</b>	Providing documentation that can authenticate and verify the certification and identity of designated incident managers and emergency responders.
<b>Credible warning</b>	a believable but nonspecific message informing of danger from an imminent attack that has yet to be confirmed and lacks sufficient information for effective prevention.
<b>Crew</b>	The personnel engaged on-board ship, excluding the master and officers and the passengers on passenger ships.
<b>Crime</b>	An act or commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. Crime can be divided into four main categories: <ul style="list-style-type: none"> <li>- Reported</li> <li>- Unreported</li> <li>- Unacknowledged (store shrinkage),</li> <li>- Undetected</li> </ul> The majority of crime is represented by the last three categories. For CPTED purposes, crime is simply the by-product of a human function that is not working properly.
<b>Crime prevention</b>	The systematic study of the interrelationships among those who commit crime, the location where crime occurs, and the victims of crime to identify patterns, and develop operational and design/engineering strategies to reduce the likelihood of crime and public fear. Central elements of crime prevention include (1) Crime Prevention through Environmental Design (CPTED): Set of design principles used by law public safety professionals, architects and engineers, to limit the ability of the physical environment to support criminal activity and public fear; (2) Crime Prevention through Environmental Design (CPTED): Set of design principles used by law public safety professionals, architects and engineers, to limit the ability of the physical environment to support criminal activity and public fear; and (3) Situational crime prevention (SCP): A set of management, policy, and legal/prosecution measures applied within a physical space to

	address specific categories of criminal occurrences. SCP is often described as the operational equivalent of CPTED design principles.
<b>Crime prevention through environmental design (CPTED)</b>	A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. CPTED usually involves the use of three principles: natural surveillance (by placing physical features, activities, and people to maximize visibility); natural access control (through the judicious placement of entrances, exits, fencing, landscaping, and lighting); and territorial reinforcement (using buildings, fences, pavement, signs, and landscaping to express ownership).
<b>Criminal records</b>	Official records related to criminal cases.
<b>Crisis</b>	Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization's financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization's reputation, products, or officers, and therefore negatively impacting its future.
<b>Crisis management (CM)</b>	The measures taken to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.
<b>Crisis management</b> <sup>1</sup>	Intervention and coordination by individuals or teams before, during, and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.
<b>Crisis Management</b> <sup>2</sup>	Measures to resolve a hostile situation, investigate, and prepare a criminal case for prosecution under federal law. Crisis management response is under the primary jurisdiction of the federal government with the Federal Bureau of Investigation acting as the lead agency. Crisis management response involves measures to confirm the threat, investigate and locate the terrorists and their weapons, and capture the terrorists.
<b>Crisis management center</b>	A specific room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis.
<b>Crisis management planning</b>	A properly funded ongoing process supported by senior management to ensure that the necessary steps are taken to identify and analyze the adverse impact of crisis events, maintain viable recovery strategies, and provide overall coordination of the organization's timely and effective response to a crisis.
<b>Crisis management team</b>	A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.
<b>Criteria</b>	The individual (criterion) or collective stated qualifications (criteria) to be compared with an applicant's or employee's actual credentials, experience, or history in determining suitability for an employment decision (hiring or otherwise).
<b>Critical asset</b>	An asset that supports national security, national economic security, and/or crucial public health and safety activities (CIAO).
<b>Critical assets</b>	Those assets essential to the minimum operations of the organization, and to ensure the health and safety of the general public.
<b>Critical function</b>	Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization.
<b>Critical incident stress debriefing</b>	A formal, yet open, discussion of incident events, which is specifically directed to emergency response personnel to resolve the emotional aftermath of the incident.

<b>Critical infrastructure</b> <sup>1</sup>	Primary infrastructure systems (e.g., utilities, telecommunications, transportation, etc.) whose incapacity would have a debilitating impact on the organization's ability to function.
<b>Critical Infrastructure</b> <sup>2</sup>	Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.
<b>Critical Infrastructures</b>	The sophisticated facilities, systems, and functions, which include human assets and physical and cyber systems, that work together in processes that are highly interdependent to provide the foundation for our national security, governance, economic vitality, and way of life.
<b>Critical mass</b>	The minimum amount of fissile material that can achieve a self-sustaining nuclear chain reaction.
<b>Critical records</b>	Records or documents that, if damaged, destroyed, or lost, would cause considerable inconvenience to the organization and/or would require replacement or recreation at a considerable expense to the organization.
<b>Criticality</b>	A fission process where the neutron production rate equals the neutron loss rate to absorption or leakage. A nuclear reactor is "critical" when it is operating.
<b>Criticality assessment (CA)</b>	Factors affecting the criticality of assets include: (1) Loss and Damage Consequences – casualty risk, environmental impact, replacement costs, and replacement/downtime; (2) Consequences to Public Services – emergency response functions, government continuity, military importance; and (3) Consequences to the General Public – available alternatives, economic impact, public health impact, functional importance and symbolic importance.
<b>Cumulative dose</b>	The total dose resulting from repeated or continuous exposures of the same portion of the body, or of the whole body, to ionizing radiation.
<b>Curie (Ci)</b>	The traditional measure of radioactivity based on the observed decay rate of 1 gram of radium. One curie of radioactive material will have 37 billion disintegrations in 1 second.
<b>Cutaneous radiation syndrome (CRS)</b>	The complex syndrome resulting from radiation exposure of more than 200 rads to the skin. The immediate effects can be reddening and swelling of the exposed area (like a severe burn), blisters, ulcers on the skin, hair loss, and severe pain. Very large doses can result in permanent hair loss, scarring, altered skin color, deterioration of the affected body part, and death of the affected tissue (requiring surgery). For more information, see CDC's fact sheet "Acute Radiation Syndrome," at <a href="http://www.bt.cdc.gov/radiation/ars.asp">http://www.bt.cdc.gov/radiation/ars.asp</a> .
<b>Cyber security</b>	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and September 11 communications and control systems.
<b>Damage assessment</b> <sup>1</sup>	An appraisal or determination of the effects of the disaster on human, physical, economic, and natural resources.
<b>Damage assessment</b> <sup>2</sup>	The process used to appraise or determine the number of injuries and deaths, damage to public and private property, and the status of key facilities and services (e.g., hospitals and other health care facilities, fire and police stations, communications networks, water and sanitation systems, utilities, and transportation networks) resulting from a manmade or natural disaster.
<b>Damage potential</b>	The potential for negative effects—including immediate and long-term damage or loss, whether tangible or intangible—resulting from an unintentional event or an attack on an asset. Mission-related damage potential (i.e., impacts that are critical to the owner's transportation institutional mission, including destruction or damage causing loss or reduction of functionality) is of special importance, together with injury or loss of life, as well as impacts on

quality of life and morale. Damage potential grows as a function of an asset's criticality. However, a critical asset may be damaged without a total loss of functionality.

<b>Data</b>	Pieces of information.
<b>Data fusion</b>	Methods to collect and display various IDS sensors and systems information
<b>Data gathering panel</b>	A local processing unit that retrieves, processes, stores, and/or acts on information in the field.
<b>Data transmission equipment</b>	A path for transmitting data between two or more components (e.g., a sensor and alarm reporting system, a card reader and controller, a CCTV camera and monitor, or a transmitter and receiver).
<b>Decision tree</b>	A device used to portray alternative courses of action and relate them to alternative decisions showing all consequences of the decision. The tree represents alternative courses or series of actions related to a previous decision.
<b>Decision-making</b>	The process of evaluating and judging information gathered and relating it to the specific requirements of the position for which the applicant is applying.
<b>Deck house</b>	A small superstructure on the top deck of a vessel that contains the helm and other navigational instruments.
<b>Decontamination</b>	The reduction or removal of a chemical, biological, or radiological material from the surface of a structure, area, object, or person.
<b>Defeat</b>	To overcome or vanquish; to beat; to prevent the success of; overpower; foil.
<b>Defend</b>	To guard from attack; to protect by opposition to resistance; to prevent from being injured or destroyed.
<b>Defense layer</b>	Building design or exterior perimeter barriers intended to delay attempted forced entry.
<b>Defensive measures</b>	Protective measures that delay or prevent attack on an asset or that shield the asset from weapons, explosives, and CBR effects. Defensive measures include site work and building design.
<b>Delay rating</b>	A measure of the effectiveness of penetration protection of a defense layer.
<b>Delegation of authority</b>	A statement provided to the Incident Commander by the Agency Executive delegating authority and assigning responsibility. The Delegation of Authority can include objectives, priorities, expectations, constraints, and other considerations or guidelines as needed. Many agencies require written Delegation of Authority to be given to Incident Commanders prior to their assuming command on larger incidents. Same as the Letter of Expectation.
<b>Delivery tactic</b>	The method of delivering a CBR agent (external or internal release)
<b>Demobilization</b>	The orderly, safe, and efficient return of an incident resource to its original location and status.
<b>Demographics</b>	Statistics relating to groups of people, such as births, deaths, ages, ethnic composition.
<b>Deny</b>	To refuse access to.
<b>Department operations center</b>	An Emergency Operating Center, specific to a single department or agency. Their focus is on internal agency incident management and response. They are often linked to and, in most cases, are physically represented in a combined agency EOC by authorized agent(s) for the department or agency.
<b>Depleted uranium</b>	Uranium containing less than 0.7% uranium-235, the amount found in natural uranium. See also enriched uranium.
<b>Depth of field</b>	The regions in front of and behind the focused distance where the image remains in focus. With a greater depth of field, more of the scene near to far is in focus. Lens aperture and scene lighting will greatly influence the D.O.F.



<b>Deputy</b>	A fully qualified individual who, in the absence of a superior, can be delegated the authority to manage a functional operation or perform a specific task. In some cases, a deputy can act as relief for a superior and, therefore, must be fully qualified in the position. Deputies can be assigned to the Incident Commander, General Staff, and Branch Directors.
<b>Design</b>	A term which, within the CPTED context, encompasses people and their physical and social surroundings.
<b>Design basis threat</b>	The threat (aggressors, tactics, and associated weapons, tools, or explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.
<b>Design basis threat (DBT)</b>	The threat (e.g., tactics and associated weapons, tools, or explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.
<b>Design constraint</b>	Anything that restricts the design options for a protective system or that creates additional problems for which the design must compensate.
<b>Design team</b>	A group of individuals from various engineering and architectural disciplines responsible for the protective system design.
<b>Detect<sup>1</sup></b>	To discover; to find out.
<b>Detect<sup>2</sup></b>	Refers to the objective of a transit agency employee's observing the environment around them. This observation activity's objective is to detect suspicious things or activities, an imminent threat, or attack in progress on the transit agency's facilities, passengers/patrons, and/or themselves.
<b>Detection</b>	The discovery or finding of a metallic object. The detection of a metallic object is transmitted to the operator by some type of <i>alarm indicator</i> , typically a visual or audible indicator.
<b>Detection layer</b>	A ring of intrusion detection sensors located on or adjacent to a defensive layer or between two defensive layers.
<b>Detection measures</b>	Protective measures that detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the response force. Detection measures include Detection Systems, Assessment Systems, and Access Control System elements.
<b>Detection system elements</b>	Detection measures that detect the presence of intruders, weapons, or explosives. Detection System elements include Intrusion Detection Systems, weapons and explosives detectors, and guards.
<b>Detector axis</b>	An imaginary line passing through and perpendicular to the detector plane that is centered vertically and horizontally within the portal of the walk-through metal detector and points in the direction of the subject's motion through the portal.
<b>Detector dog</b>	A service dog selected by the trainer and qualified by recognized standards to perform searches for hidden substances, including narcotics and explosives. Dogs used for detection typically are trained to detect each of the following odors: Drug Odors – Cocaine (a.k.a., Powder and Crack), Heroin, LSD, Marijuana, burned Marijuana odor in cloth, Methadone, Methamphetamine (Ecstasy), and Mescaline (Peyote); and Explosive Odors – black powder, smokeless powder, gunpowder, Pyrodex, handguns, bullets, shotgun shells, firecrackers, dynamite, TNT, C4, detonating cord, Ammonium Nitrate, Composition B, Penolite, emulsions, RDX, and PETN.
<b>Detector floor</b>	The bottom plane of the detector portal.
<b>Detector response</b>	The electrical signal generated by the sensor or sensor circuit of the detector and caused by an object interacting with the magnetic field emitted by the detector. The detector response is the basis on which an alarm indication is derived.

<b>Deter</b> <sup>1</sup>	To discourage or keep (a person) from doing something through fear, anxiety, doubt, etc.
<b>Deter</b> <sup>2</sup>	Refers to an activity, procedure, or physical barrier that reduces the likelihood of an incident or attack.
<b>Deterministic effects</b>	Effects that can be related directly to the radiation dose received. The severity increases as the dose increases. A deterministic effect typically has a threshold below which the effect will not occur. See also stochastic effect, non-stochastic effect.
<b>DFDCS data fusion, display, and control</b>	Applies to an extremely wide variety of systems and software applications from a diverse field of vendors or integrators that cover the complete range of data fusion, display, and control management.
<b>Director</b>	The ICS title for individuals responsible for supervision of a Branch.
<b>Dirty bomb</b>	A device designed to spread radioactive material by conventional explosives when the bomb explodes. A dirty bomb kills or injures people through the initial blast of the conventional explosive and spreads radioactive contamination over possibly a large area—hence the term “dirty.” Such bombs could be miniature devices or large truck bombs. A dirty bomb is much simpler to make than a true nuclear weapon. See also radiological dispersal device.
<b>Disaster</b> <sup>1</sup>	An event, incident, or combination of incidents, not necessarily related to transit operations, that causes multiple injuries or widespread property damage on the system or in the public transportation system’s service area
<b>Disaster</b> <sup>2</sup>	An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths.
<b>Disaster field office (DFO)</b>	The office established in or near the designated area of a Presidentially declared major disaster to support federal and state response and recovery operations.
<b>Disaster mitigation</b>	Measures, procedures, and strategies designed to reduce either the likelihood or consequences of a disaster.
<b>Disaster recovery</b>	Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.
<b>Disaster recovery center (DRC)</b>	Places established in the area of a Presidentially declared major disaster, as soon as practicable, to provide victims the opportunity to apply in person for assistance and/or obtain information relating to that assistance.
<b>Disaster/emergency management program</b>	A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization.
<b>Dispatch</b> <sup>1</sup>	See operations control center.
<b>Dispatch</b> <sup>2</sup>	The ordered movement of a resource or resources to an assigned operational mission or an administrative move from one location to another.
<b>Dispersion</b>	A measure of the extent to which values of a variable differ.
<b>Division</b> <sup>1</sup>	The organizational level responsible for operations within a defined geographic area or with functional responsibility. The Division level is organizationally situated below the Branch.
<b>Division</b> <sup>2</sup>	The partition of an incident into geographical areas of operation. Divisions are established when the number of resources exceeds the manageable span of control of the Operations Chief. A division is located within the ICS organization between the branch and resources in the Operations Section.
<b>DoD components</b>	The Office of the Secretary of Defense (OSD); the Military Departments (including their National Guard and Reserve Components); the Chairman,

	Joint Chiefs of Staff and Joint Staff; the Combatant Commands; the Office of the Inspector General of the Department of Defense; the Defense Agencies; the DoD Field Activities; and all other organizational entities within DoD.
<b>Domestic terrorism</b>	The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.
<b>Door position switch</b>	A switch that changes state based on whether or not a door is closed. Typically, a switch mounted in a frame that is actuated by a magnet in a door.
<b>Door strike, electronic</b>	An electromechanical lock that releases a door plunger to unlock the door. Typically, an electronic door strike is mounted in place of or near a normal door strike plate.
<b>Dose (radiation)</b>	Radiation absorbed by a person's body. Several different terms describe radiation dose.
<b>Dose rate (radiation)</b>	A general term indicating the quantity (total or accumulated) of ionizing radiation or energy absorbed by a person or animal, per unit of time.
<b>Dosimeter</b>	A small portable instrument (such as a film badge, thermoluminescent dosimeter [TLD], or pocket dosimeter) for measuring and recording the total accumulated dose of ionizing radiation a person receives.
<b>Dosimetry: assessment</b>	(by measurement or calculation) of radiation dose
<b>Dual purpose (or dual use) dog</b>	A service dog selected by the trainer and qualified by recognized standards to perform two distinct functions. Traditionally these functions include general patrol and another specific type of detection.
<b>Dual technology sensor</b>	A sensor that combines two different technologies in one unit.
<b>Due diligence</b>	The attention and care that a reasonable person exercises under the circumstances to avoid harm to other persons or their property. Failure to make this effort is considered negligence.
<b>Duress alarm</b>	A binary sensor device activated covertly by personnel to annunciate to an IDS the occurrence of an alarm condition.
<b>Duress alarm devices</b>	Also known as panic buttons, these devices are designated specifically to initiate a panic alarm.
<b>DVR Digital video recorder</b>	Method of recording video signals from CCTV systems by digitizing the analog video signal, compressing, and saving on computer style hard disk storage.
<b>Dwell time or dwell cycle</b>	The period of time to purge an airlock compartment after protective garments are removed and personnel enter the inner airlock compartment.
<b>EBS Electronic badging system</b>	System that saves a user's picture and other relevant data (including, if required, biometric information) into a database. This information is used to create credentials that are used by guard force personnel and access control systems for both identification & access control.
<b>Effective dose</b>	A dosimetric quantity useful for comparing the overall health affects of irradiation of the whole body. It takes into account the absorbed doses received by various organs and tissues and weighs them according to present knowledge of the sensitivity of each organ to radiation. It also accounts for the type of radiation and the potential for each type to inflict biologic damage. The effective dose is used, for example, to compare the overall health detriments of different radionuclides in a given mix. The unit of effective dose is the sievert (Sv); 1 Sv = 1 J/kg.
<b>Effective half-life</b>	The time required for the amount of a radionuclide deposited in a living organism to be diminished by 50% as a result of the combined action of radioactive decay and biologic elimination. See also biological half-life, decay constant, radioactive half-life.

<b>Effective standoff distance</b>	A standoff distance less than the Conventional Construction Standoff Distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating construction or retrofit.
<b>Electroluminescent (EL)</b>	Luminescence resulting from the application of an alternating electrical current to phosphor.
<b>Electromagnetic pulse (EMP)</b>	A sharp pulse of energy radiated instantaneously by a nuclear detonation that may affect or damage electronic components and equipment. EMP can also be generated in lesser intensity by non-nuclear means in specific frequency ranges to perform the same disruptive function.
<b>Electronic emanations</b>	Electromagnetic emissions from computers, communications, electronics, wiring, and related equipment.
<b>Electronic medium based training</b>	Any training that uses an electronic technology as a method of effectively conveying instruction and/or information. Electronic technology includes but is not limited to video or audiocassettes and video conferencing.
<b>Electronic security system (ESS)</b>	An integrated system that encompasses interior and exterior sensors, closed circuit television systems for assessment of alarm conditions, Electronic Entry Control Systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.
<b>Emergency (emergency situation)</b>	An unexpected event related to the operation of passenger train service involving significant threat to the health or safety of one or more persons, requiring immediate action. Examples include: derailment, highway/rail grade crossing accident, passenger or employee fatality or serious illness/injury, evacuation of train, or security situation.
<b>Emergency<sup>1</sup></b>	Absent a Presidentially declared emergency, any incident(s), human-caused or natural, that requires responsive action to protect life or property. Under the <i>Robert T. Stafford Disaster Relief and Emergency Assistance Act</i> , an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.
<b>Emergency<sup>2</sup></b>	The most serious event and consists of any unwanted operational, civil, natural phenomenon, or security occurrence which could endanger or adversely affect people, property, or the environment.
<b>Emergency<sup>3</sup></b>	A situation which is life threatening to passengers, employees, or other citizens, or which causes significant damage to any transit vehicle or facility that requires assessment and repair, or which reduces the ability of the system to fulfill its mission within its service area.
<b>Emergency alert system (EAS)</b>	A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communications Commission (FCC). The system provides the President and other national, state, and local officials the means to broadcast emergency information to the public before, during, and after disasters.
<b>Emergency environmental health services</b>	Services required to correct or improve damaging environmental health effects on humans, including inspection for food contamination, inspection for water contamination, and vector control; providing for sewage and solid waste inspection and disposal; cleanup and disposal of hazardous materials; and sanitation inspection for emergency shelter facilities.
<b>Emergency exit locator signs</b>	Conspicuously marked emergency marking/signage used to identify and/or direct passengers to the nearest emergency exit location.
<b>Emergency management</b>	The development, coordination and direction of planning, preparedness, and readiness assurance activities.

<b>Emergency management assistance compact (EMAC)</b>	A congressionally ratified organization that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected State can request and receive assistance from other member States quickly and efficiently, resolving two key issues upfront: liability and reimbursement.
<b>Emergency management/response personnel</b>	Includes Federal, State, territorial, tribal, substate regional, and local governments, private sector organizations, critical infrastructure owners and operators, NGOs, and all other organizations and individuals who assume an emergency management role. Also known as Emergency Responder.
<b>Emergency medical services (EMS)</b>	Services including personnel, facilities, and equipment required to ensure proper medical care for the sick and injured from the time of injury to the time of final disposition, including medical disposition within a hospital, temporary medical facility, or special care facility; release from the site; or declared dead. Further, Emergency Medical Services specifically include those services immediately required to ensure proper medical care and specialized treatment for patients in a hospital and coordination of related hospital services.
<b>Emergency mortuary services</b>	Services required to assure adequate death investigation, identification, and disposition of bodies; removal, temporary storage, and transportation of bodies to temporary morgue facilities; notification of next of kin; and coordination of mortuary services and burial of unclaimed bodies.
<b>Emergency operating procedure (EOP)</b>	Any transportation system procedure that details activities to be performed by transit employees when normal operations are not possible.
<b>Emergency operations center (EOC)<sup>2</sup></b>	Special policy and incident management area, activated under certain conditions and staffed by representatives from the transit system, including top management, to serve as an information coordination point during special events or emergencies, and to authorize decisions that require/affect the legal authority of the system.
<b>Emergency operations center (EOC)<sup>3</sup></b>	The protected site from which state and local civil government officials coordinate, monitor, and direct emergency response activities during an emergency.
<b>Emergency operations center<sup>1</sup></b>	A location from which centralized emergency management can be performed. EOC facilities are established by an agency or jurisdiction to coordinate the overall agency or jurisdictional response and support to an emergency.
<b>Emergency operations centers (EOCs)<sup>4</sup></b>	The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof.
<b>Emergency operations plan (EOP)<sup>2</sup></b>	A document that describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.
<b>Emergency operations plan<sup>1</sup></b>	The ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.
<b>Emergency plan</b>	A brief, clear and concise description of the overall emergency organization, designation of responsibilities, and descriptions of the procedures, including notifications, involved in coping with any or all aspects of a potential credible emergency.
<b>Emergency preparedness<sup>1</sup></b>	A uniform basis for operating policies and procedures for mobilizing public transportation system and other public safety resources to assure rapid, controlled, and predictable responses to various types of transportation and community emergencies.
<b>Emergency preparedness<sup>2</sup></b>	The training of personnel, acquisition and maintenance of resources, and exercising of the plans, procedures, personnel and resources essential for emergency response.

<b>Emergency public information (EPI)</b>	Information that is disseminated primarily in anticipation of an emergency or at the actual time of an emergency and, in addition to providing information, frequently directs actions, instructs, and transmits direct orders.
<b>Emergency response provider</b>	Includes Federal, State, local, and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.
<b>Emergency response team (ERT).</b>	An interagency team, consisting of the lead representative from each federal department or agency assigned primary responsibility for an ESF and key members of the FCO's staff, formed to assist the FCO in carrying out his/her coordination responsibilities.
<b>Emergency response team advance element (ERT-A).</b>	For federal disaster response and recovery activities under the Stafford Act, the portion of the ERT that is first deployed to the field to respond to a disaster incident. The ERT-A is the nucleus of the full ERT.
<b>Emergency response team national (ERT-N)</b>	An ERT that has been established and rostered for deployment to catastrophic disasters where the resources of the FEMA Region have been, or are expected to be, overwhelmed. Three ERT-Ns have been established.
<b>Emergency signage</b>	Textual and graphic messages designed to assist passengers and crew in exiting a rail car in an emergency and to assist emergency responders in gaining access to rail cars from the exterior.
<b>Emergency support function (ESF)</b>	In the Federal Response Plan (FRP), a functional area of response activity established to facilitate the delivery of federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and to maintain public safety. ESFs represent those types of federal assistance that the state will most likely need because of the impact of a catastrophic or significant disaster on its own resources and response capabilities, or because of the specialized or unique nature of the assistance required. ESF missions are designed to supplement state and local response efforts.
<b>Emergency support team (EST)</b>	An interagency group operating from FEMA Headquarters. The EST oversees the national-level response support effort under the FRP and coordinates activities with the ESF primary and support agencies in supporting federal requirements in the field.
<b>Emergency vehicles</b>	Vehicles such as fire trucks and ambulances that are critical to emergency response, and for which close proximity to inhabited buildings or containment therein is essential.
<b>Employment verification</b>	The process of contacting an applicant's past employers to confirm dates of employment, title, salary, and eligibility for rehire.
<b>Enriched uranium</b>	Uranium in which the proportion of the isotope uranium-235 has been increased by removing uranium-238 mechanically. See also depleted uranium.
<b>Entity</b>	A governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has disaster/emergency management and continuity of operations responsibilities.
<b>Entity-wide security</b>	Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.
<b>Entry control point</b>	A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.
<b>Entry control stations</b>	Entry control stations should be provided at main perimeter entrances where security personnel are present. Entry control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.
<b>Envelope</b>	Everything that separates the interior of a building, or portion of a building, from the exterior environment, including the windows, walls, foundation, basement, slab, floor, ceiling, roof, and insulation

<b>Environmental Design</b>	A term which, within the CPTED context, is rooted in the design of the man/environment relation.
<b>Epidemiology</b>	The study of the distribution and determinants of health-related states or events in specified populations; and the application of this study to the control of health problems.
<b>Equipment closet</b>	A room where field control equipment such as data gathering panels and power supplies are typically located.
<b>Equivalent security measure</b>	An alternative measure that can take the place of a 33 CFR 104 and 105 required measure. Equivalent security measures must be approved by the commandant (G-MP) as meeting or exceeding the effectiveness of the required measures in 33 CFR 104 and 105.
<b>Essential service routes</b>	Routes used when no other modes of transportation are available to the specific destination serviced.
<b>EVAC</b>	An immediate action that includes the following steps: (1) E for Evacuate the immediate area (train, bus, or building); (2) V for Vacate the general area – keep going and put distance and barriers in place between you and the incident; (3) A for Assess the situation and continue to protect yourself and others; and (4) C for Communicate by calling in a report.
<b>Evacuation</b>	Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.
<b>Evacuation of passengers</b>	The controlled removal of passengers from a bus, train or other transit vehicle during an emergency situation.
<b>Evacuation, spontaneous</b>	Residents or citizens in the threatened areas observe an emergency event or receive unofficial word of an actual or perceived threat and, without receiving instructions to do so, elect to evacuate the area. Their movement, means, and direction of travel are unorganized and unsupervised.
<b>Evacuation, voluntary</b>	This is a warning to persons within a designated area that a threat to life and property exists or is likely to exist in the immediate future. Individuals issued this type of warning or order are NOT required to evacuate; however, it would be to their advantage to do so.
<b>Evacuees</b>	All persons removed or moving from areas threatened or struck by a disaster.
<b>Evaluation and maintenance</b>	Process by which a business continuity plan is reviewed in accordance with a predetermined schedule and modified in light of such factors as new legal or regulatory requirements, changes to external environments, technological changes, test/exercise results, personnel changes, etc.
<b>Event<sup>1</sup></b>	An occurrence, not yet assessed, that may affect the performance of a system (or an entity) (CIAO). Any real-time occurrence or significant deviation from planned or expected behavior that could endanger or adversely affect people, property, or the environment.
<b>Event<sup>2</sup></b>	A planned, nonemergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.
<b>Exclusion area</b>	A restricted area containing a security interest. Uncontrolled movement permits direct access to the item.
<b>Exclusion zone</b>	An area around an asset that has controlled entry with highly restrictive access.
<b>Exercise</b>	A comprehensive training event that involves several of the functional elements of the area maritime security, vessel, or facility security plan.
<b>Expeditionary situations</b>	Situations in which existing facilities are unavailable or inadequate for incorporating CBR protection features and transportable or mobile facilities are used for field applications.
<b>Experiment</b>	A controlled event designed to determine the relationship between two or more variables.

<b>Explosives disposal container</b>	A small container into which small quantities of explosives may be placed to contain their blast pressures and fragments if the explosive detonates.
<b>Exposure (radiation)</b>	A measure of ionization in air caused by x-rays or gamma rays only. The unit of exposure most often used is the roentgen. See also contamination.
<b>Exposure (to risk)</b>	The number, types, qualities, and monetary values of various types of property or infrastructure and life that may be subject to an undesirable or injurious hazard event. The condition of being vulnerable to some degree to a particular outcome of an activity, if that outcome occurs.
<b>Exposure pathway</b>	A route by which a radionuclide or other toxic material can enter the body. The main exposure routes are inhalation, ingestion, absorption through the skin, and entry through a cut or wound in the skin.
<b>Exposure rate</b>	A measure of the ionization produced in air by x-rays or gamma rays per unit of time (frequently expressed in roentgens per hour).
<b>Express Services</b>	Ferry services that generally operate during peak commuter hours by both demand based and fixed-route service.
<b>External exposure</b>	Exposure to radiation outside of the body.
<b>Externality</b>	The discrepancy between private and social costs or private and social benefits.
<b>Externally illuminated</b>	The light source is contained outside the device, legend, or path to be illuminated. The light source is typically fluorescent, incandescent or a dedicated fluorescent or incandescent source.
<b>Facial recognition</b>	A biometric technology that is based on features of the human face.
<b>Facility</b>	Any structure that is located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. A facility may be used, operated, or maintained by a public or private entity, including any contiguous or adjoining property under common ownership or operations.
<b>Facility security officer</b>	The person responsible for the development, implementation, revision, and maintenance of the facility security.
<b>Facility security plan</b>	The plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on-board at the respective MARSEC levels.
<b>Fallout, nuclear</b>	Minute particles of radioactive debris that descend slowly from the atmosphere after a nuclear explosion.
<b>Federal</b>	Of or pertaining to the Federal Government of the United States of America.
<b>Federal coordinating officer (FCO)</b>	The person appointed by the FEMA Director to coordinate federal assistance in a Presidentially declared emergency or major disaster.
<b>Federal departments and agencies</b>	Those executive departments enumerated in 5 U.S.C. 11, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 14(1); Government corporations as defined by 5 U.S.C. 13(1); and the United States Postal Service. ( <i>HSPD-8</i> )
<b>Federal on-scene commander</b>	The FBI official designated upon JOC activation to ensure appropriate coordination of the overall United States government response with federal, state, and local authorities, until such time as the Attorney General transfers the LFA role to FEMA.
<b>Federal response plan (FRP)</b>	Establishes a process and structure for the systematic, coordinated, and effective delivery of federal assistance to address the consequences of any major disaster or emergency.
<b>Felony</b>	A serious crime usually punishable by imprisonment for more than one year or by death. Examples include burglary, arson, rape, and murder.
<b>Fence protection</b>	An intrusion detection technology that detects a person crossing a fence by various methods such as climbing, crawling, cutting, etc.



<b>Fence sensor</b>	An exterior intrusion detection sensor that detects aggressors as they attempt to climb over, cut through, or otherwise disturb a fence.
<b>Ferry</b>	A vessel that (a) is limited in its use to the carriage of deck passengers or vehicles, or both and (b) operates on a short-run, frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service. A ferry may also be a hovercraft, hydrofoil, or other high-speed vessel.
<b>Ferry service</b>	Urban Service where at least one terminal is within an urbanized area. Such service excludes international, rural, rural Interstate, island, and urban park ferries.
<b>Ferry service express</b>	Service that may operate in peak hours bypassing intervening islands. Alternatively, some trips may be operated by high-speed or passenger-only ferries as opposed to the regular ferry, which could be considered as express service of a sort.
<b>Ferry service transit</b>	A service confined to metropolitan areas and small cities where offshore islands, bays, and wide rivers preclude any other type of service at a reasonable cost. In a few places, service may operate between two points on the same shore.
<b>Fiber optics</b>	A method of data transfer by passing bursts of light through a strand of glass or clear plastic.
<b>Field assessment team (FAST)</b>	A small team of pre-identified technical experts that conduct an assessment of response needs (not a PDA) immediately following a disaster.
<b>Field of view</b>	The horizontal or vertical scene size at a given length from the camera to the subject.
<b>Field operations guide</b>	Durable pocket or desk guides that contain essential information required to perform specific assignments or functions.
<b>Final design (FD)</b>	Takes the formalized concept and engineering development and finalizes them in the plans, specifications, and bid documents required for awarding the individual construction and equipment fabrication and installation contracts.
<b>Finance/administration section <sup>1</sup></b>	A part of the general structure of the incident command system activated on long duration incidents, responsible for cost accounting and financial analysis of the incident. At the incident the Section can include the Time Unit, Procurement Unit, Compensation/Claims Unit and Cost Unit.
<b>Finance/administration section <sup>2</sup></b>	The section responsible for all administrative and financial considerations surrounding an incident.
<b>Financial mechanisms</b>	One of the three mitigation strategy classifications (engineering alternatives; management practices; <i>financial mechanisms</i> ). A set of devices relating to finances that facility owners and managers can utilize to reduce their exposure to natural and man-made hazards. These devices include purchase of insurance policies and responding to external financial incentives to engage in engineering-based or management-based risk mitigation.
<b>First (initial) costs</b>	Attribute of a capital investment. Costs incurred in placing a building or building subsystem into service, including, but not limited to, costs of planning, design, engineering, site acquisition and preparation, construction, purchase, installation, property taxes and interest during the construction period, and construction-related fees.
<b>First responder <sup>1</sup></b>	Those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6U.S.C. 11), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations. ( <i>HSPD-8</i> )
<b>First responder <sup>2</sup></b>	Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

<b>Fissile material</b>	Any material in which neutrons can cause a fission reaction. The three primary fissile materials are uranium-233, uranium-235, and plutonium-239.
<b>Fission (fissioning)</b>	The splitting of a nucleus into at least two other nuclei that releases a large amount of energy. Two or three neutrons are usually released during this transformation. See also fusion.
<b>Fixed guideways</b>	Service in which the beginning and ending points are fixed. By law, ferryboat services are considered fixed guideways. Though each trip may take a slightly different course due to water conditions, the beginning and ending points are fixed.
<b>Fixed routes</b>	Routes that have a fixed point for a beginning and end. By law, ferryboats are considered fixed guideways. Each trip may take a slightly different course, but the end and beginning are fixed points.
<b>Fixed-route</b>	Service provided on a repetitive, fixed-schedule basis along a specific route with vehicles stopping to pick up and deliver passengers to specific locations; each fixed-route trip serves the same origins and destinations, unlike demand response. Includes route deviation service, where revenue vehicles deviate from fixed routes on a discretionary basis.
<b>F-number</b>	Indicates the brightness of the image formed by the lens, controlled by the iris. The smaller the F-number the brighter the image.
<b>Force protection conditions</b>	A set of specific security measures promulgated by the commander after considering a variety of factors including the design basis threat, current events that might increase the risk of a terrorist attack, and observed suspicious activities.
<b>Forced entry</b>	Entry to a denied area achieved through force to create an opening in fence, walls, doors, etc., or to overpower guards.
<b>Fractionated exposure</b>	Exposure to radiation that occurs in several small acute exposures, rather than continuously as in a chronic exposure.
<b>Fragment retention film (FRF)</b>	A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.
<b>Frame rate</b>	In digital video, a measurement of the rate of change in a series of pictures, often measured in frames per second (fps).
<b>Frangible construction</b>	Building components that are designed to fail to vent blast pressures from an enclosure in a controlled manner and direction.
<b>Frequency Distribution</b>	A table where all score units are listed in one column and the number of individuals or cases receiving each score are indicated as frequencies in the second column.
<b>F-Stop</b>	A term used to indicate the speed of a lens. The smaller the F-number the greater amount of light passes through the lens.
<b>Function<sup>1</sup></b>	The service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.
<b>Function<sup>2</sup></b>	Function refers to the five major activities in ICS: Command, Operations, Planning, Logistics, and Finance/Administration. The term function is also used when describing the activity involved, e.g., the planning function. A sixth function, Intelligence/Investigations, may be established, if required, to meet incident management needs.
<b>Fuse</b>	A device used to protect an electric circuit from the effect of excessive current draw.
<b>Fusion</b>	A reaction in which at least one heavier, more stable nucleus is produced from two lighter, less stable nuclei. Reactions of this type are responsible for the release of energy in stars or in thermonuclear weapons.
<b>Gamma rays</b>	High-energy electromagnetic radiation emitted by certain radionuclides when their nuclei transition from a higher to a lower energy state. These rays have

	high energy and a short wave length. All gamma rays emitted from a given isotope have the same energy, a characteristic that enables scientists to identify which gamma emitters are present in a sample. Gamma rays penetrate tissue farther than do beta or alpha particles, but leave a lower concentration of ions in their path to potentially cause cell damage. Gamma rays are very similar to x-rays.
<b>Gangway</b>	A narrow, portable platform used as a passage by persons entering or leaving a vessel moored alongside a pier or quay.
<b>Geiger counter</b>	A radiation detection and measuring instrument consisting of a gas-filled tube containing electrodes, between which an electrical voltage but no current flows. When ionizing radiation passes through the tube, a short, intense pulse of current passes from the negative electrode to the positive electrode and is measured or counted. The number of pulses per second measures the intensity of the radiation field. Geiger counters are the most commonly used portable radiation detection instruments.
<b>General staff</b>	A group of incident management personnel organized according to function and reporting to the Incident Commander. The General Staff normally consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief. An Intelligence/Investigations Chief may be established, if required, to meet incident management needs.
<b>Genetic effects</b>	Hereditary effects (mutations) that can be passed on through reproduction because of changes in sperm or ova. See also somatic effects.
<b>Geographic information system (GIS)</b>	A computer system that integrates, stores, edits, and analyzes geographic information.
<b>Geophone</b>	An IDS sensor that utilizes sound and pressure to detect intrusions
<b>Glare security lighting</b>	Illumination projected from a secure perimeter into the surrounding area, making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.
<b>Glass-break detector</b>	An intrusion detection sensor that is designed to detect breaking glass either through vibration or acoustics.
<b>Glazing</b>	A material installed in a sash, ventilator, or panes (e.g., glass, plastic, etc., including material such as thin granite installed in a curtain wall).
<b>Glazing</b>	The part of a window, skylight, or door assembly that is transparent and transmits light, but not air.
<b>Government Coordinating Council (GCC)</b>	The council comprised of representatives across various levels of government (Federal, State, local, and tribal) as appropriate to the security and operational landscape of each individual sector. The GCC is the government counterpart to the Sector Coordinating Council (SCC) for each sector established to enable interagency coordination.
<b>Governor's authorized representative (GAR)</b>	The person empowered by the Governor to execute, on behalf of the State, all necessary documents for disaster assistance.
<b>Gray (Gy)</b>	A unit of measurement for absorbed dose. It measures the amount of energy absorbed in a material. The unit Gy can be used for any type of radiation, but it does not describe the biological effects of the different radiations.
<b>Grid wire sensor</b>	An intrusion detection sensor that uses a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.
<b>Gross tons</b>	The internal cubic capacity of all spaces in and on the vessel that are permanently enclosed, with the exception of certain permissible exemptions. It is expressed in tons of 100 cubic feet.
<b>Ground surface</b>	The surface on which the walk-through detector rests.
<b>Group</b>	Established to divide the incident management structure into functional areas of operation. Groups are composed of resources assembled to perform a special

	function not necessarily within a single geographic division. Groups, when activated, are located between Branches and resources in the Operations Section.
<b>Grouped frequency distribution</b>	Where individual score units are grouped together, reducing the number of discrete categories listed in the score column.
<b>Half-life</b>	The time any substance takes to decay by half of its original amount. See also effective half-life and radioactive half-life.
<b>Hand geometry</b>	A biometric technology that is based on characteristics of the human hand.
<b>Handler</b>	An officer, contractor, or other person qualified by the trainer and/or a certifying agency to care for and use a service dog.
<b>Hardened construction</b>	Below ground construction designed to resist nuclear weapons effects.
<b>Hard-wired radio</b>	A radio communications device permanently mounted in a railroad vehicle and permanently connected to an antenna mounted on the vehicle.
<b>Hazard<sup>1</sup></b>	A source of potential danger or adverse condition.
<b>Hazard<sup>2</sup></b>	Any real or potential condition that can cause injury, death, or damage or loss of equipment or property.
<b>Hazard<sup>3</sup></b>	An event or physical condition that has the potential to cause fatalities, injuries, property damage, infrastructure damage, agricultural loss, damage to the environment, interruption of business, or other types of harm or loss.
<b>Hazard mitigation</b>	Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event.
<b>Hazardous material (HazMat)</b>	Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.
<b>Health physics</b>	A scientific field that focuses on protection of humans and the environment from radiation. Health physics uses physics, biology, chemistry, statistics, and electronic instrumentation to help protect individuals from any damaging effects of radiation.
<b>High-performance photoluminescent material (HPPL)</b>	A material that is capable of emitting fluorescent and/or phosphorescent light at a high rate and for an extended period of time after absorption of light radiation from an external source by the process of photon excitation. NOTE—Following a charge of 5 foot-candles for one hour, the measured value of light emitted shall be a minimum of not less than 7.5 milli-candela per square meter (7.5 mcd/m <sup>2</sup> ) 1.5 hours after removal of the charging source.
<b>High-level radioactive waste</b>	The radioactive material resulting from spent nuclear fuel reprocessing. This can include liquid waste directly produced in reprocessing or any solid material derived from the liquid wastes having a sufficient concentration of fission products. Other radioactive materials can be designated as high-level waste, if they require permanent isolation. This determination is made by the U.S. Nuclear Regulatory Commission on the basis of criteria established in U.S. law. See also low-level waste.
<b>High-occupancy</b>	Vehicle A highway travel lane reserved for vehicles carrying two or more passengers.
<b>High-risk areas</b>	Portions of a building that are at a high risk of an internal release, such as mail-rooms, lobby areas, and supply delivery areas with separate ventilation systems as well as unscreened public access areas and any other general-access areas.
<b>High-risk target</b>	Any material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

<b>Homeland security</b>	The federal government's efforts, in coordination with state and local governments and the private sector, to develop, coordinate, fund and implement the programs and policies necessary to detect, prepare for, prevent, protect against, respond to, and recover from terrorist or other attacks within the United States.
<b>Homogeneity</b>	Uniformity of a factor within a group of subjects or data, such as age, occupation, religion.
<b>Hot spot</b>	Any place where the level of radioactive contamination is considerably greater than the area around it.
<b>Hovercraft</b>	A vessel used for the transportation of passengers and cargo that rides on a cushion of air formed under it. It is very maneuverable and amphibious.
<b>Human-caused hazard</b>	Human-caused hazards are technological hazards and terrorism. They are distinct from natural hazards primarily in that they originate from human activity. Within the military services, the term threat is typically used for human-caused hazard.
<b>Hunting</b>	An industry term used to describe a auto-iris lenses inability to stabilize under certain light conditions.
<b>Hydrofoil</b>	A motorboat that has metal plates or fins attached by struts fore and aft for lifting the hull clear of the water as speed is attained.
<b>I frames</b>	I-frames are used for random access and are used as references for the decoding of other pictures. Intra refresh periods of a half-second are common on such applications as digital television broadcast and DVD storage
<b>Icon</b>	A sign or representation that stands for an object by virtue of a resemblance or analogy to it.
<b>Identification and authentication</b>	Individuals and organizations that access the NIMS information management system and, in particular, those that contribute information to the system (e.g., situation reports), must be properly authenticated and certified for security purposes.
<b>Illuminance</b>	The amount of light (luminous flux) falling on a specific area or surface. English units are foot-candles (fc) or lumens per sq. foot (Lm/ft <sup>2</sup> ). International units (SI) are lumen per sq. meter (Lm/m <sup>2</sup> ) or lux (lx).
<b>Immediate actions (IAs)</b>	Actions transit agency employees are trained to perform in anticipation or response to a potential attack until further instructions are available. The steps are taken immediately (without management direction) upon awareness of a potential or actual incident. IAs are intended to provide immediate protection of life and property and generally take a very short time to execute. The IA ends with a notification to management (e.g., the communications center) of the conditions present.
<b>Immediate response zone (IRZ)</b>	A circular zone ranging from 10 to 15 kilometers (6 to 9 miles) from the potential chemical event source, depending on the stockpile location on-post. Emergency response plans developed for the IRZ must provide for the most rapid and effective protective actions possible, because the IRZ will have the highest concentration of agent and the least amount of warning time.
<b>Imminent threat</b>	The immediate potential of harm to people and property.
<b>Impact</b>	The amount of loss or damage that can be expected or may be expected from a successful attack of an asset (ARM).
<b>Incarceration</b>	The act or process of confining someone; imprisonment.
<b>Incident<sup>2</sup></b>	An occurrence that has been assessed as having an adverse effect of the security of performance of a critical infrastructure.
<b>Incident<sup>1</sup></b>	An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents,

earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

<b>Incident action plan</b>	An oral or written plan containing general objectives reflecting the overall strategy for managing an incident.
<b>Incident command</b>	Responsible for overall management of the incident and consists of the Incident Commander, either single or unified command, and any assigned supporting staff.
<b>Incident command post (ICP)</b>	The field location at which the primary tactical-level, on-scene incident command functions are performed. The ICP may be collocated with the incident base or other incident facilities and is normally identified by a green rotating or flashing light.
<b>Incident command system (ICS)<sup>1</sup></b>	A standardized organizational structure used to command, control, and coordinate the use of resources and personnel that have responded to the scene of an emergency. The concepts and principles for ICS include common terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.
<b>Incident Command System (ICS)<sup>2</sup></b>	The nationally used, standardized, on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, with responsibility for the management of resources to effectively accomplish stated objectives pertinent to an incident.
<b>Incident commander (IC)</b>	The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.
<b>Incident management</b>	The broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all levels of government, utilizing both governmental and nongovernmental resources to plan for, respond to, and recover from an incident, regardless of cause, size, or complexity.
<b>Incident management system</b>	In disaster/emergency management applications, the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for the management of assigned resources to effectively accomplish stated objectives pertaining to an incident.
<b>Incident management team (IMT)</b>	An IC and the appropriate Command and General Staff personnel assigned to an incident. The level of training and experience of the IMT members, coupled with the identified formal response requirements and responsibilities of the IMT, are factors in determining “type,” or level, of IMT.
<b>Incident objectives</b>	Statements of guidance and direction needed to select appropriate strategy(s) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives.
<b>Incident of national significance</b>	Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high-impact event that requires a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term community and economic recovery.
<b>Incident/attack</b>	An act against the transit system’s facilities, passengers/patrons, and employees.

<b>Independent variable</b>	A variable that causes, effects, or influences the outcome of an experiment.
<b>Individual</b>	A passenger; employee; contractor; other rail transit facility worker; pedestrian; trespasser; or any person on rail transit-controlled property.
<b>Infiltration</b>	The uncontrolled exchange of the building's interior air with outside air.
<b>Inflation</b>	A rise in the general price level over time, usually expressed as a percentage rate.
<b>Information management</b>	The collection, organization, and control over the structure, processing, and delivery of information from one or more sources and distribution to one or more audiences who have a stake in that information.
<b>Infrastructure</b>	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.
<b>Ingestion</b>	The act of swallowing; in the case of radionuclides or chemicals, swallowing radionuclides or chemicals by eating or drinking.
<b>Ingestion pathway (50-mile EPZ)</b>	A circular geographic zone (with a 50-mile radius centered at the nuclear power plant) for which plans are developed to protect the public from the ingestion of water or food contaminated as a result of a nuclear power plant accident.
<b>Inhalation</b>	The act of breathing in; in the case of radionuclides or chemicals, breathing in radionuclides or chemicals.
<b>Initial action</b>	The actions taken by those responders first to arrive at an incident site.
<b>Initial response</b>	Resources initially committed to an incident.
<b>Innocuous item test objects</b>	Test objects used to test the discrimination performance of the large object size and medium object size walk-through metal detectors.
<b>Insider compromise</b>	A person authorized access to a facility (an insider) compromises assets by taking advantage of that accessibility.
<b>Integrated testing (INT-TEST)</b>	Begins with activities to identify, plan and conduct tests to evaluate integration of the delivered and accepted project into planned revenue operations. This phase concludes with verified documentation of compatibility between system elements.
<b>Intellectual property rights (IPR)</b>	A category of intangible rights protecting commercially valuable products of the human intellect. The category comprises primarily trademark, copyright, and patent rights, but also includes trade secret rights, publicity rights, moral rights, and rights against unfair competition. (Note: Some areas of the world differ significantly in their recognition and enforcement of patents, trademarks, copyrights, and other IPR. It is important to understand the IPR climate and the ability of the legal safeguards that are applicable in each jurisdiction where there is a necessity to support your business requirements.)
<b>Intelligence officer</b>	The intelligence officer is responsible for managing internal information, intelligence, and operational security requirements supporting incident management activities. These may include information security and operational security activities, as well as the complex task of ensuring that sensitive information of all types (e.g., classified information, law enforcement sensitive information, proprietary information, or export-controlled information) is handled in a way that not only safeguards the information, but also ensures that it gets to those who need access to it to perform their missions effectively and safely.
<b>Intelligence/investigations</b>	Intelligence gathered within the Intelligence/Investigations function is information that either leads to the detection, prevention, apprehension, and prosecution of criminal activities (or the individual(s) involved) including terrorist incidents or information that leads to determination of the cause of a given incident (regardless of the source) such as public health events or fires with unknown origins. This is different from the normal operational and situational intelligence gathered and reported by the Planning Section.

<b>Intercity</b>	Connecting two or more cities.
<b>Intercoastal</b>	Describing external waterways that run along coasts or gulfs.
<b>Intercom</b>	A communications system within a train consist which is keyed into by a train crewmember for transmission/broadcast to/from specific locations within the train and used to provide train crew-to-passenger communication and intra-crew communication.
<b>Intercom door/gate station</b>	Part of an intercom system where communication is typically initiated, usually located at a door or gate.
<b>Intercom master station</b>	Part of an intercom system that monitors one or more intercom door/gate stations; typically, where initial communication is received.
<b>Intercom switcher</b>	Part of an intercom system that controls the flow of communications between various stations.
<b>Intercom system</b>	An electronic system that allows simplex, half-duplex, or full-duplex audio communications.
<b>Interdependency</b>	The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.
<b>Intermodal</b>	Those issues or activities which involve or affect more than one mode of transportation, including transportation connections, choices, cooperation and coordination of various modes. Also known as “multimodal.”
<b>Internal exposure</b>	Exposure to radioactive material taken into the body.
<b>Internally illuminated</b>	The light source is contained inside the device or legend that is illuminated. The light source is typically incandescent, fluorescent, electroluminescent, light-emitting diodes (LED) or self-illuminating.
<b>International terrorism</b>	Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
<b>Interoperability</b>	Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video—on—demand, in real—time, when needed, and when authorized.
<b>Interstate</b>	Connecting two or more states.
<b>Intracoastal</b>	Describing internal waterways such as lakes, rivers, and harbor.
<b>Intrastate</b>	Connecting within a state.
<b>Intruder</b>	Unauthorized person, animal, or object in a restricted area.
<b>Intrusion</b>	Attacks or attempted attacks from outside the security perimeter of an asset.
<b>Intrusion alarm</b>	Alarm generated by an IDS. Alarms include Intrusion, Nuisance, Environmental, and False.
<b>Intrusion detection</b>	Methods and technologies to sense and annunciate the intrusion of personnel into a defined area.
<b>Intrusion detection Sensor</b>	A device that initiates alarm signals by sensing the stimulus, change, or condition for which it was designed.
<b>Intrusion detection system (IDS)</b>	The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.



<b>Investigation</b>	The process used to determine the causal and contributing factors of an accident or hazard, so that actions can be identified to prevent recurrence.
<b>Investment cost</b>	First cost and later expenditures which have substantial and enduring value (generally more than one year) for upgrading, expanding, or changing the functional use of a building or building system.
<b>Iodine</b>	A nonmetallic solid element. There are both radioactive and non-radioactive isotopes of iodine. Radioactive isotopes of iodine are widely used in medical applications. Radioactive iodine is a fission product and is the largest contributor to people's radiation dose after an accident at a nuclear reactor.
<b>Ion</b>	An atom that has fewer or more electrons than it has protons causing it to have an electrical charge and, therefore, be chemically reactive.
<b>Ionization</b>	The process of adding one or more electrons to, or removing one or more electrons from, atoms or molecules, thereby creating ions. High temperatures, electrical discharges, or nuclear radiation can cause ionization.
<b>Ionizing radiation</b>	Any radiation capable of displacing electrons from atoms, thereby producing ions. High doses of ionizing radiation may produce severe skin or tissue damage. See also alpha particle, beta particle, gamma ray, neutron, x-ray.
<b>Iris</b>	A mechanical diaphragm which can be controlled manually or automatically to adjust the lens aperture.
<b>Irradiation</b>	Exposure to radiation.
<b>Isolated fenced perimeters</b>	Fenced perimeters with 100 feet or more of space outside the fence that is clear of obstruction, making approach obvious.
<b>Isotope</b>	A nuclide of an element having the same number of protons but a different number of neutrons.
<b>Jail</b>	A local government's detention center where persons awaiting trial or those convicted of misdemeanors are confined.
<b>Jersey barrier</b>	A protective concrete barrier initially and still used as a highway divider that now also functions as an expedient method for traffic speed control at entrance gates and to keep vehicles away from buildings.
<b>Joint Information Center (JIC)</b>	A central point of contact for all news media near the scene of a large-scale disaster. News media representatives are kept informed of activities and events by Public Information Officers who represent all participating federal, state, and local agencies that are collocated at the JIC.
<b>Joint Information System (JIS) <sup>1</sup></b>	Under the FRP, connection of public affairs personnel, decision-makers, and news centers by electronic mail, fax, and telephone when a single federal-state-local JIC is not a viable option.
<b>Joint Information System (JIS) <sup>2</sup></b>	Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.
<b>Joint Interagency Intelligence Support Element (JIISE)</b>	An interagency intelligence component designed to fuse intelligence information from the various agencies participating in a response to a WMD threat or incident within an FBI JOC. The JIISE is an expanded version of the investigative/intelligence component that is part of the standardized FBI command post structure. The JIISE manages five functions, including: security, collections management, current intelligence, exploitation, and dissemination.
<b>Joint Operations Center (JOC)</b>	Established by the LFA under the operational control of the federal OSC, as the focal point for management and direction of on-site activities, coordination/

	establishment of state requirements/priorities, and coordination of the overall federal response.
<b>Jurisdiction</b>	A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographic (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health).
<b>Jurisdictional Agency</b>	The agency having jurisdiction and responsibility for a specific geographical area, or a mandated function.
<b>K9 Supervisor</b>	Law enforcement officer or management personnel responsible for oversight of the K9 unit and deployment of resources within the unit.
<b>K9 team</b>	The handler and the assigned service dog.
<b>K9 unit</b>	A specialized unit within a law enforcement agency or other organization that is responsible for administration of the program that deploys service dogs.
<b>Key asset</b>	An organization, group of organizations, system, or group of systems, the loss of which would have widespread and dire strategic, economic or social impact.
<b>Key resources</b>	Publicly or privately controlled resources essential to the minimal operations of the economy and government.
<b>Kiloton (Kt)</b>	The energy of an explosion that is equivalent to an explosion of 1,000 tons of TNT. One kiloton equals 1 trillion (10 <sup>12</sup> ) calories.
<b>Knot</b>	The unit of speed equivalent to one nautical mile, or 6,080.20 feet per hour.
<b>Laminated glass</b>	Multiple sheets of glass bonded together by a bonding interlayer.
<b>Landscaping</b>	The use of plantings (shrubs and trees), with or without landforms and/or large boulders, to act as a perimeter barrier against defined threats.
<b>Large object size</b>	The ability to detect guns and large knives concealed on an individual that are constructed of either ferromagnetic or nonferromagnetic metal. Large knives are defined for this purpose as knives with blade lengths exceeding 7.5 cm.
<b>Large object size test objects</b>	Test objects used to test the large object size detection performance of walk-through metal detectors used as weapon detectors.
<b>Laser card</b>	A card technology that uses a laser reflected off of a card for uniquely identifying the card.
<b>Latent period</b>	The time between exposure to a toxic material and the appearance of a resultant health effect.
<b>Law enforcement incident command system (LEICS)</b>	The Incident Command System modified to reflect specific operating requirements of law enforcement.
<b>Layers of protection</b>	A traditional approach in security engineering using concentric circles extending out from an area to be protected as demarcation points for different security strategies.
<b>Lead agency</b>	The federal department or agency assigned lead responsibility under U.S. law to manage and coordinate the federal response in a specific functional area.
<b>Lead federal agency (LFA)</b>	Leads and coordinates the emergency response activities of other federal agencies during a nuclear emergency. After a nuclear emergency, the Federal Radiological Emergency Response Plan (FRERP, available at <a href="http://www.fas.org/nuke/guide/usa/doctrine/national/frerp.htm">http://www.fas.org/nuke/guide/usa/doctrine/national/frerp.htm</a> ) will determine which federal agency will be the LFA.
<b>Lens format</b>	The approximate size of a lens projected image. In most cases the lens will project a image slightly greater than the designated image size to ensure the pickup device is completely covered. It is recommended that camera and lenses are the same format size. A lens with a larger format size can be used on a smaller format camera, however a smaller format lens should never be used with a larger format camera.

<b>Letter of Expectation</b>	See Delegation of Authority.
<b>Level A</b>	A military level of packing that provides protection required to meet the most severe worldwide shipment, handling, and storage conditions.
<b>Level B</b>	A military level of packing that provides protection required to meet moderate worldwide shipment, handling, and storage conditions.
<b>Level of protection <sup>1</sup></b>	The degree to which an asset (person, equipment, object, etc.) is protected against injury or damage from an attack.
<b>Level of protection <sup>2</sup></b>	The degree to which an asset is protected against injury or damage from a CBR event.
<b>Liaison</b>	An agency official sent to another agency to facilitate interagency communications and coordination.
<b>Liaison officer</b>	A member of the Command Staff responsible for coordinating with representatives from cooperating and assisting agencies or organizations.
<b>Life-cycle cost (LCC)</b>	A technique of economic evaluation that sums over a given study period the costs of initial investment (less resale value), replacements, operation (including energy use) and maintenance of an investment decision.
<b>Limited area</b>	A restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access to the item. See controlled area and exclusion area.
<b>Line of sight (LOS)</b>	Direct observation between two points with the naked eye or hand-held optics.
<b>Line supervision</b>	A data integrity strategy that monitors the communications link for connectivity and tampering.
<b>Linear service</b>	Ferry service with multiple stops (e.g., along a waterfront).
<b>Line-of-sight sensor</b>	A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.
<b>Local emergency operations plan</b>	<p>Plan developed by designated local emergency planning agencies to comply with State and/or local requirements. EOPs typically follow the general format specified by the Federal Emergency Management Agency (FEMA) in the Federal Response Plan, and often include a Basic Plan and supporting Annexes.</p> <p>Local Emergency Planning Agencies include those agencies of local government with authority to plan for, and manage the consequences of, a major emergency within their jurisdictional boundaries. The agencies vary by community and often include local Emergency Management Agencies (EMAs); Local Emergency Planning Committees (LEPCs); municipal Offices of Emergency Management (OEMs) and local Departments of Public Safety (DPS).</p>
<b>Local government</b>	Any county, city, village, town, district, or political subdivision of any state, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, including any rural community or unincorporated town or village or any other public entity.
<b>Local radiation injury (LRI)</b>	Acute radiation exposure (more than 1,000 rads) to a small, localized part of the body. Most local radiation injuries do not cause death.
<b>Lockdown/shelter in place</b>	Terms that refer to securing a facility or vehicle from people entering or exiting the area to protect those in the lockdown or shelter in place from a threat outside of the secured area.
<b>Logistics</b>	Providing resources and other services to support incident management.
<b>Logistics section</b>	The Section responsible for providing facilities, services, and material support for the incident.
<b>Low-level waste (LLW)</b>	Radioactively contaminated industrial or research waste such as paper, rags, plastic bags, medical waste, and water-treatment residues. It is waste that does not meet the criteria for any of three other categories of radioactive waste: spent

	nuclear fuel and high-level radioactive waste; transuranic radioactive waste; or uranium mill tailings.
<b>Luminance contrast</b>	Refers to the relationship or difference between the object and its immediate background, defined by the ratio: $L_1/L_2$ Where: $L_1$ = luminance of background.
<b>Luminance contrast</b>	The amount of light reflected from an area or surface or the amount of light emitted from a surface, e.g., electroluminescent or LED material. English units are foot-lamberts (fl). International (SI) units are candela per square meter ( $cd/m^2$ ) and milli-candela per square meter ( $mcd/m^2$ ). (1 fl = $3.426 cd/m^2$ or $3426 mcd/m^2$ .)
<b>Luminescence</b>	The emission of light other than incandescent, as in phosphorescence or fluorescence by processes that derive energy from essentially non-thermal sources through excitation by radiation.
<b>Magnetic lock</b>	An electromagnetic lock that unlocks a door when power is removed.
<b>Magnetic stripe</b>	A card technology that uses a magnetic stripe on the card to encode data used for unique identification of the card.
<b>Mail-bomb delivery</b>	Bombs or incendiary devices delivered to the target in letters or packages.
<b>Major Disaster</b>	As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.
<b>Major event</b>	Refers to domestic terrorist attacks, major disasters, and other emergencies. (HSPD-8)
<b>Manageable span of control</b>	Because the responsibility of each individual supervisor is limited, the span of control typically ranges from three to seven persons, depending on the type of incident, the nature of the response, and the distance involved.
<b>Management by objective</b>	A management approach that involves a five-step process for achieving the incident goal. The Management by Objectives approach includes the following: establishing overarching incidents objectives; developing strategies based on overarching incidents objectives; developing and issuing assignments, plans, procedures, and protocols; establishing specific, measurable tactics or tasks for various incident management, functional activities, and directing efforts to attain them, in support of defined strategies; and documenting results to measure performance and facilitate corrective action.
<b>Managers</b>	Individuals within ICS organizational Units that are assigned specific managerial responsibilities (e.g., Staging Area Manager or Camp Manager).
<b>Man-trap</b>	An access control strategy that uses a pair of interlocking doors to prevent tailgating. Only one door can be unlocked at a time.
<b>Marine transportation system</b>	A national network of waterway systems, ports, and their intermodal landside connections that allows the various modes of transportation (i.e., vessels, vehicles, and other system users) to move people and goods on the water. This system includes extensive regional and local passenger ferry systems.
<b>Maritime security directive</b>	An instruction issued by the commandant or his/her delegate mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.
<b>Maritime security levels</b>	The levels reflecting the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to water subject to the jurisdiction of the United States.

<b>Maritime Transportation Security</b>	Legislation passed as public law 107-295 on November 25, 2002, that implements, mandates, and regulates the security for maritime transportation vessels, assets, and facilities.
<b>Marking</b>	A visible notice, sign, symbol, line or trace.
<b>MARSEC Level 1</b>	The level for which minimum appropriate protective security measures shall be maintained at all times.
<b>MARSEC Level 2</b>	The level for which moderate protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.
<b>MARSEC Level 3</b>	The level for which maximum protective security measures shall be maintained for a limited period of time as a result of heightened risk of a transportation security incident.
<b>Mass notification</b>	Capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations.
<b>Master</b>	The holder of a license that authorizes the individual to serve as a master, operator, or person in charge of the rated vessel.
<b>Materiality</b>	Materiality is a function of consequence and likelihood. Strategic risks have a very high materiality (i.e., very significant consequence and high likelihood), whereas traditional risks have low materiality (i.e., low consequence and/or low likelihood).
<b>Mean</b>	A measure of central tendency, usually referred to as the average.
<b>Measure of central tendency</b>	A number that represents the average of a group of data.
<b>Measurement coordinate system</b>	A mutually orthogonal three-dimensional Cartesian coordinate system referenced to the detector axis and the detector plane. The three axes are labeled “x,” “y,” and “z,” where the y axis is parallel to the detector axis and the x and z axes are in the detector plane. The orientation of the test objects and direction of the magnetic field is referenced to the measurement coordinate system.
<b>Median</b>	A measure of central tendency that represents the middle number of a group of data that is arranged from smallest to largest.
<b>Medical transitional structures and spaces</b>	Structures that are erected or leased for temporary occupancy to maintain mission-critical medical care during construction, renovation, modification, repair or restoration of an existing medical structure. Examples include urgent, ambulatory, and acute care operations.
<b>Medium object size</b>	The ability to detect small weapons and contraband items concealed on an individual that are constructed of either ferromagnetic or nonferromagnetic metal. Small weapons and contraband items are defined as any item that can be used to injure another person or to defeat security devices. Objects in this category include razor blades, hacksaw blades, handcuff keys, etc.
<b>Medium object size test objects</b>	Test objects used to test the medium object size detection performance of walk-through metal detectors used as weapon detectors.
<b>Mega-node</b>	The single point at which multiple modes intersect. In transportation systems, a mega node is a place of potential failure or bottleneck, with the potential for wide-ranging disruptions and losses.
<b>Megaton (Mt)</b>	The energy of an explosion that is equivalent to an explosion of 1 million tons of TNT. One megaton is equal to a quintillion (10 <sup>18</sup> ) calories. See also kiloton.
<b>Memoranda of understanding (MOU)</b>	Written or oral mutual-aid agreements that serve as the basis of mutual acknowledgement of the resources that each organization will provide during response and recovery efforts.
<b>Methodology</b>	An open system of procedures.
<b>Metrics</b>	Measurable standards that are useful in describing a resource’s capability.

<b>Metropolitan medical strike teams (MMSTs)</b>	Teams that are being developed to manage the immediate medical consequences of CBN terrorist events.
<b>Metropolitan routes</b>	Routes located in and serving areas designated as metropolitan. These routes are used to transport individuals from one point in a metropolitan area to another.
<b>Microwave motion sensor</b>	An intrusion detection sensor that uses microwave energy to sense movement within the sensor's field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.
<b>Microwave sensor</b>	An IDS sensor that uses the disturbance of microwave energy to annunciate an intrusion.
<b>Military installations</b>	Army, Navy, Air Force, and Marine Corps bases, posts, stations, and annexes (both contractor and government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.
<b>Military protective construction</b>	Military facilities designed to resist military conventional and nuclear weapons to the NATO (or equivalent) standards of hardened, protected, semi-hardened, collaterally protected, or splinter protected.
<b>Minimum essential infrastructure resource elements</b>	The broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency, or organization to conduct its core mission(s).
<b>Minimum measures</b>	Protective measures that can be applied to all buildings regardless of the identified threat. These measures offer defense or detection opportunities for minimal cost, facilitate future upgrades, and may deter acts of aggression.
<b>Minimum object distance (M.O.D.)</b>	The closest distance a given lens will be able to focus upon a object. Generally the smaller the focal length the shorter the M.O.D. This distance can be altered with use of extension tubes.
<b>Misdemeanor</b>	A crime that is less serious than a felony and is usually punishable by fine, penalty, forfeiture, or confinement (usually for a brief term) in a place other than prison (such as a county jail).
<b>Mitigation<sup>1</sup></b>	Sustained action that reduces or eliminates long-term risk to people and property and limits the effects of criminal and terrorist activity.
<b>Mitigation<sup>2</sup></b>	The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.
<b>Mitigation<sup>3</sup></b>	Provides a critical foundation in the effort to reduce the loss of life and property from natural and/or manmade disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect.
<b>Mitigation Strategies</b>	Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.
<b>Mitigation Strategy</b>	One of the four core components of the cost-accounting framework (bearer of costs; budget category; building/facility component; <i>mitigation strategy</i> ). Means of classifying/allocating costs within the CET software in regards to risk management. The three <i>mitigation strategy</i> classifications include engineering alternatives; management practices; financial mechanisms.

<b>Mobilization</b>	The process and procedures used by all organizations—Federal, State, tribal, and local—for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.
<b>Mobilization guide</b>	Reference document used by organizations outlining agreements, processes, and procedures used by all participating agencies/organizations for activating, assembling, and transporting resources.
<b>Mode</b> <sup>1</sup>	A specific form or variety of something. In the context of transportation, there are six modes: aviation, maritime, mass transit, highway, freight rail, and pipeline.
<b>Mode</b> <sup>2</sup>	A measure of central tendency that represents the number most frequently encountered within a group of numbers.
<b>Mode of service</b>	A system for carrying transit passengers described by specific right-of-way, technology and operational features. Typically includes the following: (1) Aerial Tramway: An electric system of aerial cables with suspended powerless passenger vehicles. The vehicles are propelled by separate cables attached to the vehicle suspension system and powered by engines or motors at a central location not on board the vehicle. (2) Automated Guideway: An electric railway (single or multi-car trains) comprised of guided transit vehicles that operate without transit personnel on-board. Service may be on a fixed schedule or in response to a passenger activated call button. Automated guideway transit includes personal rapid transit, group rapid transit and people mover systems. (3) Bus: A transit mode comprised of rubber tired passenger vehicles operating on fixed routes and schedules over roadways. Vehicles are powered by diesel, gasoline, battery, or alternative fuel engines contained within the vehicle. (4) Bus Rapid Transit: A type of bus service that operates on exclusive transitways, HOV lanes, expressways, or ordinary streets.
<b>Molecule</b>	A combination of two or more atoms that are chemically bonded. A molecule is the smallest unit of a compound that can exist by itself and retain all of its chemical properties.
<b>Monohull</b>	A vessel with a single hull.
<b>Monostatic sensor</b>	An IDS sensor that consists of one part, with transmitter and receiver mounted in the same physical device.
<b>Monte Carlo simulation</b>	A technique used to evaluate models that are too complicated for an analytical solution. It involves the use of numerous trials to find the equilibrium of a system.
<b>Mooring line</b>	A cable or line to tie up a ship.
<b>Motion detector</b>	An intrusion detection sensor that changes state based on movement in the sensor's field of view.
<b>Moving vehicle bomb</b>	An explosive-laden car or truck driven into or near a building and detonated.
<b>Multiagency Coordination (MAC) Group</b>	Typically, administrators/executives, or their appointed representatives, who are authorized to commit agency resources and funds, are brought together and form MAC Groups. MAC Groups may also be known as multiagency committees, emergency management committees, or as otherwise defined by the System.
<b>Multiagency coordination entity</b>	A multiagency coordination entity functions within a broader multiagency coordination system. It may establish the priorities among incidents and associated resource allocations, deconflict agency policies, and provide strategic guidance and direction to support incident management activities.
<b>Multiagency Coordination System(s) (MACS)</b>	Multiagency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The elements of multiagency coordination systems include facilities, equipment, personnel, proce-

dures, and communications. Two of the most commonly used elements are EOCs and MAC Groups. These systems assist agencies and organizations responding to an incident.

<b>Multijurisdictional Incident</b>	An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command.
<b>Mutual Aid Agreements and/or Assistance Agreements:</b>	Written or oral agreements between and among agencies/organizations and/or jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.
<b>NAR Nuisance alarm rate</b>	A rate or ratio of nuisance alarms compared to other alarm types.
<b>National</b>	Of a nationwide character, including the Federal, State, local and tribal aspects of governance and polity.
<b>National Disaster Medical System</b>	A cooperative, asset-sharing partnership between the Department of Health and Human Services, the Department of Veterans Affairs, the Department of Homeland Security, and the Department of Defense. NDMS provides resources for meeting the continuity of care and mental health services requirements of the Emergency Support Function 8 in the Federal Response Plan.
<b>National Incident Management System (NIMS)</b>	Provides a systematic, proactive approach guiding government agencies at all levels, the private sector, and nongovernmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.
<b>National response framework</b>	A guide to how the nation conducts all-hazards incident management.
<b>National response plan</b>	A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.
<b>Natural</b>	A term which refers to deriving access control and surveillance as a by-product of the normal and routine use of the environment.
<b>Natural disaster</b>	A physical capability with the ability to destroy or incapacitate critical infrastructures. Natural disasters differ from threats due to the absence of intent.
<b>Natural filtration</b>	Filtering that occurs when an agent is deposited in the building shell or on interior surfaces as air passes into and out of the building; generally, the tighter the building, the greater the effect of natural filtration.
<b>Natural hazard</b>	Naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, Understanding Your Risks). The risks of natural hazards may be increased or decreased as a result of human activity; however, they are not inherently human-induced.
<b>Natural protective barriers</b>	Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.
<b>Natural ventilation</b>	The exchange of the building's internal air with outside air by means of intentional openings in the building envelope such as open doors and windows.
<b>Naval vessel protection zone</b>	A 500-yard regulated area of water surrounding large U.S. naval vessels that is necessary to provide for the safety or security of these U.S. naval vessels.
<b>Network</b>	A group of assets or systems that share information or interact with each other in order to provide infrastructure services within or across sectors.



<b>Neutron</b>	A small atomic particle possessing no electrical charge typically found within an atom's nucleus. Neutrons are, as the name implies, neutral in their charge. That is, they have neither a positive nor a negative charge. A neutron has about the same mass as a proton. See also alpha particle, beta particle, gamma ray, x-ray.
<b>New Starts Project</b>	Any rail fixed guideway system funded under FTA's 49 U.S.C. 5309 discretionary construction program.
<b>Node</b>	A network intersection or junction (e.g., a subway station).
<b>Nolo Contendere</b>	The name of a plea in a criminal action, having the same legal effect as a plea of guilty, so far as regards all proceedings on the indictment, and on which the defendant may be sentenced. (Latin for "I will not contest it.")
<b>Non-exclusive zone</b>	An area around an asset that has controlled entry, but shared or less restrictive access than an exclusive zone.
<b>Nongovernmental organization (NGO)</b>	An entity with an association that is based on interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.
<b>Non-ionizing radiation</b>	Radiation that has lower energy levels and longer wavelengths than ionizing radiation. It is not strong enough to affect the structure of atoms it contacts but is strong enough to heat tissue and can cause harmful biological effects. Examples include radio waves, microwaves, visible light, and infrared from a heat lamp.
<b>Non-persistent agent</b>	An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.
<b>Non-stochastic effects</b>	Effects that can be related directly to the radiation dose received. The effect is more severe with a higher dose. It typically has a threshold, below which the effect will not occur. These are sometimes called deterministic effects. For example, a skin burn from radiation is a non-stochastic effect that worsens as the radiation dose increases.
<b>Normal User</b>	Persons whom you desire to be in a certain space.
<b>Notification</b>	The formal advising, by voice or in writing, of specific information about an incident by the process described in the emergency response procedure governing the incident.
<b>Nuclear detonation</b>	An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.
<b>Nuclear energy</b>	The heat energy produced by the process of nuclear fission within a nuclear reactor or by radioactive decay.
<b>Nuclear fuel cycle</b>	The steps involved in supplying fuel for nuclear power plants. It can include mining, milling, isotopic enrichment, fabrication of fuel elements, use in reactors, chemical reprocessing to recover the fissile material remaining in the spent fuel, reenrichment of the fuel material refabrication into new fuel elements, and waste disposal.
<b>Nuclear, biological, or chemical weapons</b>	Also called Weapons of Mass Destruction (WMD).
<b>Nucleus</b>	The central part of an atom that contains protons and neutrons. The nucleus is the heaviest part of the atom.
<b>Nuisance alarm</b>	Alarm annunciation from the detection of an intruder that is NOT an intrusion. Example is an authorized worker who enters a protected area with proper suppression of the IDS alarm.
<b>Object size classes</b>	A classification method based on the ability to detect metal objects of a minimum size. A detector may meet the requirements for one or both object size classes.

<b>Officers</b>	The ICS title for the personnel responsible for the Command Staff positions of Safety, Liaison, and Public Information.
<b>On scene coordinator</b>	The person at the scene of an emergency who is responsible for coordinating all disaster recovery activities and vehicle movements at the scene.
<b>On-scene coordinator (OSC)</b>	The federal official pre-designated by the EPA and U.S. Coast Guard to coordinate and direct response and removals under the National Oil and Hazardous Substances Pollution Contingency Plan.
<b>Open systems architecture</b>	A term borrowed from the IT industry to claim that systems are capable of interfacing with other systems from any vendor, which also uses open system architecture. The opposite would be a proprietary system.
<b>Operating cost</b>	The expenses incurred during the normal operation of a building or a building system or component, including labor, materials, utilities, and other related costs.
<b>Operational period</b>	The time scheduled for executing a given set of operation actions, as specified in the Incident Action Plan. Operational periods can be of various lengths, although usually they last 12–24 hours.
<b>Operations (OPS)</b>	Begins with the initiation of the completed project in service and concludes with the determination that the project has fulfilled its service requirements and must be replaced or removed from operations.
<b>Operations control center (OCC)</b>	A central or designated regional location of a railroad with responsibilities for directing the safe movement of trains.
<b>Operations section</b>	One of the five primary functions found in the ICS and at all emergency management levels. The Section is responsible for all tactical operations at the incident, or for the coordination of operational activities at an EOC. The Operations Section at field response level may include branches, divisions, and/or groups, task forces, teams, and single resources.
<b>Operations security</b>	The co-mingling of computer, technical counterintelligence security measures developed and implemented to augment traditional security programs (physical security, information or personnel security and communications security) as a means of eliminating or minimizing vulnerabilities that impact on technical programs.
<b>Operations support vehicles</b>	Vehicles such as airfield support equipment whose purpose is direct support to operations and which are operated only within a restricted access area.
<b>Operator interface</b>	The part of a security management system that provides that user interface to humans.
<b>Organic security</b>	Security that is part of the organization itself rather than contracted services.
<b>Organization</b>	Any association or group of persons with like objectives. Examples include, but are not limited to, governmental departments and agencies, private sector, and/or nongovernmental organizations.
<b>Organizational areas of control</b>	Controls consist of the policies, procedures, practices, and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
<b>Original equipment manufacturer (OEM)</b>	The enterprise that initially designs and builds a piece of equipment.
<b>Overpressure</b>	The difference in static pressure between the inside of a building and the ambient pressure outside of the building.
<b>Oversight agency</b>	The entity, other than the rail transit agency, designated by the state or several states to implement this part.
<b>Owner operator</b>	Any person or entity that owns or maintains operational control over any facility subject to 33 CFR Subchapter H.
<b>Parking</b>	Designated areas where vehicles may be left unattended.

<b>Participating agency</b>	Any fire, law enforcement, medical, governmental, or humanitarian agency that participates in any portion of a public transportation system's emergency response.
<b>Passenger</b>	A person who is on board, boarding, or alighting from a rail transit vehicle for the purpose of travel.
<b>Passenger operations</b>	The period of time when any aspect of rail transit agency operations are initiated with the intent to carry passengers.
<b>Passenger vessel</b>	On an international voyage, a vessel carrying more than 12 passengers, including at least one passenger-for-hire. On a domestic voyage, (1) a vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire; (2) a vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire; (3) a vessel that is chartered and carrying more than 12 passengers; (4) a submersible vessel that is carrying at least one passenger-for-hire; or (5) a wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.
<b>Passenger-only ferries</b>	Vessels having only passenger decks, though they may also have space for bicycles. They can range from small boats about 50 feet long holding about 50 people to the 310-foot-long Staten Island ferries in New York, which can accommodate 6,000 people. Because they do not have vehicle decks, they need not be square-ended and may be side-loading and have pointed bows. Catamaran (double hull) and hydrofoil (skimming the surface of the water) styles may be used for high-speed services.
<b>Passive infrared motion sensor</b>	A device that detects a change in the thermal energy pattern caused by a moving intruder and initiates an alarm when the change in energy satisfies the detector's alarm-criteria.
<b>Passive vehicle barrier</b>	A vehicle barrier that is permanently deployed and does not require response to be effective.
<b>Patch panel</b>	A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.
<b>Pathogens</b>	Living disease-producing agents of biological origin, including bacteria, viruses, and fungi.
<b>Pathways</b>	Pathways: the routes by which people are exposed to radiation or other contaminants. The three basic pathways are inhalation, ingestion, and direct external exposure. See also exposure pathway.
<b>Patrol Dog</b>	A service dog selected by the trainer and qualified by recognized standards to perform basic patrol functions.
<b>Penetrating radiation</b>	Radiation that can penetrate the skin and reach internal organs and tissues. Photons (gamma rays and x-rays), neutrons, and protons are penetrating radiations. However, alpha particles and all but extremely high-energy beta particles are not considered penetrating radiation.
<b>Perimeter barrier</b>	A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.
<b>Persistent agent</b>	An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.
<b>Personal responsibility</b>	All responders are expected to use good judgment and be accountable for their actions.
<b>Personnel accountability</b>	The ability to account for the location and welfare of incident personnel. It is accomplished when supervisors ensure that ICS principles and processes are

functional and that personnel are working within established incident management guidelines.

<b>Photon</b>	Discrete “packet” of pure electromagnetic energy. Photons have no mass and travel at the speed of light. The term “photon” was developed to describe energy when it acts like a particle (causing interactions at the molecular or atomic level), rather than a wave. Gamma rays and x-rays are photons.
<b>Physical security</b>	The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
<b>Piezoelectric</b>	An IDS sensor that uses the physical effect of voltage generation caused by the exertion of pressure on certain materials.
<b>Pilot house</b>	The enclosed space on the navigating bridge from which a ship is controlled when underway.
<b>Pinhole lens</b>	Lenses used primarily in covert applications where the camera/lens must remain out of sight.
<b>Pixel</b>	A pixel (short for picture element, using the common abbreviation “pix” for picture) is a single point in a graphic image.
<b>Plain language</b>	Communication that can be understood by the intended audience and meets the purpose of the communicator. For the purpose of NIMS, plain language is designed to eliminate or limit the use of codes and acronyms, as appropriate, during incident response involving more than a single agency.
<b>Planned Event</b>	A planned, nonemergency activity (e.g., sporting events, concerts, parades, etc.).
<b>Planning</b>	Begins with research conducted into the feasibility of a project and concludes with the creation of a concept and the decision to develop a preliminary design. This phase is managed through the local transportation planning function and proceeds through alternative analysis and special research, environmental impact assessments, corridor analyses, and major investment studies. It concludes with the formal adoption of a locally preferred alternative and the request to enter Preliminary Engineering.
<b>Planning meeting</b>	A meeting held as needed before and throughout the duration of an incident to select specific strategies and tactics.
<b>Planning section</b>	The section responsible for the collection, evaluation, and dissemination of operational information related to the incident, and for the preparation and documentation of the IAP. This Section also maintains information on the current and forecasted situation and on the status of resources assigned to the incident.
<b>Planning/intelligence</b>	This section is responsible for the collection, evaluation, and dissemination of information related to the incident or an emergency, and for the preparation and documentation of Incident Action Plans. This section also maintains information on the current and forecasted situation, and on the status of resources assigned to the incident. At the field response Level, the Section will include the Situation, Resource, Documentation, and Demobilization Units, as well as Technical Specialists.
<b>Planter barrier</b>	A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping capability of the individual planter.
<b>Plume<sup>1</sup></b>	Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.
<b>Plume<sup>2</sup></b>	The material spreading from a particular source and traveling through environmental media, such as air or ground water. For example, a plume could describe the dispersal of particles, gases, vapors, and aerosols in the atmosphere,

	or the movement of contamination through an aquifer (For example, dilution, mixing, or adsorption onto soil).
<b>Plutonium (Pu)</b>	A heavy, man-made, radioactive metallic element. The most important isotope is Pu-239, which has a half-life of 24,000 years. Pu-239 can be used in reactor fuel and is the primary isotope in weapons. One kilogram is equivalent to about 22 million kilowatt-hours of heat energy. The complete detonation of a kilogram of plutonium produces an explosion equal to about 20,000 tons of chemical explosive. All isotopes of plutonium are readily absorbed by the bones and can be lethal depending on the dose and exposure time.
<b>Point sensors</b>	A sensor that is used to monitor a single point such as door position (open or closed).
<b>Point-to-point ferry route segment/service</b>	Serving only two locations, in which case the route consists of a single nonstop ferry route segment.
<b>Polonium (Po)</b>	A radioactive chemical element and a product of radium (Ra) decay. Polonium is found in uranium (U) ores.
<b>Polycarbonate glazing</b>	A plastic glazing material with enhanced resistance to ballistics or blast effects.
<b>Population</b>	Everyone or everything defined to be within a class, category, or grouping of subjects or data.
<b>Portability</b>	Facilitates the interaction of systems that are normally distinct. Portability of radio technologies, protocols, and frequencies among emergency management/response personnel will allow for the successful and efficient integration, transport, and deployment of communications systems when necessary. Portability includes the standardized assignment of radio channels across jurisdictions, which allows responders to participate in an incident outside their jurisdiction and still use familiar equipment.
<b>Ported coaxial</b>	An IDS sensor that uses a leaky (purposely designed with poor shield cable) to detect intrusion. A RF signal is injected into the cable and interference of the field produced around the ported cable causes an IDS alarm.
<b>Practical field test</b>	A non-theoretical experiment designed to produce results which can be applied or used to make decisions.
<b>Pre-positioned resources</b>	Resources moved to an area near the expected incident site in response to anticipated resource needs.
<b>Prefilter</b>	A low- to medium-efficiency filter that precedes the HEPA filter to remove large particulates.
<b>Preliminary damage assessment (PDA)</b>	A mechanism used to determine the impact and magnitude of damage and the resulting unmet needs of individuals, businesses, the public sector, and the community as a whole. Information collected is used by the state as a basis for the Governor's request for a Presidential declaration, and by FEMA to document the recommendation made to the President in response to the Governor's request. PDAs are made by at least one state and one federal representative. A local government representative familiar with the extent and location of damage in the community often participates; other state and federal agencies and voluntary relief organizations also may be asked to participate, as needed.
<b>Prenatal radiation exposure</b>	Radiation exposure to an embryo or fetus while it is still in its mother's womb. At certain stages of the pregnancy, the fetus is particularly sensitive to radiation and the health consequences could be severe above 5 rads, especially to brain function.
<b>Preparedness <sup>1</sup></b>	Establishing the plans, training, exercises, and resources necessary to enhance mitigation of and achieve readiness for response to, and recovery from all hazards, disasters, and emergencies, including WMD incidents.
<b>Preparedness <sup>2</sup></b>	The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process.

Preparedness involves efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

<b>Preparedness</b> <sup>3</sup>	A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response.
<b>Preparedness organizations</b> <sup>1</sup>	Provides coordination for emergency management and incident response activities before a potential incident. These organizations range from groups of individuals to small committees to large standing organizations that represent a wide variety of committees, planning groups, and other organizations (e.g., Citizen Corps, Local Emergency Planning Committees (LEPCs), Critical Infrastructure Sector Coordinating Councils).
<b>Preparedness organizations</b> <sup>2</sup>	The groups and fora that provide interagency coordination for domestic incident management activities in a nonemergency context. Preparedness organizations can include all agencies with a role in incident management, for prevention, preparedness, response, or recovery activities. They represent a wide variety of committees, planning groups, and other organizations that meet and coordinate to ensure the proper level of planning, training, equipping, and other preparedness requirements within a jurisdiction or area.
<b>Pre-revenue (Interim) operations (PRE-REV)</b>	Begins with the identification and performance of tests, drills, exercises, and audits designed to verify the functional capability and readiness of the system as a whole, and concludes with verified documentation of readiness for revenue operations.
<b>Pressure mat</b>	A mat that generates an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.
<b>Pressure sensor</b>	An IDS sensor that detects pressure (usually intruding personnel) and alarms when activated.
<b>Pre-testing</b>	Administering a measurement instrument to a small group of subjects, prior to administering it to the entire group.
<b>Prevention</b> <sup>1</sup>	Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.
<b>Prevention</b> <sup>2</sup>	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.
<b>Primary asset</b>	An asset that is the ultimate target for compromise by an aggressor.
<b>Prison</b>	A state or federal facility of confinement for convicted criminals, especially felons.
<b>Private sector</b>	Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit organizations, formal and informal structures, commerce and industry, and private voluntary organizations (PVO).

<b>Private security</b>	An independent or proprietary commercial organization whose activities include safeguarding the employing party's assets, ranging from human lives to physical property (the premises and contents), responding to emergency incidents, performing employee background investigations, performing the functions of detection and investigation of crime and criminals, and apprehending offenders for consideration.
<b>Private security officer</b>	An individual, other than armored car personnel or a public employee (federal, state, or local government), employed part or full time, in uniform or plain clothes, hired to protect the employing party's assets, ranging from human lives to physical property (the premises and contents). The definition excludes individuals who are not employed in the capacity of a private security officer.
<b>Privately owned and privately operated</b>	When the title and operation of the boat and the terminal are vested by a private entity.
<b>Probability of detection (POD)</b>	A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.
<b>Probability of intercept</b>	The probability that an act of aggression will be detected and that a response force will intercept the aggressor before the asset can be compromised.
<b>Processes</b>	Systems of operations that incorporate standardized procedures, methodologies, and functions necessary to provide resources effectively and efficiently. These include resource typing, resource ordering and tracking, and coordination.
<b>Program standard</b>	A written document developed and adopted by the oversight agency that describes the policies, objectives, responsibilities, and procedures used to provide rail transit agency safety and security oversight.
<b>Progressive exercise program</b>	<p>Comprised of five categories of activities for testing and evaluating the capabilities of transportation personnel to manage emergency situations using existing plans, procedures and equipment. The categories in a progressive exercise program build on each other, in both complexity and level of assessment provided for transportation management. They include:</p> <ol style="list-style-type: none"> <li>(1) An orientation seminar is an informal discussion designed to familiarize participants with roles, plans, procedures, and resolve questions of coordination and assignment of responsibilities.</li> <li>(2) A tabletop exercise simulates an emergency situation in an informal, stress-free environment. It is designed to elicit discussion as participants examine and resolve problems based on existing crisis management plans.</li> <li>(3) A drill is a set of supervised activities that test, develop, or maintain skills in a single response procedure (e.g., communications, notification, lockdown, and fire) and the possible or probable interaction with local government agency functions (e.g., incident command posts, rescue squad entry, and police perimeter control).</li> </ol>
<b>Progressive collapse</b>	The spread of an initial local failure from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it.
<b>Proprietary security</b>	Any organization, or department of that organization, that provides full time security officers solely for itself.
<b>Protected area of a building</b>	The CP area, where personnel are able to work or shelter without wearing IPE during release of a CBR agent.
<b>Protected construction</b>	Buried or partially buried construction that provides protection against direct hits by large general purpose military bombs.
<b>Protective action guide (PAG)</b>	A guide that tells state and local authorities at what projected dose they should take action to protect people from exposure to unplanned releases of radioactive material into the environment.
<b>Protective action plan</b>	Security measures and operational procedures to protect existing buildings and their occupants from airborne hazards by reducing vulnerability, preventing a release, reducing the likelihood that releases will affect building occupants, and mitigating the hazard once a release has occurred.

<b>Protective barriers</b>	Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.
<b>Protective measures</b>	Elements of a protective system that protect an asset against a threat. Protective measures are divided into defensive and detection measures.
<b>Protective system</b>	An integration of all of the protective measures required to protect an asset against the range of threats applicable to the asset.
<b>Protocol</b>	The research design or specific steps involved in conducting a research project.
<b>Protocols</b>	Sets of established guidelines for actions (which may be designated by individuals, teams, functions, or capabilities) under various specified conditions.
<b>PTZ or P/T/Z pan tilt zoom</b>	Control of camera systems - pan is side to side motion, tilt is up and down, and zoom is FOV adjustment via camera lens control.
<b>Public access facility</b>	A facility that (1) is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104; (2) has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and (3) receives only (i) vessels not subject to part 104 of this chapter, or (ii) passenger vessels, except (A) ferries certified to carry vehicles; (B) cruise ships; or (C) passenger vessels subject to SOLAS Chapter XI.
<b>Public information</b>	Processes, procedures, and systems for communicating timely, accurate, accessible information on the incident's cause, size, and current situation; resources committed; and other matters of general interest to the public, responders, and additional stakeholders (both directly affected and indirectly affected).
<b>Public information officer</b>	A member of the Command Staff responsible for interfacing with the public and media or with other agencies with incident-related information requirements.
<b>Public safety</b>	Support mechanisms that sustain the life and vitality of a community's health, safety, and social stability by performing such services as law enforcement, fire prevention, personal and facility security, disaster preparedness, and emergency medical assistance. In some instances, public safety may refer to law enforcement officers, firefighters, rescue squads, and ambulance crews. In other instances, public safety properly encompasses private security officers, as well.
<b>Public transportation</b>	Transportation by bus, or rail, or other conveyance, either publicly or privately owned, providing to the public general or special service (but not including school buses or charter or sightseeing service) on a regular and continuing basis. Also referred to as mass transit, public transit, and transit.
<b>Public transportation infrastructure</b>	All vehicles, equipment, right-of-way, routes, support equipment and facilities, and buildings and real estate belonging to or operated by the public transportation authority.
<b>Public transportation operations control center</b>	A public transportation system's central control and communications facility for dispatching operations. Separate control centers are typically used for different modes (i.e., bus, rail and paratransit/demand-response operations). A few transit systems have co-located modal dispatching functions within a single control center.
<b>Public transportation system</b>	A public entity responsible for administering and managing transit activities and services. Public transportation systems can directly operate transit service or contract out for all or part of the total service provided. Also known as "transit systems" and "public transit systems."
<b>Publications management</b>	The publications management subsystem includes materials development, publication control, publication supply, and distribution. The development and distribution of NIMS materials is managed through this subsystem. Consistent documentation is critical to success, because it ensures that all responders are familiar with the documentation used in a particular incident regardless of the location or the responding agencies involved.



<b>Publicly owned and privately operated</b>	When the title for the boat or terminal is vested in a federal, state, county, town, township, Indian tribe, municipal or other local government and a private entity operates the boat or terminal.
<b>Qualification and certification</b>	This subsystem provides recommended qualification and certification standards for emergency responder and incident management personnel. It also allows the development of minimum standards for resources expected to have an interstate application. Standards typically include training, currency, experience, and physical and medical fitness.
<b>Quality factor (Q)</b>	The factor by which the absorbed dose (rad or gray) is multiplied to obtain a quantity that expresses, on a common scale for all ionizing radiation, the biological damage (rem) to an exposed person. It is used because some types of radiation, such as alpha particles, are more biologically damaging internally than other types.
<b>Quasi-terrorism</b>	Activities incidental to the commission of crimes of violence that are similar in form and method to terrorism, but lack an organized social, political, religious, or economic dimension.
<b>Rad (radiation absorbed dose)</b>	a basic unit of absorbed radiation dose. It is a measure of the amount of energy absorbed by the body. The rad is the traditional unit of absorbed dose. It is being replaced by the unit gray (Gy), which is equivalent to 100 rad. One rad equals the dose delivered to an object of 100 ergs of energy per gram of material.
<b>Radiation<sup>1</sup></b>	High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Particles can be either charged alpha or beta particles or neutral neutron or gamma rays.
<b>Radiation<sup>2</sup></b>	Energy moving in the form of particles or waves. Familiar radiations are heat, light, radio waves, and microwaves. Ionizing radiation is a very high-energy form of electromagnetic radiation.
<b>Radiation sickness</b>	See also acute radiation syndrome (ARS), or the CDC fact sheet “Acute Radiation Syndrome,” at <a href="http://www.bt.cdc.gov/radiation/ars.asp">http://www.bt.cdc.gov/radiation/ars.asp</a> .
<b>Radiation warning symbol</b>	A symbol prescribed by the Code of Federal Regulations. It is a magenta or black trefoil on a yellow background. It must be displayed where certain quantities of radioactive materials are present or where certain doses of radiation could be received.
<b>Radioactive contamination</b>	The deposition of unwanted radioactive material on the surfaces of structures, areas, objects, or people. It can be airborne, external, or internal. See also contamination, decontamination.
<b>Radioactive half-life</b>	The time required for a quantity of a radioisotope to decay by half. For example, because the half-life of iodine-131 (I-131) is 8 days, a sample of I-131 that has 10 mCi of activity on January 1, will have 5 mCi of activity 8 days later, on January 9. See also effective half-life.
<b>Radioactive material</b>	Material that contains unstable (radioactive) atoms that give off radiation as they decay.
<b>Radioactivity</b>	The process of spontaneous transformation of the nucleus, generally with the emission of alpha or beta particles often accompanied by gamma rays. This process is referred to as decay or disintegration of an atom.
<b>Radioassay</b>	A test to determine the amounts of radioactive materials through the detection of ionizing radiation. Radioassays will detect transuranic nuclides, uranium, fission and activation products, naturally occurring radioactive material, and medical isotopes.
<b>Radiogenic</b>	Radiogenic: health effects caused by exposure to ionizing radiation.
<b>Radiography</b>	1) Medical: the use of radiant energy (such as x-rays and gamma rays) to image body systems. 2) Industrial: the use of radioactive sources to photograph internal structures, such as turbine blades in jet engines. A sealed radiation source, usually iridium-192 (Ir-192) or cobalt-60 (Co-60), beams gamma rays at the object

to be checked. Gamma rays passing through flaws in the metal or incomplete welds strike special photographic film (radiographic film) on the opposite side.

**Radioisotope  
(radioactive isotope)**

Isotopes of an element that have an unstable nucleus. Radioactive isotopes are commonly used in science, industry, and medicine. The nucleus eventually reaches a stable number of protons and neutrons through one or more radioactive decays. Approximately 3,700 natural and artificial radioisotopes have been identified.

**Radiological dispersal  
device (RDD)**

A device that disperses radioactive material by conventional explosive or other mechanical means, such as a spray. See also dirty bomb.

**Radiological monitoring**

The process of locating and measuring radiation by means of survey instruments that can detect and measure (as exposure rates) ionizing radiation.

**Radiological or  
radiologic**

Related to radioactive materials or radiation. The radiological sciences focus on the measurement and effects of radiation.

**Radium (Ra)**

A naturally occurring radioactive metal. Radium is a radionuclide formed by the decay of uranium (U) and thorium (Th) in the environment. It occurs at low levels in virtually all rock, soil, water, plants, and animals. Radon (Rn) is a decay product of radium.

**Radon (Rn)**

A naturally occurring radioactive gas found in soils, rock, and water throughout the United States. Radon causes lung cancer and is a threat to health because it tends to collect in homes, sometimes to very high concentrations. As a result, radon is the largest source of exposure to people from naturally occurring radiation.

**Rail fixed guideway  
system**

Any light, heavy, or rapid rail system, monorail, inclined plane, funicular, trolley, or automated guideway that: 1. Is not regulated by the Federal Railroad Administration; and 2. Is included in FTA's calculation of fixed guideway route miles or receives funding under FTA's formula program for urbanized areas (49 U.S.C.. 5336); or 3. Has submitted documentation to FTA indicating its intent to be included in FTA's calculation of fixed guideway route miles to receive funding under FTA's formula program for urbanized areas (49 U.S.C.. 5336).

**Rail transit agency**

An entity that operates a rail fixed guideway system.

**Rail transit system (RTS)**

The organization or portion of an organization that operates rail transit service and related activities. Syn: operating agency, operating authority, transit agency, transit authority, transit system.

**Rail transit vehicle**

The rail transit agency's rolling stock, including but not limited to passenger and maintenance vehicles.

**Rail Transit-Controlled  
Property**

Property that is used by the rail transit agency and may be owned, leased, or maintained by the rail transit agency.

**Railroad Carfloat**

A barge equipped with railroad tracks used to move rail cars across water. Typically, a tugboat tows the carfloat.

**Random**

Totally by chance.

**Range**

A simple measure of dispersion.

**Raw data**

Data that have not yet been transformed.

**Readiness**

The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.

**Reception area**

A location separate from staging areas, where resources report in for processing and out-processing. Reception Areas provide accountability, security, situational awareness briefings, safety awareness, distribution of IAPs, supplies and equipment, feeding, and bed down.

<b>Reconnaissance</b>	The surveying of a location and surrounding area to note locations of things of value or interest and security resources.
<b>Recover</b>	The likelihood of some event occurring. A numerical property attached to an activity or event whereby the likelihood of its future occurrence is expressed or clarified.
<b>Recovery<sup>1</sup></b>	The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; postincident reporting; and development of initiatives to mitigate the effects of future incidents.
<b>Recovery<sup>2</sup></b>	The long-term activities beyond the initial crisis period and emergency response phase of disaster operations that focus on returning all systems in the community to a normal status or to reconstitute these systems to a new condition that is less vulnerable.
<b>Recovery plan</b>	A plan developed by a State, local, or tribal jurisdiction with assistance from responding Federal agencies to restore the affected area.
<b>Recovery/resumption</b>	Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.
<b>Redundant communications system</b>	A backup system of communications to be used in the event of a failure of the primary communications system. Such redundant systems may consist of a portable radio carried by a train crewmember, a cellular telephone available to a crewmember or multiple hardwired radios in the consist of a train.
<b>Reflectance factor</b>	The ratio of the luminous flux reflected by a surface to the luminous flux it receives.
<b>Region</b>	As used in this document, “region” generally refers to a geographic area consisting of contiguous State, local, and tribal entities located in whole or in part within a designated planning radius of a core high threat urban area. The precise boundaries of a region are self defined.
<b>Regional operations center (ROC)</b>	The temporary operations facility for the coordination of federal response and recovery activities located at the FEMA Regional Office (or Federal Regional Center) and led by the FEMA Regional Director or Deputy Director until the DFO becomes operational. After the ERT-A is deployed, the ROC performs a support role for federal staff at the disaster scene.
<b>Regulatory body</b>	Any state board, commission, department, or office, except those in the legislative or judicial branches, authorized by law to conduct adjudicative proceedings, issue permits, registrations, licenses, or other forms of authorization to offer or perform private security officer services, or to control or affect the interests of identified persons.
<b>Rehearsal</b>	The act of training by practicing the act being planned.
<b>Reimbursement</b>	Provides a mechanism to recoup funds expended for incident-specific activities.
<b>Relative risk</b>	The ratio between the risk for disease in an irradiated population to the risk in an unexposed population.
<b>Reliability<sup>1</sup></b>	Consistency in data measurement.
<b>Reliability<sup>2</sup></b>	To get back; to regain; to get back (a position of readiness).
<b>Rem (roentgen equivalent, man)</b>	A unit of equivalent dose. Not all radiation has the same biological effect, even for the same amount of absorbed dose. Rem relates the absorbed dose in human tissue to the effective biological damage of the radiation. It is deter-

mined by multiplying the number of rads by the quality factor, a number reflecting the potential damage caused by the particular type of radiation. The rem is the traditional unit of equivalent dose, but it is being replaced by the sievert (Sv), which is equal to 100 rem.

<b>Remanufactured equipment</b>	A car that has been structurally restored and has new or rebuilt components at a cost of 60% or more of vehicle replacement costs to extend its service life.
<b>Replacement costs</b>	Building component replacement and related costs, included in the capital budget, that are expected to be incurred during the study period.
<b>Report printers</b>	A separate, dedicated printer attached to the Electronic Security Systems used for generating reports utilizing information stored by the central computer.
<b>Request-to-exit device</b>	Passive infrared motion sensors or push buttons that are used to signal an Electronic Entry Control System that egress is imminent or to unlock a door.
<b>Resilience</b>	The capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack, natural disaster, or other incident.
<b>Resolution</b>	The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution.
<b>Resource management<sup>1</sup></b>	Efficient incident management requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under the NIMS includes mutual-aid agreements; the use of special Federal, State, local, and tribal teams; and resource mobilization protocols.
<b>Resource management<sup>2</sup></b>	Those actions taken by a government to: identify sources and obtain resources needed to support disaster response activities; coordinate the supply, allocation, distribution, and delivery of resources so that they arrive where and when most needed; and maintain accountability for the resources used.
<b>Resource tracking</b>	A standardized, integrated process conducted prior to, during, and after an incident by all emergency management/response personnel and their associated organizations.
<b>Resources</b>	Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.
<b>Resources unit</b>	Functional unit within the Planning Section responsible for recording the status of resources committed to the incident. This unit also evaluates resources currently committed to the incident, the effects additional responding resources will have on the incident, and anticipated resource needs.
<b>Response</b>	Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.
<b>Response force</b>	The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordnance disposal team, or a fire department.

<b>Response time</b>	The length of time from the instant an attack is detected to the instant a security force arrives on site.
<b>Restore</b>	To bring back to a former or normal position.
<b>Restricted area</b>	Any area with access controls that is subject to these special restrictions or controls for security reasons. See controlled area, limited area, exclusion area, and exclusion zone.
<b>Retinal pattern</b>	A biometric technology that is based on features of the human eye.
<b>Retrofit</b>	The modification of an existing building or facility to include new systems or components.
<b>Retrograde</b>	To return resources back to their original location.
<b>Retroreflective material</b>	A material that is capable of reflecting light rays back to the light source.
<b>Retrospective</b>	Looking back at or examining data that have already been acquired.
<b>RF data transmission</b>	A communications link using radio frequency to send or receive data.
<b>Ribbon fuse</b>	A cylindrical fuse consisting of a ribbon shaped fusible metal enclosed in a glass or transparent plastic cylinder with end caps.
<b>Risk<sup>1</sup></b>	Refers to exposure to conditions (criminal or terrorist) that can cause death, physical harm, or equipment/property damage.
<b>Risk<sup>2</sup></b>	A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.
<b>Risk<sup>3</sup></b>	A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the Transportation Systems Sector-Specific Plan (SSP), risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss within or utilizing the sector.
<b>Risk<sup>4</sup></b>	The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.
<b>Risk<sup>5</sup></b>	The likelihood that an event will occur which will cause the loss or diminished use of an asset – a function of asset value and the impact and likelihood of threat and vulnerabilities (envoy). The combination of two factors: (1) the value placed on an asset and consequence of an undesired on that asset; (2) the likelihood that a specific vulnerability will be exploited by a specific threat (ARM). The probability that a particular critical infrastructure’s vulnerability being exploited by a particular threat weighted by the impact of that exploitation (CIAO). Measure of the potential damage to or loss of an asset based on the probability of an undesirable occurrence (RAM-Wsm). The potential for realization of unwanted, negative consequences of an event.
<b>Risk acceptance</b>	Willingness of an individual, group, or society to accept a specific level of risk to obtain some gain or benefit.
<b>Risk analysis</b>	The body of theory and practice that has evolved to help decision-makers assess their risk exposures and risk attitudes so that the investment that is “best for them” is selected.
<b>Risk assessment<sup>1</sup></b>	Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization’s operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.
<b>Risk assessment<sup>2</sup></b>	A systematic process whereby assets are identified and valued, credible threats to those assets are enumerated, applicable vulnerabilities are documented, potential impacts or consequences of a loss event are described, and a qualitative or quantitative analysis of resulting risks is produced. Risks are generally reported in order of priority or severity and attached to some description of a level of risk.

<b>Risk assessment</b> <sup>3</sup>	A comprehensive study of a transit agency to identify components most vulnerable to criminal activity, including acts of terrorism and quasi-terrorism, and to assess the impact of such activity on passengers, employees, and the agency.
<b>Risk level</b>	A combination of the two factors pertaining to impact of loss and probability of adverse event (ARM).
<b>Risk management</b> <sup>1</sup>	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk.
<b>Risk management</b> <sup>2</sup>	The process of measuring or assessing risk and then developing strategies to manage the risk. Involves a prioritization process through which risks with the greatest adverse consequences and greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later if at all. Requires balancing risks with a high probability of occurrence but lower loss against risks with high loss but lower probability.
<b>Risk mitigation</b>	The actions or decisions designed to reduce the financial and nonpecuniary risk from uncertain events.
<b>Risk views</b>	Risk views describe types of systems in terms of mode, geography, function, and ownership. These four views capture multiple ways of addressing systems and allow for a robust assessment of the Transportation Systems Sector.
<b>Roadways</b>	Any surface intended for motorized vehicle traffic.
<b>Roentgen</b>	A unit of exposure to x-rays or gamma rays. One roentgen is the amount of gamma or x-rays needed to produce ions carrying 1 electrostatic unit of electrical charge in 1 cubic centimeter of dry air under standard conditions.
<b>Roll-On/Roll-Off (RO/RO) Vessel</b>	A vessel with ramps that allows wheeled vehicles to be loaded and discharged without cranes.
<b>Root cause analysis</b>	A technique used to identify the conditions that initiate the occurrence of an undesired activity or state.
<b>Rotakin CCTV video target</b>	Developed by UK Police Scientific Development Board for testing CCTV system level performance and resolution capabilities, including playback and recordings, end to end. Also known as Rotatest.
<b>Rotating drum or rotating plate vehicle barrier</b>	An active vehicle barrier used at vehicle entrances to controlled areas based on a drum or plate rotating into the path of the vehicle when signaled.
<b>RS-232 data</b>	IEEE Recommended Standard 232; a point-to-point serial data protocol with a maximum effective distance of 50 feet.
<b>RS-422 data</b>	IEEE Recommended Standard 422; a point-to-point serial data protocol with a maximum effective distance of 4,000 feet.
<b>RS-485 data</b>	IEEE Recommended Standard 485; a multi-drop serial data protocol with a maximum effective distance of 4,000 feet.
<b>Rural service</b>	Providing transportation across rivers and lakes when the construction of bridges is not warranted. Typically, these routes are short, operate on demand, carry a limited number of vehicles, and accommodate pedestrians and bicycles.
<b>S.I. units</b>	The Systeme Internationale (or International System) of units and measurements. This system of units officially came into being in October 1960 and has been adopted by nearly all countries, although the amount of actual usage varies considerably.
<b>Sacrificial roof or wall</b>	Roofs or walls that can be lost in a blast without damage to the primary asset.
<b>Safe activity</b>	A target neutral activity that results in increased natural surveillance.
<b>Safe haven</b>	Secure areas within the interior of the facility. A safe haven should be designed such that it requires more time to penetrate by aggressors than it takes for the response force to reach the protected area to rescue the occupants. It may be a haven from a physical attack or air-isolated haven from CBR contamination.

<b>Safety</b>	Freedom from harm resulting from unintentional acts or circumstances.
<b>Safety officer</b>	A member of the Command Staff responsible for monitoring incident operations and advising the IC on all matters relating to operational safety, including the health and safety of emergency responder personnel.
<b>Scramble keypad</b>	A pad that uses keys on which the numbers change pattern with each use to enhance security by preventing eavesdropping observation of the entered numbers.
<b>Screening</b>	A reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers, and its crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury due to sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices or other items that pose a real danger of violence or a threat to security are not present.
<b>Seasonal service</b>	Service provided during a limited period each year.
<b>Secondary asset</b>	An asset that supports a primary asset and whose compromise would indirectly affect the operation of the primary asset.
<b>Secondary enclosure</b>	A portable enclosure system that can be installed within a facility if the facility cannot be sealed economically to maintain an overpressure but is suitable as a shell.
<b>Secondary hazard</b>	A threat whose potential would be realized as the result of a triggering event that of itself would constitute an emergency (e.g., dam failure might be a secondary hazard associated with earthquakes).
<b>Section</b>	The organizational level having responsibility for a major functional area of incident management, e.g., Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established). The section is organizationally situated between the branch and the Incident Command.
<b>Sector</b>	The logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The Transportation Systems Sector is one of 17 critical infrastructure and key resources (CI/KR) sectors.
<b>Sector coordinating council</b>	The private sector counterpart to the GCC, this council is a self organized, self-run, and self-governed representative of the sector's key stakeholders.
<b>Sector partnership model</b>	The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector entities.
<b>Sector-specific agency (SSA)</b>	Federal departments and agencies identified in Homeland Security Presidential Directive 7 (HSPD-7) as responsible for CI/KR protection activities in specified CI/KR sectors. The sector-specific agency for transportation is the Transportation Security Administration (TSA).
<b>Sector-specific plan (SSP)</b>	The augmenting plan that complements and extends the National Infrastructure Protection Plan (NIPP) Base Plan, detailing the application of the NIPP framework specific to each CI/KR sector. SSPs are developed by the SSAs in close collaboration with other security partners. This document is the SSP for the Transportation Systems Sector.
<b>Secure/access mode</b>	The state of an area monitored by an intrusion detection system in regards to how alarm conditions are reported.
<b>Security</b>	Freedom from harm resulting from intentional acts or circumstances.
<b>Security analysis</b>	The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.
<b>Security and Emergency Preparedness Plan</b>	The formal plan that documents the transportation's system security program and also addressed the elements of that program that affect emergency preparedness for events resulting from intentional acts.

<b>Security breach</b>	An unforeseen event or occurrence that endangers life or property and may result in the loss of services or system equipment.
<b>Security console</b>	Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.
<b>Security engineering</b>	The process of identifying practical, risk managed short- and long-term solutions to reduce and/or mitigate dynamic manmade hazards by integrating multiple factors, including construction, equipment, manpower, and procedures.
<b>Security engineering design process</b>	The process through which assets requiring protection are identified, the threat to and vulnerability of those assets is determined, and a protective system is designed to protect the assets.
<b>Security incident</b>	An unforeseen event or occurrence that does not necessarily result in death, injury, or significant property damage but may result in minor loss of revenue.
<b>Security management system database</b>	In a Security Management System, a database that is transferred to various nodes or panels throughout the system for faster data processing and protection against communications link downtime.
<b>Security management system distributed processing</b>	In a Security Management System, a method of data processing at various nodes or panels throughout the system for faster data processing and protection against communications links downtime.
<b>Security partner</b>	Federal, State, regional, Territorial, local, or tribal governmental entities; private sector owners and operators; and representative organizations, academic and professional entities, and certain not-for-profit private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.
<b>Security screen</b>	An IDS sensor that utilizes a mesh of breakwires to alarm an IDS when open or broken.
<b>Security sweep</b>	A walkthrough to visually inspect unrestricted areas to identify unattended packages, briefcases, or luggage and determine that all restricted areas are secure.
<b>Security threat</b>	Any intentional action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services.
<b>Segmentation for fingerprints</b>	The separation of an N finger image into N single finger images
<b>Segmented routes</b>	Portions of a fixed route. When a ferry stops in between the two fixed points, it has just completed a segment of the overall route.
<b>Segregation of duties</b>	Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to minimum essential infrastructure resource elements.
<b>Selection</b>	The act or process of choosing individuals who possess certain characteristics or qualities.
<b>Semi-hardened construction</b>	Construction that provides protection against near-miss detonations of large general purpose military bombs and direct hits from smaller munitions.
<b>Semi-isolated fenced perimeters</b>	Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence and where the general public or other personnel seldom have reason to be in the area.
<b>Senior FEMA Official (SFO)</b>	The official appointed by the Director of FEMA, or his representative, that is responsible for deploying to the JOC to serve as the senior interagency consequence management representative on the Command Group, and to manage and coordinate activities taken by the Consequence Management Group.
<b>Sensitive Information</b>	Information or knowledge that might result in loss of an advantage or level of security if disclosed to others.
<b>Sensitive security information (SSI)</b>	A specific category of transportation security information that the Transportation Security Administration has determined must be protected from improper disclosure to ensure transportation security as defined by 49 CFR Part 1520.



<b>Sensitivity</b>	Ability of an analytical method to detect small concentrations of radioactive material.
<b>Sensor processing</b>	Equipment and computer processors that receive sensor inputs and determine if an alarm condition exists. Provides binary output of processing decision.
<b>Serial interface</b>	An integration strategy for data transfer where components are connected in series.
<b>Service area</b>	The geographic boundaries which define the legal and/or management commitment of a public transportation system to provide service to passengers.
<b>Service dog</b>	A dog owned, trained, certified, and insured by a transportation system, its designees, or its contractors to perform work.
<b>Shelter-in-place</b>	The process of securing and protecting people and assets in the general area in which a crisis occurs.
<b>Shelter-in-place protection mode</b>	Mode that consists of de-energizing the ventilation system and closing the outside air intake and exhaust dampers using a master control capability.
<b>Shielded wire</b>	Wire with a conductive wrap used to mitigate electromagnetic emanations.
<b>Shielding</b>	The material between a radiation source and a potentially exposed person that reduces exposure.
<b>Sievert (Sv)</b>	Unit used to derive a quantity called dose equivalent. This relates the absorbed dose in human tissue to the effective biological damage of the radiation. Not all radiation has the same biological effect, even for the same amount of absorbed dose. Dose equivalent is often expressed as millionths of a sievert, or micro-sieverts ( $\mu\text{Sv}$ ). One sievert is equivalent to 100 rem.
<b>Significance levels</b>	The likelihood that numerical correlation values are reflective of real relationships and are not due to chance occurrences.
<b>Simulation exercise</b>	A test in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises are performed under conditions as close as practicable to “real world” conditions.
<b>Single resource</b>	An individual, a piece of equipment and its personnel complement, or a crew/team of individuals with an identified work supervisor that can be used on an incident.
<b>Situation assessment/size up</b>	Includes information developed by the first person at the scene of an emergency and is basic information transmitted to the communications center, and then conveyed to other agency elements concerned with the control of the event. Situation assessments should be updated as the event changes and control measures are implemented to return the situation to normal.
<b>Situation report</b>	Often contain confirmed or verified information regarding the specific details relating to the incident.
<b>Situational crime prevention</b>	A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.
<b>Smart card</b>	A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.
<b>Social security number</b>	A nine digit number resembling “123-00-1234” that is issued to an individual by the U.S. Social Security Administration. The original purpose of this number was to administer the Social Security program, but it has come to be used as a “primary key” (a de facto national ID number) for individuals within the United States. The nine-digit Social Security number is divided into three parts. The first three digits are the area number. Prior to 1973, the area number reflected the state in which an individual applied for a Social Security number. Since 1973,

the first three digits of a Social Security number are determined by the ZIP code of the mailing address shown on the application for a Social Security number. The middle two digits are the group number. They have no special geographic or data significance but merely serve to break the number into conveniently sized blocks for orderly issuance. The last four digits are serial numbers.

<b>Software level integration</b>	An integration strategy that uses software to interface systems. An example of this would be digital video displayed in the same computer application window and linked to events of a security management system.
<b>Somatic effects</b>	Effects of radiation that are limited to the exposed person, as distinguished from genetic effects, which may also affect subsequent generations.
<b>Span of control</b>	The number of individuals a supervisor is responsible for, usually expressed as the ratio of supervisors to individuals. (Under the NIMS, an appropriate span of control is between 1:3 and 1:7.)
<b>Spatial definition</b>	A natural form of access control that relies on space to control access to property.
<b>Special needs population</b>	Pertaining to a population whose members may have additional needs before, during, and after an incident in one or more of the following functional areas: maintaining independence, communication, transportation, supervision, and medical care. Individuals in need of additional response assistance may include those who have disabilities; who live in institutionalized settings; who are elderly; who are children; who are from diverse cultures, who have limited English proficiency, or who are non-English speaking; or who are transportation disadvantaged.
<b>Specific threat</b>	Known or postulated aggressor activity focused on targeting a particular asset.
<b>Splinter protected construction</b>	Construction that provides protection against weapon fragments and small arms fire and also prevents magnification of blast pressure from reflection off vertical surfaces.
<b>Stack effect</b>	Thermally driven air density differences between the building indoor and outdoor ambient conditions.
<b>Staging area <sup>1</sup></b>	Established for the temporary location of available resources. A Staging Area can be any location in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment.
<b>Staging area <sup>2</sup></b>	Location established where resources can be placed while awaiting a tactical assignment. The Operations Section manages Staging Areas.
<b>Standard operating guidelines</b>	A set of instructions having the force of a directive, covering those features of operations which lend themselves to a definite or standardized procedure without loss of effectiveness.
<b>Standard operating procedure (SOP)</b>	Complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.
<b>Standby mode</b>	Mode in which the CP system is energized only when there is a known threat of attack.
<b>Stand-off distance</b>	A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.
<b>Stand-off weapons</b>	Weapons such as anti-tank weapons and mortars that are launched from a distance at a target.
<b>State</b>	When capitalized, refers to any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.
<b>State Coordinating Officer (SCO)</b>	The person appointed by the Governor to coordinate state, commonwealth, or territorial response and recovery activities with FRP-related activities of the Federal Government, in cooperation with the FCO.

<b>State liaison</b>	A FEMA official assigned to a particular state, who handles initial coordination with the state in the early stages of an emergency.
<b>Stationary vehicle bomb</b>	An explosive-laden car or truck stopped or parked near a building.
<b>Statistical analysis</b>	The application of mathematics to large amounts of raw data to yield meaningful summary measurements.
<b>Stochastic effect</b>	Effect that occurs on a random basis independent of the size of dose. The effect typically has no threshold and is based on probabilities, with the chances of seeing the effect increasing with dose. If it occurs, the severity of a stochastic effect is independent of the dose received. Cancer is a stochastic effect. See also non-stochastic effect, deterministic effect.
<b>Strategic</b>	Strategic elements of incident management are characterized by continuous long-term, high-level planning by organizations headed by elected or other senior officials. These elements involve the adoption of long-range goals and objectives, the setting of priorities; the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness.
<b>Strategic Risk</b>	Those risks that impact the entire Transportation Systems Sector, threatening disruption across multiple stakeholder communities. The consequences of strategic risks can cross multiple sectors and can have far-reaching, long-term effects on the national economy, natural environment, or public confidence. Strategic risks are those that breach the threshold of risks that stakeholders are reasonably expected to manage on their own and move into an area of risk management. Illustrative examples of strategic risks to the sector could include: disruption of a mega-node in the transportation system (large-scale impact on national economic security), use of a component of the transportation system as a weapon of mass destruction (terrorism event leading to loss of life and of public confidence), and release of a biological agent at a major rail transfer station or hub airport (terrorism event affecting national public health and safety).
<b>Strategic risk objective (SRO)</b>	A measurable target that, when attained, contributes to the accomplishment of a strategic goal.
<b>Strategy</b>	The general plan or direction selected to accomplish incident objectives.
<b>Strike team</b>	A set number of resources of the same kind and type that have an established minimum number of personnel.
<b>Structural glazed window systems</b>	Window systems in which glazing is bonded to both sides of the window frame using an adhesive such as a high-strength, high-performance silicone sealant.
<b>Substate region</b>	A grouping of jurisdictions, counties, and/or localities within a State brought together for specified purposes (e.g., homeland security, education, public health), usually containing a governance structure.
<b>Superstructure</b>	The supporting elements of a building above the foundation.
<b>Supervisor</b>	The ICS title for an individual responsible for a Division or Group.
<b>Supporting agency</b>	An agency that provides support and/or resource assistance to another agency.
<b>Supporting technologies</b>	Any technology that may be used to support the NIMS is included in this subsystem. These technologies include orthophoto mapping, remote automatic weather stations, infrared technology, and communications, among various others.
<b>Surface burst</b>	A nuclear weapon explosion that is close enough to the ground for the radius of the fireball to vaporize surface material. Fallout from a surface burst contains very high levels of radioactivity.
<b>Survey</b>	An on-scene examination and evaluation of the physical characteristics of a vessel or facility and its security systems, processes, procedures, and personnel.
<b>System<sup>1</sup></b>	A collection of assets that comprises a dynamic, complex, and unified whole. A system maintains its existence and functions as a whole through the interaction of its parts.

<b>System</b> <sup>2</sup>	A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional), and procedures (standard operating, emergency operating, and training), which are integrated to perform a specific operational function in a specific environment.
<b>System security</b>	The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.
<b>System security management</b>	An element of management that defines the system security requirements and ensures the planning, implementation, and accomplishments of system security tasks and activities.
<b>System security plan</b>	A document developed and adopted by the rail transit agency describing its security policies, objectives, responsibilities, and procedures.
<b>System security program</b>	The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle.
<b>Systems-based risk management (SBRM)</b>	A risk management framework that helps define and clarify countermeasure programs aimed at a specific SRO, which will be integrated into the sector's strategic plan. SBRM is an important element of the sector's approach to determining its risk priorities, documenting them as SROs, determining approaches for achieving these objectives, and defining what success means for each of the SROs through performance measures. The SBRM process yields strategic countermeasures.
<b>Tabletop exercise</b>	A test method that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.
<b>Tactics</b>	The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.
<b>Tamper switch</b>	Intrusion detection sensor that monitors an equipment enclosure for breach.
<b>Tangle-foot wire</b>	Barbed wire or tape suspended on short metal or wooden pickets outside a perimeter fence to create an obstacle to approach.
<b>Target capabilities list</b>	Provides guidance on the specific capabilities and levels of capability that Federal, State, local, and tribal entities will be expected to develop and maintain.
<b>Target/asset</b>	Persons, facilities, activities, or physical systems that have value to the owner or to society as a whole.
<b>Task force</b>	Any combination of resources assembled to support a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader.
<b>Taut wire sensor</b>	An intrusion detection sensor utilizing a column of uniformly spaced horizontal wires, securely anchored at each end and stretched taut. Each wire is attached to a sensor to indicate movement of the wire.
<b>Technical assistance</b> <sup>1</sup>	The provisioning of direct assistance to states and local jurisdictions to improve capabilities for program development, planning, and operational performances related to responses to WMD terrorist incidents.
<b>Technical assistance</b> <sup>2</sup>	Support provided to State, tribal, and local jurisdictions when they have the resources but lack the complete knowledge and skills needed to perform a required activity (such as mobile-home park design or hazardous material assessments).
<b>Technical security</b>	Measures taken to identify, prevent or neutralize technical threats including electronic or electro-optic eavesdropping, wiretapping, bugging, signal intercept, covert/illicit surveillance, and attacks on Information Technology (IT) or telecommunications systems.

<b>Technical specialists</b>	Personnel with special skills that can be used anywhere within the ICS organization. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically certified in their fields or professions.
<b>Technical surveillance countermeasures</b>	Employment of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities.
<b>Technological hazards</b>	Incidents that can arise from human activities such as manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.
<b>Technology standards</b>	Standards for key systems may be required to facilitate the interoperability and compatibility of major systems across jurisdictional, geographic, and functional lines.
<b>Technology support</b>	Facilitates incident operations and sustains the research and development programs that underpin the long-term investment in the Nation's future incident management capabilities.
<b>Telephoto</b>	A term used to describe lenses that have a high focal number causing the reproduced image to appear larger than human eye reproduction.
<b>Tempest</b>	An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations" (e.g., TEMPEST tests, TEMPEST inspections).
<b>Terrestrial radiation</b>	Radiation emitted by naturally occurring radioactive materials, such as uranium (U), thorium (Th), and radon (Rn) in the earth.
<b>Terrorism<sup>1</sup></b>	An intentional act of violence that is intended to inflict significant damage to property, inflict casualties, and produce panic and fear.
<b>Terrorism<sup>2</sup></b>	The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
<b>Terrorism<sup>3</sup></b>	Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States in which it occurs and is intended to intimidate or coerce the civilian population or influence a government or affect the conduct of a government by mass destruction, assassination, or kidnapping. See Section 2 (15), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).
<b>Terrorism<sup>4</sup></b>	The FBI defines terrorism as, "the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in the furtherance of political or social objectives.
<b>Terrorist activity</b>	Includes a number of activities (including casing, reconnaissance, rehearsal, surveillance, and actual acts of violence) that are used to further a plan to perform an act of terrorism.
<b>Test object</b>	An item used to test the walk-through detection performance. The test object is an encased replica of a metallic item that is either a weapon, can be used as a weapon, or can be used to defeat security devices. The shape of the encasement is a parallelepiped. The encasement has up to 12 holes that allow the replica to be oriented with respect to the measurement coordinate system; no more than nine possible orientations are allowed, one to three orientations for each, but no more than three, unique orthogonal surfaces of the parallelepiped.
<b>Testing</b>	Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in the Business Continuity Plan.

<b>The General Risk Equation</b>	RISK = PROBABILITY × CONSEQUENCE “Probability” is an indication of the frequency and severity of an event – a characterization of “threat.” “Consequence” is an indication of the effects of that event on people, assets, or functions.
<b>Thermally tempered glass (TTG)</b>	Glass that is heat-treated to have a higher tensile strength and resistance to blast pressures, although with a greater susceptibility to airborne debris.
<b>Thermonuclear device</b>	A “hydrogen bomb.” A device with explosive energy that comes from fusion of small nuclei, as well as fission.
<b>Thorium (Th)</b>	A naturally occurring radioactive metal found in small amounts in soil, rocks, water, plants, and animals. The most common isotopes of thorium are thorium-232 (Th-232), thorium-230 (Th-230), and thorium-238 (Th-238).
<b>Threat<sup>1</sup></b>	The potential intentional act capable of disrupting or negatively impacting an asset. In other words, threats are deliberate attempts of a person or group to achieve various criminal or terrorist ends that may involve loss of life, loss of function, loss of visibility, and other objectives. Threats are distinct from hazards because they are not acts of nature, accidents, or organic happenstances for which tunnels are normally designed. Rather, threats are typically characterized as acts of intrusion; placement of explosive devices; and/or chemical, biological, or radiological attacks. In the case of terrorism, a threat consists of a scenario that combines a weapon, a host (i.e., an aggressor), a delivery mode, and tactics (i.e., a path of approach, the use of stealth or force, and the actual target of weapon placement). While hazards are associated with safety, threats are associated with security.
<b>Threat<sup>2</sup></b>	Any verbal or physical behavior or communication that reasonably could be interpreted as communicating or conveying intent to cause physical harm to a person or property.
<b>Threat aggressors</b>	Delivery tactics, and associated weapons, tools, or explosives against which a facility is protected; established by evaluating aggressor likelihood and objectives with respect to the assets.
<b>Threat analysis</b>	A continual process of compiling and examining all available information concerning potential threats and human-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.
<b>Threat and vulnerability assessment</b>	An evaluation performed to consider the likelihood that a specific threat will endanger the system, and to prepare recommendations for the elimination or mitigation of all threats with attendant vulnerabilities that meet pre-determined thresholds. These assessments typically include both revenue and non-revenue operations. Critical elements of these assessments include: (1) Threat Analysis: Defines the level or degree of the threats against a specific facility by evaluating the intent, motivation, and possible tactics of those who may carry them out. (2) Threat Probability: The probability a threat will occur at a specific facility during its life cycle (typically quantified as 25 years). Threat probability may be expressed in quantitative or qualitative terms. An example of a qualitative threat-probability ranking system is as follows: - Frequent: Event will occur within the system’s lifecycle (25 years) - Probable: Expect event to occur within the system’s lifecycle (25 years) - Occasional: Circumstances expected for that event; it may or may not occur within the system’s lifecycle (25 years) - Remote: Possible but unlikely to occur within the system’s lifecycle (25 years) - Improbable: Event will not occur within the system’s lifecycle (25 years) (3) Threat Severity: A qualitative measure of the worst possible consequences of a specific threat in a specific facility: - Category 1 - Catastrophic. May cause death or loss of a significant component of the transit system, or significant financial loss. - Category 2 - Critical. May cause severe injury, severe illness, major transit system damage, or major financial loss.

	- Category 3 - Marginal. May cause minor injury or transit system damage, or financial loss.
	- Category 4 - Negligible. Will not result in injury, system damage, or financial loss.
	(4) Threat Resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat.
	(5) Scenario analysis: An interpretive methodology that encourages role-playing by transportation personnel, emergency personnel.
	(6) Vulnerability Analysis: The systematic identification of physical, operational and structural components within transportation facilities and vehicles that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a given transit facility or vehicle, in its technological systems, and in the way it is operated (e.g., security procedures and practices or administrative and management controls). Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.
<b>Threat assessment</b>	The process to identify threat categories and adversaries, assessing the intent of each adversary, the capability of each adversary, the frequency of past incidents and an estimation of the threat relative to each critical asset.
<b>Threat assessment (TA)</b>	Threats fall into three categories: (1) Natural Disaster Events; (2) Unintentional Events (failures, incidents); and (3) Intentional Acts or Attacks. While generalized threat information can help in risk assessment, well constructed scenario based threat analysis represents the most effective method of establishing an effective threat threshold for a given target. Questions such as: "How likely is the event or an attack to occur?" or "How susceptible is the location to adverse weather?" or "How attractive is the target?" all help inform scenario based threat assessment.
<b>Threat management team</b>	Also termed an Incident Management Team. Personnel designated within an organization to receive, respond to, and resolve reported situations made under an organization's workplace violence program.
<b>Tier</b>	Groupings of jurisdictions that account for reasonable differences in expected capability levels among entities based on assessments of total population, population density, critical infrastructure, and other significant risk factors.
<b>Time/date stamp</b>	Data inserted into a CCTV video signal with the time and date of the video as it was created.
<b>TNT equivalent weight</b>	The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.
<b>Tone generator</b>	An inaudible cue, which alerts radio relay stations to activate themselves to allow the transmission of a message.
<b>Tools</b>	Those instruments and capabilities that allow for the professional performance of tasks, such as information systems, agreements, doctrine, capabilities, and legislative authorities.
<b>Toxic-free area</b>	An area within a facility in which the air supply is free of toxic chemical or biological agents.
<b>Toxicity</b>	A measure of the harmful effects produced by a given amount of a toxin on a living organism.
<b>Toxins</b>	Metabolic byproducts of living organisms that are classified as biological agents even though they are nonliving substances.
<b>Tracking</b>	A zoom lens' ability to remain in focus throughout the entire zoom range.
<b>Tracking and reporting resources</b>	A standardized, integrated process conducted throughout the duration of an incident. This process provides incident managers with a clear picture of where resources are located, helps staff prepare to receive resources, protects the safety of personnel and security of supplies and equipment, and enables the coordination of movement of personnel, equipment, and supplies.

<b>Trade secret</b>	All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.
<b>Train crewmember</b>	Railroad employee involved with the train movement of railroad rolling equipment and working together with other train crewmembers as an operating crew. This operating crew unit is under the charge and control of one crewmember, generally the conductor of the train, and is subject to the railroad operating rules and program of operational tests and inspections, as well as governed by the Hours of Service Act.
<b>Trainer</b>	An officer, contractor, or other employee qualified by a professional training center or certification agency as an expert in the training and use of service dogs and their handlers.
<b>Training</b>	An act, method, or process of instruction; to teach so as to make fit, qualified, or proficient.
<b>Transit bus</b>	A bus designed for frequent-stop service with front and center doors, normally with a rear-mounted diesel engine and low-back seating, and without luggage storage compartments or restroom facilities. Transit buses include motorbus and trolley coach.
<b>Transit operator</b>	A transportation system employee who is certified by the system to drive or operate a transit vehicle in passenger service, and who must comply with the procedures and rules specified by the system.
<b>Transit Supervisor</b>	A transportation system manager who has specific responsibilities in an emergency situation. The term supervisor typically refers to either a Line Supervisor (Rail) or a Street Supervisor (Bus), defined by the emergency response procedure governing a specific incident.
<b>Transitional structures and spaces</b>	Structures or spaces within buildings that are used to temporarily (less than 1 year) relocate occupants of another building while that building undergoes renovations, modifications, repairs, or restorations.
<b>Transportation</b>	Conveyance of passengers or goods. There are six modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline.
<b>Transportation security incident</b>	A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.
<b>Tribal</b>	Any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaskan Native Claims Settlement Act (85 stat. 688) [43 U.S.C.A. and 1601 et seq.], that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.
<b>Triple-standard concertina (TSC) wire</b>	This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two other rolls that run parallel to each other while resting on the ground, forming a pyramid.
<b>Tritium</b>	(Chemical symbol H-3) A radioactive isotope of the element hydrogen (chemical symbol H). See also deuterium.
<b>Twisted pair wire</b>	Wire that uses pairs of wires twisted together to mitigate electromagnetic interference.
<b>Two-person rule</b>	A security strategy that requires two people to be present in or gain access to a secured area to prevent unobserved access by any individual.



<b>Type</b>	A classification of resources in the ICS that refers to capability. Type 1 is generally considered to be more capable than Types 2, 3, or 4, respectively, because of size; power; capacity; or, in the case of incident management teams, experience and qualifications.
<b>Ultrasonic</b>	An IDS sensor system that utilizes high frequency sound for intrusion detection.
<b>Unaccompanied baggage</b>	Any baggage, including personal effects, not accompanied by a person who is boarding the vessel.
<b>Unified area command</b>	Established when incidents under an Area Command are multijurisdictional. See Area Command.
<b>Unified command</b>	An ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.
<b>Unified command system</b>	A unified team effort which allows all agencies with responsibility for the incident, either geographical or functional, to manage an incident by establishing a common set of incident objectives and strategies.
<b>Uniformat II</b>	An elemental format based on major components common to most buildings. It serves as a consistent reference for analysis, evaluation, and monitoring of buildings during the planning, feasibility, and design stages. It also enhances reporting at all stages in construction. The two cost types, building/facility elements and building/facility site work, under the building/facility component cost classification are associated with the elemental classification <i>UNIFORMAT II</i> . Subcategories under <i>UNIFORMAT II</i> include: substructure, shell, interiors, services, equipment & furnishings, special construction/demolition.
<b>Unit</b>	An organizational element having functional responsibility. Units are commonly used in Incident Planning, Logistics, or Finance/Administration sections and can be used in operations for some applications. Units are also found in EOC organizations.
<b>Unit leader</b>	The individual in charge of managing Units within an ICS functional section. The Unit can be staffed by a number of support personnel providing a wide range of services. Some of the support positions are pre-established within ICS (e.g., Base Camp Manager), but many others will be assigned as Technical Specialists.
<b>Unity of command</b>	The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.
<b>Universal task list</b>	A comprehensive menu of tasks from all sources that may be performed in major events illustrated by the National Planning Scenarios. Entities at all levels of government should use the UTL as a reference to help them develop proficiency through training and exercises to perform their assigned missions and tasks in major events.
<b>Unsafe condition or act</b>	Any condition or act which endangers life or property.
<b>Unshielded wire</b>	Wire that does not have a conductive wrap.
<b>Unstable nucleus</b>	A nucleus that contains an uneven number of protons and neutrons and seeks to reach equilibrium between them through radioactive decay (i.e., the nucleus of a radioactive atom).
<b>UPS Uninterruptible power supply</b>	System used to provide back up power in the event of loss of AC line power. Usually a system of AC to DC and DC to AC converters with a battery supply source.
<b>Uranium (U)</b>	A naturally occurring radioactive element whose principal isotopes are uranium-238 (U-238) and uranium-235 (U-235). Natural uranium is a hard,

	silvery-white, shiny metallic ore that contains a minute amount of uranium-234 (U-234).
<b>Urban services</b>	Services that provide trips into major cities or within their metropolitan commuting areas and experience periods of demand similar to those associated with other transportation services. Operators provide point-to-point transit or stops (e.g., across a harbor), linear service with multiple stops (e.g., along a waterfront), circulator service (e.g., fixed route, not fixed schedule), and water taxi service (e.g., fixed landings, passenger pick-up on demand).
<b>Useful field of view (UFOV)</b>	Useful field of view refers to the sensory, perceptual and attentional processes that address the ability to attend to one's surroundings, detect information and identify that which demands action. In terms of behavior, UFOV includes that information which can be extracted from a glance.
<b>Validity</b>	The extent to which differences in scores reflect true differences among subjects or groups of data in the characteristic that the measurement instrument attempts to measure.
<b>Vault</b>	A reinforced room for securing items.
<b>Vehicle ferries</b>	Vessels having at least one deck for vehicles, with additional decks for passengers.
<b>Vertical rod</b>	Typical door hardware often used with a crash bar to lock a door by inserting rods vertically from the door into the doorframe.
<b>Vessel Security Officer</b>	The person on-board the vessel, accountable to the master, and designated by the company as responsible for (a) security of the vessel, including implementation and maintenance of the vessel security plan, and (b) liaison with the facility security officer and the vessel's company security officer.
<b>Vessel security plan</b>	The plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with the vessel's cargoes and persons on-board at the respective MARSEC levels.
<b>Vessel stores</b>	(1) Materials on-board a vessel for the upkeep, maintenance, safety, operation, or navigation of the vessel and (2) materials on-board for the safety or comfort of the vessel's passengers or crew, including any provisions for the vessel's passengers or crew.
<b>Vessel traffic service (VTS)</b>	A national transportation system that collects, processes, and disseminates information on the marine operating environment and maritime vessel traffic in major U.S. ports and waterways.
<b>Vessel-to-port interface</b>	The interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, or vessel stores or the provisions of port services to or from the vessel.
<b>Vibration sensor</b>	An intrusion detection sensor that changes state when vibration is present.
<b>Video intercom system</b>	An intercom system that also incorporates a small CCTV system for verification.
<b>Video motion</b>	An IDS sensor system that analyses and compares video signal for the detection of intrusion.
<b>Video motion detection</b>	Motion detection technology that looks for changes in the pixels of a video image.
<b>Video multiplexer</b>	A device used to connect multiple video signals to a single location for viewing and/or recording.
<b>Video type lens</b>	An auto-iris lens with internal circuitry for processing of the video signal which controls the iris movements.
<b>Violence risk assessment</b>	Also termed a Threat Assessment. A Violence Risk Assessment refers to the investigative and analytical process followed by a specifically qualified professional to determine the nature of the threat and level of risk of violence presented by an individual and the steps to be taken to mitigate the risk.
<b>Visual displays</b>	A display or monitor used to inform the operator visually of the status of the electronic security system.

<b>Visual surveillance</b>	The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets.
<b>Vital records</b> <sup>1</sup>	Records or documents, for legal, regulatory, or operational purposes, that if irretrievably damaged, destroyed, or lost, would materially impair the organization's ability to continue business operations.
<b>Vital records</b> <sup>2</sup>	The essential agency records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records), or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).
<b>VMS Video monitoring system</b>	A complete video system including cameras, lenses, camera control, camera and control power, signal transmission, video display, video switching, video control, and video recording.
<b>Voice recognition</b>	A biometric technology that is based on nuances of the human voice.
<b>Volume sensors</b>	Sensor used to monitor a physical space such as a room interior, volume around a door, or volume adjacent to a fence.
<b>Volumetric motion sensor</b>	An interior intrusion detection sensor that is designed to sense aggressor motion within a protected space.
<b>Volunteer</b>	For purposes of NIMS, a volunteer is any individual accepted to perform services by the lead agency (which has authority to accept volunteer services) when the individual performs services without promise, expectation, or receipt of compensation for services performed. See 16 U.S.C. 742f(c) and 29 CFR 553.101.
<b>Vulnerability</b> <sup>1</sup>	Any weakness which can be exploited by an adversary to gain access to an asset (ARM). An exploitable security weakness or deficiency at a facility (RAM-Wsm). The level of exposure of human life, property, and resources to damage from hazards (NOAA). A feature of a system, which, if exploited by an attacker, would enable the attacker to breach security. A characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.
<b>Vulnerability</b> <sup>2</sup>	A characteristic or flaw that renders an asset or system susceptible to destruction, incapacitation, or exploitation.
<b>Vulnerability Assessment (VA)</b>	<p>Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. A systematic evaluation process in which qualitative and/or quantitative techniques are applied to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts.</p> <p>In general, determining the vulnerability of a critical asset is the least difficult area of risk assessment. Both quantifiable and qualitative analysis can be performed to measure the current vulnerability status of the asset, as well as the effect of ongoing risk management improvements. Similarly, the return on investment of future actions can be forecast with some level of certainty. Vulnerability assessment considers the likeliness of a given scenario occurring by chance or intention. VA also postulates susceptibility and resultant damage.</p>
<b>Waivers</b>	Exemptions from requirements. Prior to operating, any facility owner or operator may apply for a waiver for any requirement that the facility owner or operator considers unnecessary in light of the nature or operating conditions of the facility.
<b>Warning</b>	The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause.

<b>Water taxis</b>	Very small passenger-only ferries (about 50 feet or less in length) that may operate in both fixed-route and on-demand service, depending on the time of day and patronage levels. They can load and unload very quickly and operate very frequently, sometimes to several different points around a harbor or along a river.
<b>Waterborne contamination</b>	Chemical, biological, or radiological agent introduced into and fouling a water supply.
<b>Weapon of mass destruction (WMD) <sup>1</sup></b>	Title 18, Section 2332a of U.S.C. defines WMD as bombs, grenades, rockets, missiles or similar devices, large-bore weapons, or parts to assemble such weapons; poison gas; any weapon involving a disease organism; any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.
<b>Weapons of mass destruction (WMD) <sup>2</sup></b>	Any device, material, or substance used in a manner, in a quantity or type, or under circumstances showing an intent to cause death or serious injury to persons, or significant damage to property. An explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life.
<b>Weapons-grade material</b>	Nuclear material considered most suitable for a nuclear weapon. It usually connotes uranium enriched to above 90-percent uranium-235 or plutonium with greater than about 90-percent plutonium-239.
<b>Weigand protocol</b>	A security industry standard data protocol for card readers.
<b>Whole body count</b>	The measure and analysis of the radiation being emitted from a person's entire body, detected by a counter external to the body.
<b>Whole body exposure</b>	An exposure of the body to radiation, in which the entire body, rather than an isolated part, is irradiated by an external source.
<b>Working radio</b>	A radio that can transmit to and receive from the operations control center (OCC) of the railroad (through repeater stations, if necessary) from any location within the rail system, with the exception of limited segments of territory where topography or transient weather conditions temporarily prevent effective communication.
<b>Working wireless communications</b>	A hard-wired radio, portable radio, cellular telephone, or other means of two-way communication, with the capability to communicate with either the OCC or an emergency responder of the railroad from any location within the rail system (with the exception of limited segments of territory where topography or transient weather conditions temporarily prevent effective communication).
<b>Workplace violence</b>	Workplace violence refers to a broad range of behaviors falling along a spectrum that, due to their nature and/or severity, significantly affect the workplace, generate a concern for personal safety, or result in physical injury or death.
<b>Workplace violence program</b>	A collection of policies, structures, and practices adopted by an organization to help prevent workplace violence and to assist the organization in effectively managing reported incidents of workplace violence or threats.
<b>Workplace violence typology</b>	U.S. occupational health and safety agencies have developed a workplace violence classification system, or Workplace Violence Typology, that categorizes workplace violence incidents according to the relationship of perpetrator to victim.
<b>X-ray</b>	Electromagnetic radiation caused by deflection of electrons from their original paths, or inner orbital electrons that change their orbital levels around the atomic nucleus. X-rays, like gamma rays can travel long distances through air and most other materials. Like gamma rays, x-rays require more shielding to

reduce their intensity than do beta or alpha particles. X-rays and gamma rays differ primarily in their origin: x-rays originate in the electronic shell; gamma rays originate in the nucleus.

**Zoom**

The ability of a CCTV camera to close and focus or open and widen the field of view.

**Zoom Ratio**

The ratio of the starting focal length (wide) to the ending focal length (telephoto) of a zoom lens. A 10X zoom will magnify the image at the wide end by 10 times.

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

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