



U.S. Department
of Transportation
**Federal Transit
Administration**

Security and Emergency Preparedness Action Items for Transit Agencies

A Resource Document for Transit Agencies

September 2014

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for implementing this resource is estimated to average one hour per emergency type, including the time for reviewing instructions, gathering and maintaining the data needed, and completing and reviewing the results. Send comments regarding this burden estimate or any other aspect of this document, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2014	3. REPORT TYPE AND DATES COVERED		
4. TITLE AND SUBTITLE Security and Emergency Preparedness Action Items for Transit Agencies: A Resource Document for Transit Agencies			5. FUNDING NUMBERS VT56A4/MJ555– FTA SAFETY AND SECURITY ASSESSMENTS (BMI)	
6. AUTHOR(S) Kevin L. Chandler, Jodi M. Rizek , and Pamela J. Sutherland			8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Battelle, 505 King Avenue, Columbus, OH 43201			10. SPONSORING/ MONITORING AGENCY REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Transit Safety and Oversight Federal Transit Administration, 1200 New Jersey Ave, S.E., Washington, D.C. 20590			10. SPONSORING/ MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT No Restrictions. Available From: National Technical Information Service/NTIS, Springfield, Virginia, 22161. Phone 703.605.6000, Fax 703.605.6900, Email [orders@ntis.fedworld.gov]			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) Prepared by the Federal Transit Administration's (FTA) Office of Transit Safety and Oversight, <i>Security and Emergency Preparedness Action Items for Transit Agencies: A Resource Document for Transit Agencies</i> is part of FTA's technical assistance to transit agencies. FTA and TSA collaborated to update and consolidate the FTA Tops 20 Action Items into 17 Action Items, which are aligned with TSA's BASE and the NTAS. These Action Items apply to all transit modes directly operated or contracted by transit agencies. Transit Agencies are encouraged to include all of these Action Items in their security programs scaled appropriately to risk environment and operation size. This document provides an explanation of the current 17 Action Items, including supporting topics that further explain the content of each Action Item. High-level elements are used to organize and group similar Action Items. Relevant resource documents developed by FTA, DHS, TSA, FEMA, NIST, TRB, USCG, and APTA's security standards program have been included for each high-level element. These documents were selected to provide users with additional information and provide industry benchmarks for potential implementation.				
14. SUBJECT TERMS Federal Transit Administration, Office of Transit Safety and Oversight, Security, Emergency Preparedness			15. NUMBER OF PAGES 26	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT None	

Table of Contents

	Page
Acronyms and Abbreviations	5
Introduction.....	8
Management and Accountability.....	10
Action Item 1. Establish written system security plans (SSPs) and emergency operations/response plans	11
Action Item 2. Define roles and responsibilities for security and emergency preparedness.....	11
Action Item 3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control.....	11
Action Item 4. Coordinate security and emergency operations/response plans with local and regional agencies	12
Security and Emergency Response Training	14
Action Item 5. Establish and maintain a security and emergency training program.....	14
National Terrorism Advisory System (NTAS).....	15
Action Item 6. Establish plans and procedures to respond to the National Terrorism Advisory System (NTAS) alert levels	15
Public Awareness	16
Action Item 7. Implement and reinforce a public security and emergency awareness program.....	16
Risk Management and Assessment	17
Action Item 8. Establish and use a risk management process	17
Risk Information Collection and Sharing.....	18
Action Item 9. Establish and use an information sharing process for threat and intelligence information	18
Drills and Exercises.....	19
Action Item 10. Conduct tabletop and functional drills.....	19
Cyber-security	20
Action Item 11. Develop a comprehensive cyber-security strategy	20
Facility Security, Access Controls, and Background Investigations.....	22
Action Item 12. Control access to security critical facilities with identification (ID) badges for all visitors, employees and contractors	22
Action Item 13. Conduct physical security inspections.....	22
Action Item 14. Conduct background investigations of employees and contractors.....	22

Table of Contents (cont.)

	Page
Document Control	25
Action Item 15. Control access to documents on security critical systems and facilities.....	25
Action Item 16. Process for handling and access to sensitive security information (SSI).....	25
Security Program Audits	26
Action Item 17. Establish and conduct security program audits	26

List of Tables

Table 1. Resource Document Links.....	9
---------------------------------------	---

Acronyms and Abbreviations

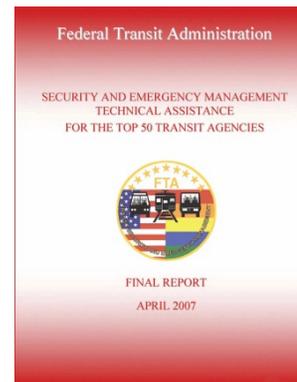
APTA	-	American Public Transportation Association
BASE	-	Baseline Assessment and Security Enhancement
CEO	-	chief executive officer
CCTV	-	closed circuit television
COOP	-	continuity of operations plan
CPG	-	comprehensive preparedness guide
CPTED	-	crime prevention through environmental design
CFR	-	Code of Federal Regulations
DCS	-	distributed control system
DHS	-	U.S. Department of Homeland Security
DOT	-	U.S. Department of Transportation
EOP	-	emergency operations plan
EOP	-	emergency operations procedure
ERP	-	emergency response plan
FBI	-	Federal Bureau of Investigation
FEMA	-	Federal Emergency Management Agency
FTA	-	Federal Transit Administration
HSAS	-	Homeland Security Advisory System
HSEEP	-	Homeland Security Exercise and Evaluation Program
HSIN	-	Homeland Security Information Network
HVAC	-	heating, ventilation, and air conditioning
ICS	-	incident command system
ICS	-	industrial control systems
ID	-	identification
IDPS	-	intrusion detection and prevention system
IED	-	improvised explosive device
IT	-	information technology
JTTF	-	Joint Terrorism Task Force
LAN	-	local area network
MAA	-	mutual aid agreement
MOA	-	memorandum of agreement
MOU	-	memorandum of understanding

Acronyms and Abbreviations (cont.)

NCHRP	-	National Cooperative Highway Research Program
NDRF	-	National Disaster Recovery Framework
NIMS	-	National Incident Management System
NIPP	-	National Infrastructure Protection Plan
NIST	-	National Institute of Science and Technology
NRF	-	National Response Framework
NTAS	-	National Terrorism Advisory System
NTD	-	National Transit Database
NVIC	-	Navigation and Vessel Inspection Circular
NYCTA	-	New York City Metropolitan Transportation Authority
PLC	-	programmable logic controller
PT-ISAC	-	Public Transportation – Information Sharing and Analysis Center
SCADA	-	supervisory control and data acquisition
SEPP	-	security and emergency preparedness plan
SOP	-	standard operations procedure
SSI	-	sensitive security information
SSP	-	system security plan
STSI	-	Surface Transportation Security Inspector
TCRP	-	Transit Cooperative Research Program
TEWG	-	Terrorism Early Warning Group
TSA	-	Transportation Security Administration
TSOC	-	Transportation Security Operations Center
TRB	-	Transportation Research Board
TVC	-	threat, vulnerability, and consequence
US-CERT	-	United States Computer Emergency Readiness Team
USCG	-	U.S. Coast Guard
WAN	-	wide area network
WMD	-	weapons of mass destructions

Introduction

Following the events of September 11, 2001, the Federal Transit Administration (FTA) developed security and emergency preparedness resources and provided technical assistance to transit agencies across the U.S. One of these activities was the development of the “Top 20 Security and Emergency Preparedness Action Items for Transit Agencies,” which was published by FTA in 2003. In 2006 FTA and TSA collaborated to update and consolidate the FTA Top 20 Action Items into the (17) “TSA/FTA Security and Emergency Preparedness Action Items for Transit Agencies.” The organization of these 17 Action Items and experience from the FTA and TSA technical assistance efforts were used by TSA to develop their voluntary security and emergency preparedness assessment tool, Baseline Assessment and Security Enhancement (BASE). TSA’s Surface Transportation Security Inspector (STSI) activity uses the BASE checklist to work with transit agencies on a voluntary basis to complete programmatic assessments of the security and emergency preparedness program.



In 2012, FTA and TSA revised the Action Items to ensure alignment with changes being made to TSA’s BASE. These recent changes are reflected in the Action Items presented in this document. The main changes to the Action Items were to add cyber-security as a topic, replace the now defunct color-coded Homeland Security Advisory System (HSAS) with the National Terrorism Advisory System (NTAS) and to revise and highlight the priorities of risk management and risk information gathering and analysis. All changes were made in consultation through the TSA’s Mass Transit Sector Coordinating Council chaired by the American Public Transportation Association (APTA).

These security and emergency preparedness Action Items are intended to reflect the high-level priority topics included in a transit agency’s security and emergency preparedness program¹. These Action Items apply to all transit modes directly operated or contracted by transit agencies (e.g., bus, bus rapid transit, light rail/streetcar, heavy rail, commuter rail, and paratransit). Transit agencies are encouraged to include all of these Action Items in their security programs scaled appropriately to risk environment and operation size.

This document provides an explanation of the current 17 Action Items, including supporting topics that further explain the content of each Action Item. High-level elements are used to organize and group similar Action Items. Relevant resource documents developed by FTA, DHS, TSA, FEMA, NIST, TRB, USCG and APTA’s security standards program have been included for each high-level element. These documents were selected to provide users with additional information and provide industry benchmarks for potential implementation. Table 1 provides links to the websites where these resource documents are located.

¹ Note that emergency preparedness at a transit agency is shared between the safety and security programs. In this document, emergency preparedness is presented from only the security program perspective.

Table 1. Resource Document Links

Source	Website(s)
APTA	http://www.apta.com/resources/standards/security/Pages/default.aspx
DHS	http://www.dhs.gov/preparedness-response-and-recovery-publications
FEMA	http://www.fema.gov/national-preparedness-resource-library http://www.fema.gov/media-library/assets/documents/25975
FTA	http://www.fta.dot.gov/TSO/12537.html http://www.fta.dot.gov/EmergencyManagement.html , http://bussafety.fta.dot.gov/help.php?id=6
NIST	http://www.nist.gov/publication-portal.cfm
TRB	http://pubsindex.trb.org/results.aspx#
TSA	http://www.tsa.gov/stakeholders
USCG	http://www.uscg.mil/hq/cg5/nvic/Security.asp

Management and Accountability

There are four Action Items under this element that address development, approval, and rolling out the security program and emergency operations/response plans, including regional coordination for these activities. The system security plan (SSP) or security and emergency preparedness plan (SEPP) provide an up-to-date description of the security program at a transit agency and used as the baseline to compare/audit and test the security-related activities. Capital projects also are also a part of the security program and emergency operations/response planning.

It is critical that the processes and activities described in the program documentation and emergency operations/response plans are well understood, approved, and endorsed by executive/senior level management at the transit agency. In addition, it is just as important that the roles and responsibilities for executing the security program and emergency operations/response plans are rolled out to and understood by staff. Performance metrics should be established so that managers and supervisors are held accountable and that all tasks have been addressed.

Transit agencies often have many emergency operations/response plans. These plans are developed in a similar fashion as the program documentation and require an update process to keep the plans current and accurate. Some plans describe operations for a specific type of event, and others describe overall operations or response. Types of emergency operations, contingency, or response plans are:

- Emergency operations plan (EOP)/emergency response plan (ERP) – includes specific plans such as hazardous material, bomb threat, suspicious package/improvised explosive device (IED), active shooter, weapons of mass destruction (WMD), and heightened threat/alert conditions
- Cyber incident response
- Business continuity planning – includes continuity of operations plan (COOP), loss of communications, loss of power
- Pandemic planning
- Weather/natural disaster plans – hurricane, winter (snow/ice), summer/heat, tornado, flood, earthquake, fire, and drought; this includes special staging of vehicles
- Special events plans – parades, festivals, and sporting events; this includes special staging of vehicles
- Evacuation plans – these could be notice or no-notice, includes facilities and stations, and special needs passengers

Another high-priority activity is coordination with local, regional, State, and Federal agencies with security and emergency preparedness/response responsibilities that overlap with the transit agency. The transit agency is expected to reach-out and participate in local, regional, State, and Federal planning, training/awareness, and drills and exercises. This participation needs to be used to advise the safety and security programs with those local, regional, State, and Federal expectations. The transit agency will also want to share important information with local and regional responders to protect the responders and the transit agency assets.

Action Item 1. Establish written system security plans (SSPs) and emergency operations/response plans

- a. Ensure that security and emergency operations/response plans are signed/approved by senior level management
- b. Review plans and documentation at least annually and update as circumstances warrant
- c. Ensure the security and emergency operations/response plans integrate visibility, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and to enhance deterrent effect
- d. Establish and maintain standard security and emergency operations procedures (SOPs/EOPs) for each mode operated, including procedures for operations control centers
- e. Establish plans and procedures that address specific threats from (i) improvised explosive devices (IED), (ii) weapons of mass destruction (WMD), and (iii) other high consequence risks identified in transit risk assessments
- f. Apply security design and crime prevention through environmental design (CPTED) criteria for major capital construction projects, system modifications, and procurements
- g. Ensure the security and emergency operations/response plans address continuity of operations
- h. Ensure security and emergency operations/response plans address business recovery

Action Item 2. Define roles and responsibilities for security and emergency preparedness

- a. Assign security and emergency preparedness activities to a senior level manager
- b. Maintain a current record of the name and title of the Primary and Alternate Security Coordinator (includes Security Directors and Transit Police Chiefs)
- c. Ensure that Security Coordinators report to senior level management
- d. Maintain accurate contact information for Security Coordinators and ensure they are accessible by telephonic and electronic communications means at all times
- e. Ensure that management defines and delegates security duties to front line employees
- f. Ensure that security and emergency operations/response plans are distributed to appropriate departmental personnel in the organization
- g. Hold regular senior staff and middle management security coordination meetings
- h. Hold informational briefings with appropriate personnel whenever security plans and procedures are substantially updated
- i. Establish lines of delegated authority/succession of security responsibilities and inform personnel

Action Item 3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control

- a. Hold regular supervisor and foreperson security review and coordination briefings
- b. Develop and maintain an internal security incident reporting system
- c. Ensure that a Security Review Committee (or other designated group) regularly reviews security incident reports, trends, and security program audit findings, and

makes recommendations to senior level management for changes to plans and procedures

Action Item 4. Coordinate security and emergency operations/response plans with local and regional agencies

- a. Coordinate with Federal and State governmental entities associated with public transportation security (e.g., Surface Transportation Security Inspectors (STSI) Area Office, State Office of Homeland Security, FTA Regional Office, Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF), Office of State Safety Oversight, etc.) in the regional area of the transit agency
- b. Ensure consistency with the National Incident Management System (NIMS) and the National Response Framework (NRF)
- c. Establish memorandums of agreement (MOA) or mutual aid agreements (MAA) with local government, fire, police and other entities with shared infrastructure (e.g., other transit agencies or rail systems)
- d. Maintain communications interoperability with first responders with security responsibilities in the transit system's regional area

Related Resource Documents

Security Program Documentation

- *The Public Transportation System Security and Emergency Preparedness Planning Guide*, FTA, 2003
- *Bus Safety and Security Program, Safety, Security, and Emergency Preparedness Excellence – A Roadmap*, FTA, 2012
- *Transit Security Design Considerations*, FTA, 2004
- *Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)*, APTA-SS-SRM-RP-001-09, Rev. 1, 2012
- *Security Planning for Public Transit*, APTA-SS-SIS-RP-011-13, 2013
- *Security Considerations for Public Transit*, APTA-SS-SIS-S-010-13, 2013
- *Random Counterterrorism Measures on Transit Systems*, APTA-SS-SRM-RP-006-11, 2011

Emergency Operations/Response and Regional Coordination

- *Response and Recovery for Declared Emergencies and Disasters, A Resource Document for Transit Agencies*, FTA, 2013
- *Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems*, FTA, 2004 (Law Enforcement Sensitive)
- *National Incident Management System*, DHS, 2008
- *National Response Framework (NRF)*, DHS, 2013
- *National Disaster Recovery Framework (NDRF)*, DHS, 2011
- *Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, Version 2.0*, FEMA, 2010
- *TCRP Report 160, Paratransit Emergency Preparedness and Operations Handbook*, TRB/TCRP, 2013
- *The Role of Transit in Emergency Evacuation*, TRB SF-294, 2008

- *TCRP Report 86, Volume 8, Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies*, TRB/TCRP, 2005
- *Standard for a Continuity of Operations Plan*, APTA-SS-SEM-S-001-08, 2008
- *Standard for Security & Emergency Management Aspects of Special Events Service*, APTA-SS-SEM-S-003-08, 2008
- *Recommended Practice for Participating in Mutual Aid*, APTA-SS-SEM-RP-011-09, 2009
- *Recommended Practice for First Responder Familiarization of Transit Systems*, APTA-SS-SEM-RP-002-08, 2008
- *Emergency Communication Strategies for Transit Agencies*, APTA-SS-SEM-RP-009-09, 2009
- *Developing a Contagious Virus Response Plan*, APTA-SS-SEM-S-005-09, 2009
- *Shelter of Transit Vehicles and Nonrevenue Equipment During Emergencies*, APTA-SS-SEM-S-006-09, 2009
- *Recommended Practice Creating an Alternate or Backup OCC*, APTA-SS-SEM-RP-007-09, 2009

Security and Emergency Response Training

Security and emergency response training is focused on assurance of job-specific certification and proficiency. Establishing a strong security and emergency response program is vital to ensuring that an agency can respond quickly during an unplanned or planned event. Employees and contractors who may provide a primary response to an event because of their job function should receive advanced and refresher training on a regular basis. The training should reinforce roles and responsibilities in an event, as well as measure proficiency in carrying out assigned duties. Proficiency expectations for employees and contractors should determine content of the training classes.

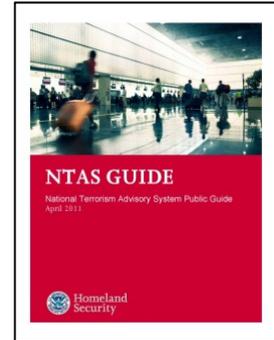
- Action Item 5.** Establish and maintain a security and emergency training program
- a. Provide ongoing basic training to all employees in (i) security orientation/awareness and (ii) emergency response
 - b. Provide ongoing advanced (i) security and (ii) emergency response training by job function, including actions at incremental threat levels, to field supervisors, controllers/dispatchers, fare inspectors, law enforcement personnel, operators, maintenance personnel (field and vehicle)
 - c. Provide ongoing advanced security training programs for transit managers, including but not limited to chief executive officers (CEOs), General Managers, Operations Managers, and Security Coordinators (includes Security Directors and Transit Police Chiefs)
 - d. Regularly update security awareness, emergency response, and counter-terrorism training materials to address (i) improvised explosive devices (IEDs), (ii) weapons of mass destruction (WMD) and (iii) other high consequence risks identified through the transit agency's system risk assessments
 - e. Ensure that security training programs reinforce security roles, responsibilities, and duties of employees, and ensure proficiency in their performance
 - f. Ensure security training programs emphasize integration of visible deterrence, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and heighten deterrent effect
 - g. Establish a system that records personnel training in (i) security and (ii) emergency response: initial training, recurrent training (periodic, refresher), establish and maintain a security notification process to inform personnel of significant updates to security and emergency operations/response plans and procedures

Related Resource Documents

- *Immediate Actions for Transit Employees: Protecting Against Life-Threatening Emergencies, A Resource Document for Transit Agencies*, FTA, 2011
- *Security Awareness Training for Transit Employees*, APTA-SS-SRM-RP-005-12, 2012

National Terrorism Advisory System (NTAS)

In support of terrorism prevention and protection, the National Terrorism Advisory System (NTAS)² was implemented in 2011 and the Homeland Security Advisory System (HSAS) color codes were discontinued. The NTAS is a two-level terrorism threat advisory scale, “elevated” and “imminent.” An elevated threat alert “warns of a credible terrorist threat against the United States.” An imminent threat alert “warns of a credible, specific, and impending terrorist threat against the United States.” In addition, the TSA works with public transportation agencies and provides communications of potential security protective measures and strategies that can be used during higher-threat levels, such as NTAS threat advisories.



Action Item 6. Establish plans and procedures to respond to the National Terrorism Advisory System (NTAS) alert levels

- a. Security and emergency operations/response plans and procedures should identify incremental actions to be implemented at NTAS alert levels
- b. Exercises should test implementation of the preventive measures for NTAS alert levels, including random application of security measures

Related Resource Documents

- *National Terrorism Advisory System Public Guide*, DHS, 2011
- *TSA Mass Transit, Bus and Passenger Rail Security Awareness Message, Protective Measures December 6, 2011*, TSA
- *Random Counterterrorism Measures on Transit Systems*, APTA-SS-SRM-RP-006-11, 2011

² The NTAS and related documents are available from DHS at <http://www.dhs.gov/national-terrorism-advisory-system>.

Public Awareness

This element is focused on establishing activities for public communications and awareness of security and emergency preparedness. Communications include public address systems, electronic message boards, posters, channel cards on vehicles, fliers, internet website, email, phone systems, etc. The frequency of messaging and content of the communication under various hazard and threat situations needs to be considered. All types of emergency situations need to be considered such as natural and man-made situations. Special event communications should also be included in these activities.

Part of this activity includes establishing the ability for the public to communicate problems (hazards and threats) within the transit system. This activity also includes communicating the agency's interest in having this hazard and threat information and how the agency will respond to anything reported. Based on experience through day-to-day operations, real emergencies, and drills and exercises, the transit agency should make improvements and changes to these communications activities and products on a regular basis.

Action Item 7. Implement and reinforce a public security and emergency awareness program

- a. Develop and implement a public security and emergency awareness program
- b. Prominently display security awareness and emergency preparedness information materials throughout the system (e.g., channel cards, posters, fliers)
- c. Incorporate general security awareness and emergency preparedness into public announcement messages (e.g., security messages and evacuation procedures) in stations (e.g., electronic message boards, voice) and on board vehicles
- d. Post security awareness and emergency preparedness information on the transit agency website
- e. Ensure security awareness materials and announcements emphasize the importance of vigilance and provide clear direction to the public on reporting of suspicious activities
- f. Vary the content and appearance of messages to retain public interest
- g. Increase the frequency of security/emergency awareness activities (e.g., public address announcements) as threat situation changes
- h. Issue public service announcements in local media (e.g., newspaper, radio and/or television)
- i. Provide volunteer training to the public for system evacuations and emergency response

Related Resource Documents

- *Transit Watch*, FTA
- *See Something, Say Something*, NYCTA, endorsed by DHS
- *Security Planning for Public Transit*, APTA-SS-SIS-RP-011-13, 2013
- *Security Considerations for Public Transit*, APTA-SS-SIS-S-010-13, 2013

Risk Management and Assessment

Risk management is a continuous process of identifying and monitoring critical assets; assessing threats, vulnerabilities and consequences; setting goals; and developing mitigation strategies. By using a risk management process that is based on a system-wide approach to managing risks, transit agencies can work to identify critical assets and processes so they can be properly protected. This will help the transit agency minimize threats and vulnerabilities to the transit system to a level as low as reasonably practicable while also reducing consequences from an unplanned or planned event.

Risk management at transit agencies typically includes hazard analysis for safety; threat, vulnerability, and consequence (TVC) assessment for security, and capabilities assessment for emergency preparedness. In addition, it is essential that the transit agency have an all-hazards prioritization process to manage conflicts between the safety and security program assessments and also to take advantage of synergies that improve both programs at the same time. Another aspect of risk management and assessment is that these apply to operations and maintenance of the transit system and capital projects.

Action Item 8. Establish and use a risk management process

- a. Establish a risk management process that is based on a system-wide assessment of risks and obtain management approval of this process
- b. Ensure proper training of management and staff responsible for managing the risk assessment process
- c. Update the system-wide risk assessment whenever a new asset/facility is added or modified, and when conditions warrant (e.g., changes in threats or intelligence)
- d. Use the risk assessment process to prioritize security investments
- e. Coordinate with regional security partners, including Federal, State, and local governments and entities with shared infrastructure (e.g., other transit agencies or rail systems), to leverage resources and experience for conducting risk assessments (e.g., leverage resources such as the Security Analysis and Action Program operated by TSA's Surface Transportation Security Inspectors (STSI))

Related Resource Documents

- *The Public Transportation System Security and Emergency Preparedness Planning Guide*, FTA, 2003
- *Handbook for Transit Safety and Security Certification*, FTA, 2000
- *An Introduction to All-hazards Preparedness for Transit Agencies*, FTA, 2010
- *Risk Management Fundamentals, Homeland Security Risk Management Doctrine*, DHS, 2011
- *Threat and Hazard Identification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201, First Edition*, DHS, 2012
- *Crime Prevention through Environmental Design (CPTED)*, APTA-SS-SIS-RP-007-10, 2010

Risk Information Collection and Sharing

This element addresses risk monitoring and continuous improvement of the transit agency security program. Risk monitoring is the process for measuring the effectiveness of risk controls and mitigation set through risk management and assessment, and results in risk-based, data-driven decision-making. The action item (below) is focused on risk information collection and sharing at the transit agency and with local, regional, State, and Federal partners and information sharing organizations. In addition, the transit agency is responsible for notifying and reporting specific events to local, State, and Federal agencies, such as FTA's National Transit Database (NTD), the State Safety Oversight Agency for rail transit agencies, and TSA's Transportation Security Operations Center (TSOC).

Action Item 9. Establish and use an information sharing process for threat and intelligence information

- a. Participate in information sharing networks or arrangements with:
 - i. State and local law enforcement and homeland security officials
 - ii. DHS's Homeland Security Information Network (HSIN) and its mass transit portal (The HSIN portal enables secure information sharing among transit agencies and passenger rail systems at no cost to users)
 - iii. FBI Joint Terrorism Task Force (JTTF) and/or other regional anti-terrorism task force (e.g., Terrorism Early Warning Group (TEWG), US Attorney's Office)
 - iv. TSA Surface Transportation Security Inspectors (STSI)
 - v. Public Transportation Information Sharing and Analysis Center (PT-ISAC)
- b. Through training and awareness programs, ensure transit agency employees understand the what, how, and when to report observed suspicious activity or items
- c. Use exercises to test employee awareness and the effectiveness of reporting and response procedures
- d. Ensure public awareness materials and announcements provide clear direction to the public on reporting of suspicious activity
- e. Maintain plans and procedures to ensure that designated Security Coordinator(s) report threats and significant security concerns to appropriate law enforcement authorities and TSA's Transportation Security Operations Center (TSOC)
- f. Maintain plans and procedures that ensure actionable security events are included in reports to the FTA's National Transit Database (NTD)

Related Resource Documents

- *The Public Transportation System Security and Emergency Preparedness Planning Guide*, FTA, 2003
- *National Transit Database (NTD), Safety and Security Reporting Manual*, FTA, 2013

Drills and Exercises

A robust drills and exercises program can play an important role in a transit agency's overall security program. Exercises can vary in type, participants, and scope, but in every case can offer transit agencies with valuable information regarding their security and emergency response readiness. In addition, they offer the transit agency an opportunity to coordinate with security partners and other stakeholders. Once the exercise is complete, a well-developed after-action report can offer valuable information that can be used to improve the security and emergency preparedness activities as well as update existing security program documentation and training content.

Action Item 10. Conduct tabletop and functional drills

- a. Conduct tabletop exercises at least every six months to exercise system security programs and emergency operations/response plans
- b. Participate as an active player in full-scale, regional exercises held at least annually
- c. Coordinate with regional security partners, including Federal, State, and local governmental representatives and other affected entities (e.g., other transit agencies or rail systems) to integrate their representatives into exercise programs
- d. Exercise plans and procedures for threat scenarios involving (i) improvised explosive devices (IEDs), (ii) weapons of mass destruction (WMD), and (iii) other high consequence risks identified through the transit agency's system risk assessments
- e. Conduct de-briefings for tabletop and full scale exercises
- f. Develop after-action reports and review results of all tabletop and full scale exercises
- g. Update plans and procedures to incorporate after-action report findings, recommendations, and corrective actions

Related Resource Documents

- *TCRP Report 86, Volume 9, Guidelines for Transportation Emergency Training Exercises*, TRB/TCRP, 2006
- *Homeland Security Exercise and Evaluation Program (HSEEP), Volume 1: HSEEP Overview and Exercise Program Management*, DHS, 2007
- *Transit Incident Drills and Exercises*, APTA-SS-SEM-S-004-9, 2009

Cyber-security

This element includes computer systems, networks, communications equipment, signaling equipment, control systems and dispatching equipment as summarized below:

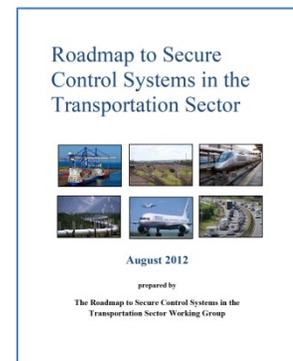
- **Control systems** include train control systems (automatic train control (ATC) and positive train control (PTC)) and supervisory control and data acquisition (SCADA) systems.
- **Communication systems** include radio, closed circuit television (CCTV), intercom, public information displays, and public address systems used to provide transit passengers with information.
- **Security control systems** include CCTV, intrusion detection, video surveillance, alarm, and other monitoring systems designed to provide real-time views of system assets.
- **Data transmission systems** include fiber optic networks, copper networks, leased lines, and wireless network systems that provide the data communications infrastructure between a transit agency's control center and other transit buildings and properties and for local area networks (LANs) and wide area networks (WANs).
- **Fare collection systems** collect transit payments from fare collection devices at each station.
- **Vehicle monitoring systems** are control systems, similar to those for train control, used for automatic vehicle monitoring of buses, streetcars, and other surface systems, including non-revenue equipment.

Action Item 11. Develop a comprehensive cyber-security strategy

- a. Based on risk assessments, designate critical operational control, communications, and information technology (IT) assets
- b. Develop and update written strategies and plans for implementation and update of cyber-security, including cyber incident response
- c. Develop and update cyber-security training for all transit agency staff, including specific training for staff responsible for critical IT assets
- d. Monitor information and intelligence from United States Computer Emergency Readiness Team (US-CERT) and PT-ISAC in regards to cyber-security

Related Resource Documents

- *Roadmap to Secure Control Systems in the Transportation Sector*, DHS, 2012
- *NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments*, NIST, 2012
- *NIST Special Publication 800-64, Revision 2, Security Considerations in the System Development Life Cycle*, NIST, 2008
- *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS) and other control system configurations such as Programmable Logic Controllers (PLC)*, NIST, 2011



- *NIST Special Publication 800-94, Revision 1 (Draft), Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST, 2012
- *NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers*, NIST, 2006
- *Securing Control and Communications Systems in Transit Environments, Part 1: Elements, Organization and Risk Assessment/Management*, APTA-SS-CCS-RP-001-10, 2010
- *Securing Control and Communications Systems in Rail Transit Environments Part 2*, APTA-SS-CCS-RP-002-13, 2013

Facility Security, Access Controls, and Background Investigations

This element addresses traditional facility physical security and includes access control for all transit agency controlled facilities, security critical facilities, background investigations, identification (ID) badges and use with access control, and physical inspections and monitoring of security critical facilities. The content of the background investigations will vary depending on the employee or contractor job requirements and need for access to security critical facilities and documents. As Action Item 14 indicates, care is needed to follow and address local legal rules on background investigations. In addition, procurement of contractor services will need to include the transit agency's requirements for background investigations and sharing of critical information for granting ID badges and access to security critical facilities and documents.

Also included in this element are designing in security (and emergency response/preparedness) and technologies to support surveillance.

Action Item 12. Control access to security critical facilities with identification (ID) badges for all visitors, employees and contractors

- a. Identify security critical facilities and assets
- b. Use ID badges for employee access control
- c. Use ID badges for visitors and contractors
- d. Develop a written policy and procedures for restricting access (e.g., card key, ID badges, keys, safe combinations, etc.) to security critical facilities and assets. Ensure that procedures are updated when new threats, audit findings or circumstances warrant.
- e. Use risk assessment priorities and crime prevention through environmental design (CPTED) criteria for access control and facility security. Implement closed circuit television (CCTV) surveillance and intrusion detection as needed or required.

Action Item 13. Conduct physical security inspections

- a. Conduct, monitor and document facility security inspections (e.g., perimeter/access control) on a regular basis, with increasing frequency in response to changing threat level
- b. Develop and use plans and procedures for vehicle (e.g., buses and rail cars) inspections that correspond to changing threat levels
- c. Develop and use plans and procedures for inspections of rights-of-way corresponding to changing threat levels
- d. Vary the manner in which inspections of facilities, vehicles, and rights-of-way are conducted to avoid setting discernible and exploitable patterns and to integrate unpredictability

Action Item 14. Conduct background investigations of employees and contractors

- a. Conduct background investigations (i.e., criminal history and motor vehicle records) on all new front-line operations and maintenance employees, and employees with access to sensitive security information (SSI) and security critical facilities and systems.

- b. Conduct background investigations on contractors, including vendors, with access to sensitive security information (SSI) and security critical facilities systems.
- c. Ensure that background investigations are consistent with applicable laws
- d. Document the background investigation process, including criteria for background investigations by employee type (e.g., operator, maintenance, safety/security sensitive, contractor, etc.)

Related Resource Documents

- *The Public Transportation System Security and Emergency Preparedness Planning Guide*, FTA, 2003
- *Transit Security Design Considerations*, FTA, 2004
- *Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems*, FTA, 2004
- *Risk Assessment, A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, FEMA 452, 2005
- *National Infrastructure Protection Plan (NIPP)*, DHS, 2013
- *Navigation and Vessel Inspection Circular (NVIC) No. 10-02, Security Guidelines for Vessels*, USCG, 2002
- *Navigation and Vessel Inspection Circular (NVIC) No. 11-02, Recommended Security Guidelines for Facilities*, USCG, 2003
- *TCRP Report 86, Volume 4, Intrusion Detection for Public Transportation Facilities Handbook*, TRB/TCRP, 2003
- *TCRP Report 86, Volume 6, Applicability of Portable Explosive Detection Devices in Transit Environments*, TRB/TCRP, 2004
- *TCRP Report 86, Volume 12, Making Transportation Tunnels Safe and Secure*, TRB/TCRP, 2006
- *NCHRP Report 525, Volume 14, Security 101: A Physical Security Primer for Transportation Agencies*, TRB/NCHRP, 2009
- *NCHRP Report 525, Volume 15, Costing Asset Protection: An All Hazards Guide for Transportation Agencies (CAPTA)*, TRB/NCHRP, 2009
- *Security Lighting for Revenue Transit Facilities*, APTA-SS-SIS-RP-001-10, 2010
- *Security Lighting for Nonrevenue Transit Facilities*, APTA-SS-SIS-RP-002-10, 2010
- *Fencing Systems to Control Access*, APTA-SS-SIS-RP-003-10, 2010
- *Chain Link, Mesh, or Woven Fencing Systems to Control Access*, APTA-SS-SIS-RP-004-10, 2010
- *Gates to Control Access*, APTA-SS-SIS-RP-005-10, 2010
- *Ornamental Fencing Systems to Control Access*, APTA-SS-SIS-RP-006-10, 2010
- *Crime Prevention through Environmental Design (CPTED)*, APTA-SS-SIS-RP-007-10, 2010
- *Safe Mail and Package Handling*, APTA-SS-SEM-RP-008-09, 2009
- *White Paper Operational Strategies for Emergency Smoke Ventilation in Tunnels*, APTA-SS-SEM-WP-013-10, 2010
- *Anti-Vehicle Barriers for Public Transit*, APTA-SS-SIS-RP-009-12, 2012
- *Security Considerations for Public Transit*, APTA-SS-SIS-S-010-13, 2013
- *Security Planning for Public Transit*, APTA-SS-SIS-RP-011-13, 2013

- *Security Operations for Public Transit*, APTA-SS-SIS-RP-012-13, 2013
- *Physical Security for Public Transit*, APTA-SS-SIS-RP-013-13, 2013
- *White Paper on Random Inspections of Carry-on Items in Transit Systems*, APTA-SS-SRM-WP-002-10, 2010
- *Recommended Practice Conducting Nonrevenue Vehicle Security Inspections*, APTA-SS-SRM-RP-003-009, 2009
- *Recommended Practice for Conducting Background Investigations*, APTA-SS-SRM-RP-004-11, 2011
- *Random Counterterrorism Measures on Transit Systems*, APTA-SS-SRM-RP-006-11, 2011
- *Recognizing and Responding to Unattended Packages, Objects and Baggage*, APTA-SS-SRM-RP-007-12, 2012
- *Recommended Practice Identifying Suspicious Behavior in Mass Transit*, APTA-SS-SRM-RP-009-09, 2009
- *Recommended Practice Conducting Revenue Vehicle Security Inspections*, APTA-SS-SRM-RP-012-09, 2009
- *Additional Guidance on Background Checks, Redress and Immigration Status*, TSA, 2006

Document Control

This element addresses the need to determine, designate, mark, and control detailed documents that are related to security critical systems and facilities. Access to these documents may require a need-to-know, which will require a process/procedure for determining and granting that need-to-know. It will be important that there is a process for access to these documents and information for emergency responders. Procurement processes should include the ability to share sensitive information and documents in a manner that maximizes protection of the information while at the same time providing access to appropriate bidders of work to be completed for the transit agency. Federal requirements for protecting sensitive security information (SSI) are defined for DOT and FTA in 49 CFR Part 15 and for DHS and TSA in 49 CFR Part 1520.

Action Item 15. Control access to documents on security critical systems and facilities

- a. Identify and protect documents on security critical systems, such as tunnels, facility heating, ventilation, and air conditioning (HVAC) systems, and surveillance, monitoring, and intrusion detection systems
- b. Limit access to documents on security critical systems to persons with a need to know
- c. Identify a department/person responsible for administering the document control policy
- d. Ensure that the Security Review Committee (or other designated group) has meetings/briefings that include reviewing document control compliance issues

Action Item 16. Process for handling and access to sensitive security information (SSI)

- a. Be familiar with the requirements pertaining to the proper-handling of SSI materials (reference 49 Code of Federal Regulations (CFR) Parts 15 and 1520), such as security plans and risk and vulnerability assessments
- b. Ensure that the Security Review Committee (or other designated group) regularly reviews matters pertaining to access and handling of SSI material

Related Resource Documents

- *Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit Agencies, FTA, 2009*
- *Sensitive Security Information (SSI) Best Practices Guide for non-DHS Employees and Contractors, TSA Brochure, 2012*

Security Program Audits

This element addresses the security program audits by internal transit agency staff or outside auditors. These audits are focused on testing the security program documentation and comparing to actual practice to assure that the documentation and practice match. In addition, these audits are an opportunity to consider additional security program capabilities based on recent experience at the transit agency, from other agencies, or in the region of operation and the transit industry. For transit agencies with their own police department, these security program audits may be separate or in conjunction with audits required for accreditation.

Action Item 17. Establish and conduct security program audits

- a. Conduct security program audits at least annually
- b. Ensure that the Security Review Committee (or other designated group) addresses the findings and recommendations from audits, and updates plans and procedures as necessary

Related Resource Documents

- *The Public Transportation System Security and Emergency Preparedness Planning Guide*, FTA, 2003
- *Bus Safety and Security Program, Safety, Security, and Emergency Preparedness Excellence – A Roadmap*, FTA, 2012
- *Transit Security Design Considerations*, FTA, 2004
- *Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)*, APTA-SS-SRM-RP-001-09, Rev. 1, 2012
- *Security Planning for Public Transit*, APTA-SS-SIS-RP-011-13, 2013
- *Security Considerations for Public Transit*, APTA-SS-SIS-S-010-13, 2013
- *Random Counterterrorism Measures on Transit Systems*, APTA-SS-SRM-RP-006-11, 2011