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

Management and Accountability

1. Establish Written System Security Programs and Emergency Management Plans:

a. Ensure that Security and Emergency Management Plan(s) is/are signed/approved by senior level management

b. Review plans at least annually and update as circumstances warrant

c. Ensure the Security and Emergency Management Plan(s) 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 protocols that address specific threats from (i) Improvised Explosive Devices (IED), (ii) Weapons of Mass Destruction, and (iii) other high consequence risks identified in transit risk assessments

f. Apply security design and crime prevention criteria through environmental design (CPTED) for major capital construction projects, system modifications, and procurements

g. Ensure the Security and Emergency Management Plan(s) address(es) Continuity of Operations

h. Ensure the Security and Emergency Management Plan(s) address(es) Business Recovery

2. Define roles and responsibilities for security and emergency management.

a. Assign Security and Emergency Management Programs to (a) Senior Level Manager(s)

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 management plan(s) is/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 protocols are substantially updated

i. Establish lines of delegated authority/succession of security responsibilities and inform personnel

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 program audit findings, and makes recommendations to senior level management for changes to plans and processes

4. Coordinate Security and Emergency Management Plan(s) with local and regional agencies

a. Coordinate with Federal and State governmental entities associated with public transportation security (example: STSI Area Office, State

Office of Homeland Security, FTA Regional Office, 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 Plan (NRP)

c. Establish Memorandums of Agreement or Mutual Aid Agreements with local government, fire, police and other entities with shared infrastructure (example: other transit agencies or rail systems)

d. Maintain communications interoperability with first responders with security responsibilities in the transit system's regional area

Security and Emergency Response Training

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 Homeland Security Advisory System (HSAS) threat advisory levels, to:

- Field Supervisors
- Controllers/Dispatchers
- Fare Inspectors
- Law Enforcement personnel
- Operators
- Maintenance personnel
  - Field personnel
  - Vehicle personnel

c. Provide ongoing advanced security training programs for transit managers, including but not limited to CEOs, General Managers,

Operations Managers, and Security Coordinators (includes Security Directors and Transit Police Chiefs)

d. Regularly update security awareness, emergency response, and counterrorism training materials to address (i) Improvised Explosive Devices, (ii) Weapons of Mass Destruction 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 management plans and procedures

Homeland Security Advisory System (HSAS)

6. Establish plans and protocols to respond to the DHS Homeland Security Advisory System (HSAS) threat levels

a. Security and emergency management plans and procedures should identify incremental actions to be implemented at each HSAS threat level

b. Exercises should test implementation of the preventive measures for each HSAS threat level, including random application of security measures

Public Awareness

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 (security messages and evacuation procedures)

   - In stations (electronic message boards, voice)

   - 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 the HSAS threat advisory level is raised

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

Drills and Exercises

8. Conduct Tabletop and Functional drills

a. Conduct tabletop exercises at least every six months to exercise system security programs and emergency management 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 (example: 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, protocols and processes to incorporate after-action report findings, recommendations, and corrective actions

Establish a Risk Management and Information Sharing Process

9. Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences (Note: **Risk management** includes mitigation measures selected after **risk assessment** has been completed)

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 (example: other transit agencies or rail systems), to leverage resources and experience for conducting risk assessments (example: leverage resources such as the Security Analysis and Action Program operated by TSA's Surface Transportation Security Inspectors)

10. Participate in an information sharing process for threat and intelligence information

a. Participate in information sharing networks or arrangements with:

- State and local law enforcement and homeland security officials
- ~~o~~ DHS' 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)
- FBI Joint Terrorism Task Force (JTTF) and/or other regional anti-terrorism task force (e.g. Terrorism Early Warning Group (TEW), US Attorney's Office)
- TSA Surface Transportation Security Inspectors (STSI)
- Public Transportation Information Sharing and Analysis Center (PT-ISAC)

11. Establish and Use a Reporting Process for Suspicious Activity (internal and external)

a. Through training and awareness programs, ensure transit agency employees understand the what, how, and when to report observed suspicious activity or items

b. Use exercises to test employee awareness and the effectiveness of reporting and response procedures

c. Ensure public awareness materials and announcements provide clear direction to the public on reporting of suspicious activity

~~d.~~ Maintain protocols 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)

e. Maintain protocols that ensure actionable security events are included in reports to the FTA's National Transit Database (NTD)

Facility Security and Access Controls

12. Control Access to Security Critical Facilities with 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 policy is updated when new threats, audit findings or circumstances warrant.

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 elevation of the HSAS threat advisory level

b. Develop and use protocols for vehicle (e.g. buses and rail cars) inspections that correspond to HSAS threat advisory levels

c. Develop and use protocols for inspections of rights-of-way corresponding to HSAS threat advisory 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

Background Investigations

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 and security critical facilities and systems.

b. Conduct background investigations on contractors, including vendors, with access to sensitive security information and security critical facilities and 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 (operator, maintenance, safety/security sensitive, contractor, etc.)

Document Control

15. Control access to documents of security critical systems and facilities

a. Identify and protect documents on security critical systems, such as tunnels, facility 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

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 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 the access to and handling of SSI material

Security Program Audits

17. Audit Program

a. Conduct security program audits at least annually

- o Internal
- o External

b. Ensure that the Security Review Committee (or other designated group) addresses the findings and recommendations from audits, and updates plans, protocols and processes as necessary. (see 3c)

Footnotes:

(1) These action items covers all modes directly operated or contracted by the transit agency (e.g., bus, bus rapid transit, light rail, heavy rail, commuter rail, paratransit etc.)

(2) For additional information please reference:

FTA Safety & Security website: **http://transit-safety.volpe.dot.gov**

(3) Contact **MTActionItems@dhs.gov** for Questions or Comments

December, 2006