

# 19. SAFETY AND SECURITY

## **BASIC REQUIREMENT**

Any recipient of Urbanized Area Formula Grant Program funds must annually certify that it is spending at least one percent of such funds for transit security projects or that such expenditures for security systems are not necessary.

Under the safety authority provisions of the Federal transit laws, the Secretary has the authority to investigate the operations of the grantee for any conditions that appear to create a serious hazard of death or injury, especially to patrons of the transit service. States are required to oversee the safety of rail fixed guideway systems through a designated oversight agency, per [49 CFR Part 659](#), Rail Fixed Guideway Systems, State Safety Oversight.

Under security, a list of [17 Security and Emergency Management Action Items](#) has been developed by FTA and the Department of Homeland Security's Transportation Security Administration (TSA). This list of 17 items, an update to the original FTA Top 20 security action items list, was developed in consultation with the public transportation industry through the Mass Transit Sector Coordinating Council, for which the American Public Transportation Association (APTA) serves as Executive Chair. Security and Emergency Management Action Items for Transit Agencies aim to elevate security readiness throughout the public transportation industry by establishing baseline measures that transit agencies should employ.

The goal of FTA's Safety and Security Program is to achieve the highest practical level of safety and security in all modes of transit. To this end, FTA continuously promotes the awareness of safety and security throughout the transit community by establishing programs to collect and disseminate information on safety/security concepts and practices. In addition, FTA develops guidelines that transit systems can apply in the design of their procedures and by which to compare local actions. As such, many of the questions in this review area are designed to determine what efforts grantees have made to develop and implement safety, security, and emergency management plans. While there may not be specific requirements associated with all of the

questions, grantees are encouraged to implement the plans, procedures, and programs referenced in these questions. For this reason, findings in this area will most often result in advisory comments rather than deficiencies.

## **AREAS TO BE EXAMINED**

### **1. Safety**

- a. Policy and Management
- b. Administration and Procedures
- c. Personnel and Training
- d. Safety Reporting
- e. Safety Training

### **2. Security and Emergency Management**

- a. Security Expenditures
- b. Management and Accountability
- c. Security and Emergency Response Training
- d. Homeland Security Advisory System (HSAS)
- e. Public Awareness
- f. Drills and Exercises
- g. Risk Management and Information Sharing
- h. Facility Security and Access Control
- i. Background Investigations
- j. Document Control
- k. Security Audits

## **REFERENCES**

1. [49 USC Chapter 53](#), Federal Transit Act, Section 5307(d)(1), Security Expenditures.
2. [49 CFR Part 630](#), "Uniform System of Accounts and Records and Reporting."
3. [49 CFR Part 659](#), "Rail Fixed Guideway Systems, State Safety Oversight."
4. [TSA/FTA 17 Security and Emergency Management Action Items for Transit Agencies](#).

# QUESTIONS FOR THE REVIEW

## Part A. Safety

1. *Does the grantee have a written policy on safety? Has it been signed by the CEO?*
2. *Does the grantee have a written system safety program plan (SSPP) for its transit services? Does the SSPP address management of the safety function?*
3. *How is the safety function managed? Are there staff safety personnel? If so, are responsibilities and authorities clear? To whom do they report?*

### EXPLANATION

FTA is concerned about the safety of both transit passengers and transit workers. FTA can conduct safety investigations when conditions of any facility, equipment, or manner of operation appear to create a serious hazard of death or injury.

Recognizing that safety is an integral part of transit operations, grantees are encouraged to have a written safety policy and safety plan. The safety plan should assign responsibilities for safety management from the most senior executive to the first-line supervisory level. Endorsement by the CEO conveys this importance. At a minimum, a grantee's safety plan should address compliance with applicable legal requirements. Striving for continual improvement to achieve a high level of safety performance should be a program goal. Guidance on the development of a written bus transit system safety program plan is available in an APTA publication entitled, *Manual for the Development of Bus Transit System Safety Program Plans* (1998). Note that the grantee may have a safety plan developed from another source, which responds to specific state or local requirements.

These questions are intended to provide an overall understanding of how safety is incorporated into the organization, what kind of emphasis is placed on safety, how the safety program is managed, and how various responsibilities are communicated to personnel at all levels.

### REASON FOR THE QUESTION

Suggested practice

### SOURCES OF INFORMATION

If the grantee has a written safety policy or system safety program plan, it should be examined at the site visit. Reviewers should discuss with the grantee the reporting relationships in regard to safety to ensure that the safety function is managed adequately.

### DETERMINATION

If the grantee has a safety policy and safety plan signed by the CEO, no advisory comment is made. If the grantee does not have a safety policy or safety plan, an advisory comment is made. If the safety plan does not address the management of the safety function, if staff responsibilities are not clearly delineated, or the CEO has not signed it, an advisory comment is made.

### SUGGESTED CORRECTIVE ACTION

If the grantee does not have a written safety policy or system safety program plan, the grantee is encouraged to prepare a plan. If the safety plan does not adequately address management of the safety function, the grantee should revise the plan to correct any deficiencies.

4. *What are the investigation procedures for major incidents? What circumstances and conditions determine which incidents will be investigated? Who does the investigation? To whom do reports go? What follow-up action is taken and by whom?*
5. *What key safety issues have been identified and how are they being addressed?*
6. *Is there a process for hazard identification and resolution? When corrective action is needed, how is it initiated and followed up?*

### EXPLANATION

Safety issues include more than vehicle and passenger accidents and workplace injuries. As such, the grantee's safety-related responsibilities may be numerous. They may include, for example:

- investigating major incidents
- identifying workplace hazards
- proper handling of hazardous materials
- emergency preparedness.

Reviewers should ensure that the grantee has established procedures to investigate, identify, and address safety issues. The process should be both reactive in terms of investigating incidents and proactive in terms of identifying and responding to key safety issues and potential hazardous conditions.

### REASON FOR THE QUESTION

Suggested practice

### SOURCES OF INFORMATION

The minutes from safety committee and/or accident/incident review committee meetings should be made available during the site visit. Emergency management plans and procedures should be requested. The grantee should be able to provide safety statistics for the past three years for major incidents involving passengers, property damage, and work-related accidents. At the site visit or the desk review, newspaper articles or other publications describing accidents or safety incidents may be found. This does not necessarily indicate poor safety practices; however, the incident should be discussed at the site visit. Insurance companies also conduct assessments of their clients. Such reports are another source of information. Claims records and insurance costs identified in financial reports also provide information. Both costs and the actual number of incidents should be examined.

Procedures manuals and employee handbooks may contain information related to safety. Copies of these documents should be examined on site to determine if safety procedures are addressed for various functions (e.g., transportation, maintenance, procurement, and stores). Determine who is responsible for maintaining safety information, handbooks, procedures manuals, and materials safety data sheets (MSDS).

### DETERMINATION

If the grantee has procedures to investigate incidents and accidents, no advisory comment is made. If incident and accident investigation procedures appear to be lacking, an advisory comment is made. If the grantee has procedures in place to identify and resolve workplace hazards, no advisory comment is made. If hazard identification and resolution procedures are lacking, an advisory comment is made.

### SUGGESTED CORRECTIVE ACTION

If procedures for investigating incidents appear to be lacking, the grantee is encouraged to develop and implement adequate procedures. If procedures for dealing with workplace hazards, safe materials

handling, etc. appear to be lacking, the grantee is encouraged to establish appropriate procedures.

7. *Does management hold line personnel accountable for safety? Do line personnel job descriptions (senior level to first-line supervisors) include a provision for safety accountability? Are safety responsibilities clearly defined? Do annual evaluations include an appraisal of safety performance?*

8. *Is there safety training for employees performing safety sensitive functions? Who performs the training? How is it done? Do supervisors receive formal safety training? If so, please describe.*

### EXPLANATION

Grantees are encouraged to clearly define the safety responsibilities for all employees and establish a comprehensive safety training program. By providing training to the appropriate personnel, grantees can enhance safety performance in all areas (e.g., accidents, workplace hazards, and emergency preparedness). Training may consist of initial training to new hires as well as recurrent training to all employees. Additional training may be provided on a case-by-case basis, if employees have a high number of incidents in a particular area of concern.

### REASON FOR THE QUESTION

Suggested practice

### SOURCES OF INFORMATION

Ask the grantee to provide an overview of its training program for drivers, mechanics, supervisors, and other line personnel. Job descriptions and requirements for safety sensitive positions and supervisory personnel should be discussed with the grantee. The grantee should provide training records of its employees (line personnel and supervisors) to be examined on site. Additionally, training manuals, safety handouts, safety postings and other materials should be made available.

### DETERMINATION

If the grantee has clearly defined safety responsibilities for safety-sensitive and supervisory personnel and provided adequate training, no advisory comment is made. If safety responsibilities have not been clearly defined, an advisory comment is made. If safety-sensitive and supervisory personnel have not received adequate safety training, an advisory comment is made.

### **SUGGESTED CORRECTIVE ACTION**

If the grantee has not clearly defined safety responsibilities, it should do so. If the grantee does not have an adequate safety training program, the grantee is encouraged to develop one.

### **9. *Has the grantee submitted transit safety data in NTD for the past year in a timely manner?***

#### **EXPLANATION**

All transit agencies, regardless of the number of vehicles operated, are required to provide information by mode and type of service in the Safety & Security Module of NTD on a monthly basis. If a grantee operates nine or fewer vehicles and has been granted a waiver, it is exempt from the safety and security reporting requirements.

The NTD Safety & Security Module has three components: Major Incident Reporting, Non-Major Incident Safety, and Non-Major Incident Security reporting. Grantees are required to submit information for each component and for all modes except commuter rail. Agencies that operate commuter rail service do not have to report Major Safety Incident and Non-Major Incident Safety data to FTA since these data are available from FRA. However, agencies operating commuter rail service must complete the NTD Major Security Incident and Non-Major Incident Security reports. Major Incident forms are due thirty days after the major incident occurred.

A Major Incident is defined as an event involving a transit vehicle or transit-controlled property, involving one or more of the following:

- A fatality
- Injuries requiring immediate medical attention away from the scene for two or more persons
- Property damage equal to or exceeding \$25,000
- An evacuation due to life safety reasons
- A collision at a grade crossing
- A main-line derailment
- A collision with person(s) on a rail right of way resulting in injuries that require immediate medical attention away from the scene for one or more persons
- A collision between a rail transit vehicle and another rail transit vehicle or a transit non-revenue vehicle resulting in injuries that require immediate medical attention away from the scene for one or more persons.
- Forcible rape
- Confirmed terrorist/security events
  - Bombings
  - Chemical/biological/radiological/other release

- Cyber incident
- Hijacking
- Sabotage

Non-Major Incident Safety data include any incident not reported as a Major Incident and meeting one or more of the following criteria:

- Injuries requiring immediate medical attention away from the scene for one person
- Property damage equal to or exceeding \$7,500, but less than \$25,000
- All non-arson fires not qualifying as a Major Incident.

#### **REASON FOR THE QUESTION**

49 CFR 630

#### **SOURCES OF INFORMATION**

Ask the grantee to provide a summary of its Major Incidents for the past year. Verify that this information is being reported into NTD as required.

Examine three months of Non-Major Incident (Safety) data and ensure that the grantee is reporting information as required.

#### **DETERMINATION**

If the grantee has submitted the safety data for the past year, the grantee is not deficient. If the grantee has not submitted Major Incident data for the past year or is not submitting information for the current year, the grantee is deficient in the NTD requirements. If the grantee has not submitted Non-Major Incident Safety data, the grantee is deficient in the NTD requirements. [Note: If these findings are made, they are to be discussed in the NTD area of the report.]

#### **SUGGESTED CORRECTIVE ACTION**

The grantee needs to submit information in the NTD as required.

### **Part B. Security and Emergency Management**

### **10. *Does the grantee utilize the one percent expenditure of its Urbanized Area Formula Grant funds for transit security?***

- a) *If yes, how did the grantee utilize the one percent expenditure over the last three years?*

b) *If no, why does the grantee consider that existing security measures meet agency needs?*

*Provide project and expenditure information for the last three years in Exhibit 19.1.*

#### **EXPLANATION**

The grantee is required to certify that it is spending at least one percent of the Urbanized Area Formula Grant (UAFG) Program funds it receives annually for transit security projects or that such expenditures are not necessary. This certification is part of the annual certifications and assurances.

For grantees that spend the one percent, examples of appropriate security expenditures include facility perimeter security and access control systems (e.g., fencing, lighting, gates, card reader systems, etc.), closed circuit television camera systems (at stations, platforms, bus stops and on-board vehicles), security and emergency management planning, training and drills (SAFETEA-LU expanded the definition of security related capital projects to include planning, training and drills, such that these expenditures are now eligible expenses for grantees in UZAs over 200,000 population to apply towards the 1% for security requirement.) and any other project intended to increase the security and emergency management of an existing or planned transit system. Grantees should provide detail on how these funds were spent during the review period.

There are three reasons that grantees may have for considering the one percent security expenditure to be unnecessary: (1) No deficiencies identified from conducting a recent threat and vulnerability assessment; (2) TSA/FTA Security and Emergency Management Action Items met or exceeded; or (3) Other. For the Other category, the primary basis is that a grantee spends sufficient local funds on security projects and therefore does not need to spend formula grant funds on security projects. Regardless of their reasons for deciding not to spend FTA formula funds on transit-related security, grantees should provide information and documentation that supports this decision.

#### **REASON FOR THE QUESTION**

[49 USC 5302\(a\)\(1\) and 5307\(d\)\(1\)\(J\)](#)

#### **SOURCES OF INFORMATION**

These questions should be asked at the site visit. If a grantee is spending at least one percent of its formula funds on security projects, the grantee should be asked to provide the detail of these expenditures for each year of the review period in the requested format

as well as documentation that supports these expenditures.

If the grantee has decided that it is not necessary to expend one percent of its UAFG funds, the grantee should provide a written explanation and any information that supports this decision. Such information may include the recommendations/findings from (1) a threat and vulnerability assessment and (2) a TSA/FTA Security and Emergency Management Action Items assessment. If the grantee indicates that it spends local funds on security, the grantee should provide expense detail in the requested format as well as documentation that supports these expenditures.

#### **DETERMINATION**

If the grantee has been spending at least one percent of its Urbanized Area Formula Grant Program funds on transit security projects, the grantee is not deficient. If the grantee has decided that the expenditure is not necessary and can provide an explanation and adequate documentation, the grantee is not deficient. If the grantee decides that expenditures for security are necessary but cannot document the expenditures, the grantee is deficient. If a grantee decides that expenditures for security are necessary but expenditures fall short of the one percent requirement, the grantee is deficient. If the grantee cannot provide adequate documentation of its security expenditures using formula funds, the grantee is deficient. If the grantee decides that expenditures for security are not necessary but cannot explain or provide adequate documentation to support its decision, the grantee is deficient.

#### **SUGGESTED CORRECTIVE ACTION**

The grantee should provide a plan for meeting the one percent expenditure requirement and report on implementation of this plan to FTA. The grantee should provide a plan for documenting the amount of formula funds spent on transit security. The grantee should provide an explanation and adequate documentation on why the expenditure is not necessary.



## **Management and Accountability**

11. *Does the grantee have written security and emergency management plans for all modes of operation?*
12. *Do the security and emergency management plans define roles and responsibilities for transit personnel?*
13. *Do the security and emergency management plans ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control?*

### **EXPLANATION**

FTA has specific requirements for a written system security plan for rail fixed guideway systems (RFGS). FTA encourages all transit systems, particularly those in areas with populations of 200,000 or more, to develop and implement a transit system security program plan and emergency management plans that cover passengers, employees, vehicles, and facilities, including the planning, design, and construction of new facilities. Guidance on the development and implementation of system security program plans is available in a report entitled, [The Public Transportation System Security and Emergency Preparedness Planning Guide](#) (DOT-VNTSC-FTA-03-01), dated January 2003.

Grantees should ensure that security and emergency management plans are endorsed by senior level management in order that they are communicated throughout the agency from the highest level. Plans should be reviewed annually and updated as circumstances warrant. Plans should integrate visibility, randomness, and unpredictability into security deployment activities in order to avoid exploitable patterns and to enhance deterrent effects. Plans should also address Continuity of Operations and Business Recovery in the event that normal operations need to be suspended or altered as the result of a catastrophic incident. In addition, plans and protocols should address specific threats from Improvised Explosive Devices (IED), Weapons of Mass Destruction (WMD), and other high consequence risks identified in transit risk assessments. Grantees should also establish and maintain standard security and emergency operations procedures (SOPs/EOPs) for each mode operated, including procedures for operations control centers.

In situations where grantees are planning the construction or modification of systems and facilities, security design and crime prevention criteria through environmental design (CPTED) should be applied to ensure a secure environment for the riding public and employees.

The security and emergency management programs should be assigned to the senior level managers in the grantee's organization. The names and titles of the Primary and Alternate Security Coordinator (including Security Directors and Transit Police Chiefs) should be recorded and maintained on file. The telephone numbers, e-mail addresses and other contact information for these individuals should be accurately maintained so that they are accessible at all times. The Security Coordinators also should report to the senior level management of the organization. Security duties should be defined and properly delegated to front line employees. The grantee should distribute the security and emergency management plans to appropriate personnel. Regular security coordination meetings involving all personnel assigned security responsibilities should be held. Informational briefings with appropriate personnel also should be held whenever security protocols are substantially updated. In order to ensure continuity of the plans, the grantee should establish lines of delegated authority and/or succession of security responsibilities and inform the affected personnel.

The grantee should hold regular supervisor and foreperson security review and coordination briefings for operations and maintenance personnel. An internal security incident reporting system should be developed and maintained and a Security Review Committee should be established in order to regularly review security incident reports, trends, and program audit findings, and make recommendations to senior level management for changes to plans and processes.

***Note: Due to the Sensitive Security Information (SSI) designation of grantees' security and emergency management plan, they must be examined on-site. Reviewers must not remove security and emergency management plans from the grantee's premises or request them in advance of the review.***

### **REASON FOR THE QUESTION**

[49 CFR 659.31](#)

[TSA/FTA Action Item No. 1](#)

[TSA/FTA Action Item No. 2](#)

[TSA/FTA Action Item No. 3](#)

### **SOURCES OF INFORMATION**

If the grantee has written security and emergency management plans, these should be examined at the site visit. At the site visit or the desk review, newspaper articles or other publications describing

security incidents may be found. Such articles may highlight an incident. Though this does not necessarily indicate poor security practices, the incident should be discussed at the site visit.

The security and emergency management plans may not be stand-alone documents, but may be chapters or sections of a more comprehensive safety/security plan, such as a System Safety Program Plan for a Rail Fixed Guideway System. The plan should cover all modes the contractor operates, including contracted services.

#### **DETERMINATION**

If the grantee has a security plan for all modes, no advisory comment is made. If a grantee does not have a security plan for all modes, an advisory comment is made. If a grantee has a security plan for each mode, but it does not include personnel roles and responsibilities, protocols to address specific threats, a Continuity of Operations, a Business Recovery Plan, or other elements described in the Explanation, an advisory comment is made. . If the plans do not have an endorsement from the top official, an advisory comment is made. If responsibilities have not been clearly defined, an advisory comment is made.

If the grantee has an emergency management plan, no advisory comment is made. If the grantee does not have an emergency management plan or if the plan does not cover all modes, an advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

If the grantee does not have a written security and emergency management plan for all modes, the grantee is encouraged to prepare and implement one. If the grantee has a plan, but it does not include the specific elements described above, the grantee is encouraged to update its plan according to the TSA/FTA guidelines.

#### **14. *Are the security and emergency management plans coordinated with local agencies?***

##### **EXPLANATION**

A grantee's security and emergency management plans should be an integrated system program and be coordinated with local first responders. Coordination should include mutual aid agreements with these agencies and should address communications interoperability with first responders (e.g., police and fire departments) in the grantee's service area. Grantees also should coordinate with federal and state entities associated with public transportation security such as the TSA's Surface Transportation Security Inspection Program (STSIP) area office, the

FBI's Joint Terrorism Task Force (JTTF), the State Homeland Security Office, and FTA Regional Office. Coordinated plans should be consistent with the [National Incident Management System](#), (NIMS) and the [National Response Framework](#) (NRF). NIMS provides a unified approach to incident management including standard command and management structures and an emphasis on preparedness, mutual aid and resource management. The NRP forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents.

#### **REASON FOR THE QUESTION**

[TSA/FTA Action Item No. 4](#)

#### **SOURCES OF INFORMATION**

Ask the grantee to provide copies of security plans and procedures. Also, ask the grantee to provide copies of any inter-agency agreements that outline a coordinated emergency response. If no formal agreements exist, ask if the grantee has met with representatives of other agencies to discuss and/or plan emergency response coordination. Ask the grantee whether its plans are consistent with NIMS and the NRP.

#### **DETERMINATION**

If the grantee has coordinated with other agencies at the local, state and federal levels, no advisory comment is made. If the grantee has not coordinated with other agencies, an advisory comment is made. If the grantee is a party to an agreement that outlines emergency response coordination, no advisory comment is made. If no agreement exists, but the grantee has taken steps to establish coordinated emergency response procedures with other agencies, no advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

If the grantee has not coordinated with other local, state and federal agencies, it is encouraged to do so. The grantee should establish contacts with other agencies and begin developing coordinated emergency response procedures.

#### ***Security and Emergency Response Training***

#### **15. *Has the grantee established a security and emergency training program?***

##### **EXPLANATION**

The grantee should provide ongoing basic training to all employees in security orientation and awareness and emergency response. Ongoing training should be provided to employees that have direct security

responsibilities such as operating, maintenance, law enforcement and fare inspection. Ongoing training should include advanced security and emergency response training by job function and actions required at incremental Homeland Security Advisory System (HSAS) threat advisory levels. Security training programs should emphasize integration of visible deterrence, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and heighten deterrent effect.

Advanced security training programs also should be established for transit managers, including but not limited to CEOs, General Managers, Operations Managers, and Security Coordinators (includes Security Directors and Transit Police Chiefs). The materials should be updated regularly to address high consequence risks that have been identified by the grantee's risk assessments. Training should reinforce roles and responsibilities and should ensure that employees are proficient in their duties at all times.

The grantee should establish a system that records personnel training in security and emergency response that, at a minimum, documents employee's initial training, and any recurrent training (e.g., periodic and/or refresher). Grantees should also establish and maintain a security notification process to inform personnel of significant updates to security and emergency management plans and procedures, as necessary.

#### **REASON FOR THE QUESTION**

[TSA/FTA Action Item No. 5](#)

#### **SOURCES OF INFORMATION**

Procedure manuals, employee handbooks, and training materials may provide information on the grantee's efforts to train employees in security and emergency response. Ask the grantee if security training seminars or workshops have been conducted for all employees.

Ask the grantee if records are kept concerning security and emergency training and if so, review a sample to verify the grantee's recordkeeping system. Ask whether or not the grantee has a notification process to inform employees of significant updates to plans and procedures.

#### **DETERMINATION**

If the grantee has provided training to operating and non-operating personnel, no advisory comment is made. If training has not been provided to operating personnel, an advisory comment is made. If training has not been provided to non-operating personnel, an advisory comment is made. If the grantee maintains records of security training, no advisory comment is made. If the grantee does not maintain training records, an advisory comment is made. If the grantee has a process to notify employees of significant

updates to security plans and procedures, no advisory comment is made. If the grantee does not have such a process, then an advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

The grantee should implement a security and emergency response training program for operating and/or non-operating personnel and maintain records of employee training. If necessary, the grantee should establish and maintain a notification process to inform employees of updates to security and emergency plans and procedures.

### ***Homeland Security Advisory System (HSAS)***

- 16. Have protocols been established to respond to the Department of Homeland Security Advisory System Threat Levels?*

#### **EXPLANATION**

FTA recommends that all grantees have an updated security plan that addresses terrorism as well as procedures to respond incrementally to the HSAS threat levels issued by the Department of Homeland Security.

#### **REASON FOR THE QUESTION**

[TSA/FTA Action Item No. 6](#)

#### **SOURCES OF INFORMATION**

The grantee's security plan and/or procedures should be examined to ensure that there are protocols for responding to the Department of Homeland Security's threat advisory levels.

#### **DETERMINATION**

If the grantee has protocols for responding to threat advisory levels, no advisory comment is made. If the grantee does not have protocols for responding to threat advisory levels, an advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

The grantee is encouraged to develop protocols to respond to Department of Homeland Security threat advisory levels.

### ***Public Awareness***

- 17. Have public awareness materials been developed and distributed on a system-wide basis?*

## EXPLANATION

The grantee should disseminate information to the riding public on identifying and reporting suspicious or illegal activity. Public service announcements, billboards, and brochures are effective mechanisms to provide security information to passengers. Grantees also should consider implementing FTA's Transit Watch program at their agency.

## REASON FOR THE QUESTION

[TSA/FTA Action Item No. 7](#)

## SOURCES OF INFORMATION

Ask the grantee to provide any information related to security that has been disseminated to passengers.

## DETERMINATION

If passengers have received information on recognizing and reporting suspicious or illegal activity, the grantee is not deficient. If security information has not been provided to passengers, an advisory comment is made.

## SUGGESTED CORRECTIVE ACTION

If information on recognizing and reporting suspicious or illegal activity has not been provided to the riding public, the grantee is encouraged to do so.

## Drills and Exercises

18. *Are tabletop and functional drills conducted at least once every six months, and are full-scale exercises, coordinated with regional emergency response providers, performed at least annually?*

## EXPLANATION

It is good practice for grantees to conduct tabletop exercises on a semi-annual basis and full scale exercises on an annual basis. Such drills and exercises should be coordinated 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. Recommended exercise plans and procedures include threat scenarios involving improvised explosive devices (IEDs), weapons of mass destruction (WMD), and other high consequence risks identified through the grantee's risk assessments. Following each exercise and drill, the grantee should conduct and/or participate in de-briefings to examine the results of the exercise and/or drill and develop after-action reports to address any updates to plans and procedures that might be warranted.

## REASON FOR THE QUESTION

[TSA/FTA Action Item No. 8](#)

## SOURCES OF INFORMATION

Ask the grantee what drills and/or exercises have been conducted. Ask the grantee to provide a list of the drills and exercises showing the dates that they were conducted and the other agencies that participated. Review any after-action reports and determine if plans and/or procedures were updated accordingly.

## DETERMINATION

If the grantee has conducted drills and/or exercises of potential emergency events, no advisory comment is made. If the grantee has not conducted such drills and/or exercises, an advisory comment is made.

## Risk Management and Information Sharing

19. *Has the grantee established a risk management process to assess and manage threats, vulnerabilities and consequences? Did the process identify mitigation measures after the risk assessment had been completed?*

## EXPLANATION

Grantees are encouraged to establish a risk management process that is based on a system-wide assessment of risks and obtain management approval of this process. As part of the process, grantees should ensure proper training of management and staff responsible for managing the risk assessments. Whenever a new asset/facility is added or modified, and when conditions warrant (e.g. changes in threats or intelligence), the risk assessment process should be updated. The risk assessment process should be used to prioritize security investments.

As with the overall security and emergency management plans, the risk assessment process should be coordinated with regional security partners, including federal, state, and local governments as well as agencies with shared infrastructure (e.g., other transit agencies or rail systems). Coordination will assist grantees to leverage resources and experience for conducting risk assessments.

## REASON FOR THE QUESTION

[TSA/FTA Action Item No. 9](#)

## SOURCES OF INFORMATION

Ask the grantee if it has established a risk assessment process. Ask the grantee to provide

documentation (e.g., risk assessments and mitigation measures) that demonstrates such a process has been established.

#### **DETERMINATION**

If the grantee has established a risk management process, no advisory comment is made. If the grantee has not established a risk management process, an advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

The grantee should establish a risk management process and conduct risk assessments according to the established process.

**20.** *Does the grantee participate in information sharing networks such as the FBI's Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force and/or the Public Transportation Intelligence Sharing & Analysis Center (PT-ISAC)?*

#### **EXPLANATION**

Grantees are encouraged to participate in intelligence sharing networks such as the FBI's JTTF (if they have their own law enforcement personnel) or PT-ISAC in order to facilitate coordination on regional security matters throughout the area and share intelligence with law enforcement and other agencies. The PT-ISAC is a clearinghouse of security threats, vulnerabilities and solutions for the public transit industry. Members report and receive information through the PT-ISAC to assist them and other members in preparing for and responding to threats. APTA is the coordinator for the PT-ISAC. Other intelligence sharing networks include the DHS Homeland Security Information Network (HSIN) and the TSA's Surface Transportation Security Inspectors (STSI).

#### **REASON FOR THE QUESTION**

[TSA/FTA Action Item No. 10](#)

#### **SOURCES OF INFORMATION**

Ask the grantee if it participates in an information sharing network such as the JTTF, PT-ISAC, or other agency to share intelligence on potential threats.

#### **DETERMINATION**

If the grantee participates in an information sharing network for the purpose of sharing intelligence on potential threats, no advisory comment is made. If the grantee does not participate in an information sharing network, an advisory comment is made.

#### **SUGGESTED CORRECTIVE ACTION**

If the grantee is not participating in a regional task force, the grantee should join the JTTF, ST-ISAC or other regional task force in order to share intelligence on potential threats.

**21.** *Does the grantee have a process to ensure that security threats, concerns and incidents are reported appropriately? Is security information reported through the National Transit Database (NTD)?*

#### **EXPLANATION**

All grantees, regardless of the size of their urbanized areas, are required to report security data as part of their National Transit Database (NTD) report. Transit agencies are required to provide information by mode and type of service in the Safety & Security Module of NTD on a monthly basis. If a grantee operates nine or fewer vehicles and has been granted a waiver, it is exempt from the safety and security reporting requirements.

The NTD Safety & Security Module has three components: Major Incident Reporting, Non-Major Incident Safety, and Non-Major Incident Security reporting. Grantees are required to submit information for each component and for all modes except commuter rail. Agencies that operate commuter rail service do not have to report Major Safety Incident and Summary Safety data to FTA since these data are available from FRA. However, agencies operating commuter rail service must complete the NTD Major Security Incident and Non-Major Incident Security reports. Major Incident forms are due thirty days after the major incident occurred.

Non-Major Incident Security data include any incident not reported as a Major Incident and meeting one or more of the following criteria:

Occurrence of Part I Offenses (except homicide):

- Robbery
- Aggravated assault
- Burglary
- Larceny/theft
- Motor vehicle theft
- Arson

Arrest/Citation for Part II Offenses:

- Other assaults
- Vandalism
- Trespassing
- Fare evasion

Occurrence of Other Security Issues:

- Bomb threat

- Non-violent civil disturbance

Occurrence of Suicides and Attempts

### REASON FOR THE QUESTION

[49 CFR 630](#)  
[TSA/FTA Action Item No. 11](#)

### SOURCES OF INFORMATION

Ask the grantee to provide a summary of its Major Incidents for the past year. Verify that this information is being reported to NTD as required (see Question 9). Examine three months of Non-Major Incident Security data and ensure that the grantee is reporting information as required.

### DETERMINATION

If the grantee has submitted the security data for the past year, the grantee is not deficient. If the grantee has not submitted the required security data for the past year or is not making current-year submissions as required, the grantee is deficient in the NTD requirements [Note: If this finding is made, it is to be discussed in the NTD area of the report.]

### SUGGESTED CORRECTIVE ACTION

If the grantee is not reporting NTD information, the grantee needs to submit information in the NTD as required.

## Facility Security and Access Control

22. *Are ID badges used for all visitors, employees, and contractors to control access to key critical facilities?*
23. *Has the grantee conducted a physical inspection of facilities to ensure that access is controlled and that facilities are secure?*

### EXPLANATION

Grantees should identify security critical facilities and assets and ensure that access to these facilities is controlled. Grantees should develop written procedures to control access to security critical facilities and areas. The use of ID badges, while not required, is encouraged, for employees, visitors, and contractors that need entry to controlled areas. As with all policies and procedures, access control procedures should be updated as conditions warrant (e.g., new threats are identified).

Grantees should conduct, monitor and document facility security inspections (e.g., perimeter/access control) on a regular basis. The frequency of such

inspections should increase in response to elevation of the HSAS threat advisory level. In addition, grantees should develop and use protocols for vehicle (e.g. buses and rail cars) inspections as well as protocols for inspections of rights-of-way corresponding to HSAS threat advisory levels. In order to integrate unpredictability in the process, grantees should vary the manner in which inspections of facilities, vehicles, and rights-of-way are conducted to avoid setting discernible and exploitable patterns.

### REASON FOR THE QUESTION

[TSA/FTA Action Item No. 12](#)  
[TSA/FTA Action Item No. 13](#)

### SOURCES OF INFORMATION

Review the grantee's policies and procedures that pertain to granting access to security critical systems and facilities.

### DETERMINATION

If the grantee has policies and procedures for granting access to security critical systems and facilities, no advisory comment is made. If the grantee does not have policies and procedures for granting access to security critical systems and facilities, an advisory comment is made.

### SUGGESTED CORRECTIVE ACTION

The grantee should develop procedures for access control for security critical systems and facilities.

## Background Investigations

24. *Have background investigations been conducted on all new front-line operations and maintenance employees?*
25. *Have criteria for background investigations been established?*

### EXPLANATION

Operating personnel have a responsibility for the safety of the public that they serve. As such, it is imperative that grantees take all available precautions in the hiring process to ensure the public's safety and security. Criminal background checks can be used to identify individuals that may pose a potential threat to the public safety and security. Although the focus of background checks is on new hires, grantees are encouraged to conduct checks for all operating employees, particularly those with access to safety and/or security critical systems (e.g., revenue vehicle operations and maintenance, signal rooms, and control centers). Grantees should establish specific criteria for background checks by employee type

(e.g., operator, maintenance employees, safety/security sensitive, and contractors). These criteria should be documented.

### REASON FOR THE QUESTION

[TSA/FTA Action Item No. 14](#)

### SOURCES OF INFORMATION

Ask the grantee if criminal background checks are performed on applicants for operating positions. If available, examine recent job applications (blank) or descriptions of application requirements. An individual's criminal background information is strictly confidential. Under no circumstances should a reviewer request to see individual records. Answers to these questions should be discussed in general terms within the context of the grantee's hiring practices.

### DETERMINATION

If the grantee conducts criminal background checks on applicants for operating positions, no advisory comment is made. If criminal background checks are not conducted for new hires, an advisory comment is made. If the grantee conducts background checks for new hires, but has not done so for existing employees, no advisory comment is made. However, grantees should be encouraged to check the criminal backgrounds of all operating employees, particularly those with access to safety and/or security critical systems.

### SUGGESTED CORRECTIVE ACTION

The grantee should implement a program to conduct criminal background checks on all applicants for operating positions and for existing operating employees.

### Document Control

26. *Is access to documents of security critical systems and facilities controlled?*
27. *Does the grantee have a process for handling of and access to Sensitive Security Information (SSI)?*

### EXPLANATION

Controlling access to documents of security critical systems safeguards the public, transit employees and transit assets from potential sabotage and security risks. Grantees should ensure that an appropriate level of security is provided around the plans and designs of its operating and maintenance facilities and its infrastructure (e.g., tunnels, bridges, electrical substations, etc.). Also, measures to protect

documentation for security detection systems also should be tightly controlled. The grantee should develop document control procedures to ensure that such documents are identified and that a person or department is made responsible for administering the document control program.

### REASON FOR THE QUESTION

[TSA/FTA Action Item No. 15](#)

[TSA/FTA Action Item No. 16](#)

### SOURCES OF INFORMATION

Grantees should be asked if there are adequate document control procedures to safeguard Sensitive Security Information (SSI) and documentation of security critical systems. Policies and procedures also should be reviewed.

### DETERMINATION

If the grantee has procedures to control access to documentation of security critical systems and facilities and security sensitive documents, no advisory comment is made. If the grantee does not have procedures to control access to documentation of security critical systems and facilities and security sensitive documents, an advisory comment is made.

### SUGGESTED CORRECTIVE ACTION

The grantee should develop procedures to control access to documentation for security critical systems and security sensitive documents.

### Security Audits

28. *Has the grantee conducted periodic audits of security policies and procedures?*

### EXPLANATION

It is important for grantees to audit security and emergency response procedures and to take all necessary steps to identify potential security and emergency events. In determining the likelihood of security and emergency scenarios, a grantee can take actions to reduce the chances of an event occurring or, at a minimum, lessen its effects. For example, identifying fire hazards and implementing measures to address them can reduce or even eliminate the risk of fires from potential sources. Some events, such as natural disasters, are not preventable. However, with proper planning, the effects of these events can be mitigated.

**REASON FOR THE QUESTION**

[TSA/FTA Action Item No. 17](#)

**SOURCES OF INFORMATION**

Ask the grantee what audits have been conducted. Review any reports or memoranda that contain security audit information. Review security committee meeting minutes if available. Ask the grantee if procedures and plans have been updated to reflect findings from security audits.

**DETERMINATION**

If the grantee has conducted an audit of its security policies and procedures, no advisory comment is made. If the grantee has not conducted an audit of its security policies and procedures, an advisory comment is made.

**SUGGESTED CORRECTIVE ACTION**

The grantee should have audits of its security and emergency response plans performed and to update plans and procedures as necessary.