

# Top 20 Security Program Action Items for Transit Agencies

The following Action Items identify the most important elements that transit agencies should incorporate into their System Security Program Plans. These top twenty (20) items are based on good security practices identified through FTA's Security Assessments and Technical Assistance provided to the largest transit agencies. Specific information on these elements may be found in FTA's *Transit System Security Program Planning Guide*. FTA is working with transit agencies to encourage them to incorporate these practices into their programs.

## Management and Accountability

1. Written security program and emergency management plans are established.
2. The security and emergency management plans are updated to reflect anti-terrorist measures and any current threat conditions.
3. The security and emergency management plans are an integrated system program, including regional coordination with other agencies, security design criteria in procurements and organizational charts for incident command and management systems.
4. The security and emergency management plans are signed, endorsed and approved by top management.
5. The security and emergency management programs are assigned to a senior level manager.
6. Security responsibilities are defined and delegated from management through to the front line employees.
7. All operations and maintenance supervisors, forepersons, and managers are held accountable for security and emergency management issues under their control.

## Security Problem Identification

8. A threat and vulnerability assessment resolution process is established and used.
9. Security sensitive intelligence information sharing is improved by joining InfraGuard, the FBI Regional Task Force and the Surface Transportation Intelligence Sharing & Analysis Center (ISAC); security information is reported through the National Transit Database (NTD).

## Employee Selection

10. Background investigations are conducted on all new front-line operations and maintenance employees.
11. Criteria for background investigations are established.

## Training

12. Security orientation or awareness materials are provided to all front-line employees.
13. Ongoing training programs on safety, security and emergency procedures by work area are provided.
14. Public awareness materials are developed and distributed on a system wide basis.

### **Audits and Drills**

15. Periodic audits of security and emergency management policies and procedures are conducted.
16. Tabletop and functional drills are conducted at least once every six months and full-scale exercises, coordinated with regional emergency response providers, are performed at least annually.

### **Document Control**

17. Access to documents of security critical systems and facilities are controlled.
18. Access to security sensitive documents is controlled.

### **Access Control**

19. Background investigations are conducted of contractors or others who require access to security critical facilities, and ID badges are used for all visitors, employees and contractors to control access to key critical facilities.

### **Homeland Security**

20. Protocols have been established to respond to the Office of Homeland Security Threat Advisory Levels.