

# PROTECT CAPABILITY MASS TRANSIT PROTECTION

1. Detect Threats
2. Maintain Risk Management Program
3. Mitigate Consequences
4. Educate the Public on Risk information
5. Deter and Defend (Interdict) Threats
6. Prepare to Respond and Recover

## User Instructions

The Target Capabilities List (TCL) provides guidance on target outcomes, risk factors, and resource considerations for capability-based preparedness by helping determine: How prepared are we? How prepared do we need to be? What should we do to close the gaps?

- The **Classes** table groups jurisdictions/entities into appropriate Classes at the top row of the Target Capability based on primary and additional risk factors outlined on the left.
  - Locate your jurisdiction/entity's initial Class placement defined in Section A – Primary Risk Factors.
  - Additional risk factors identified in Section B may be considered for a jurisdiction/entity to increase its Class for the given capability.
  - Since each jurisdiction/entity is unique, any number or combination of risk factors may be considered to justify a Class designation.
- The **Performance Objective** table outlines the level of capability and target outcomes for each Class to build capabilities against.
  - Match your jurisdiction's Class for the capability with the corresponding column.
  - Use the Performance Measures found within your Class to assess your jurisdiction's ability to execute each Performance Objective.
  - The jurisdiction/entity/incident commander determines *how* to achieve target outcomes.
  - No jurisdiction or entity is expected to deliver a capability by itself – rather, capabilities may be met through mutual aid and regional collaboration.
- The **Resource Elements** table directs users to key resources and additional guidance for how Performance Objectives can be accomplished through plans, personnel/teams, equipment, training and exercises.
  - The *Planning Table* identifies Federal guidance, industry standards, Standard Operating Procedures (SOPs), or Emergency Operation Plan (EOP) guidance for a jurisdiction or entity's plans for delivering the capability during a major incident.
  - The *Personnel/Teams Table* identifies what baseline competencies and skill-sets personnel and teams delivering a capability should possess.
  - The *Equipment Table* identifies what equipment jurisdictions should have access to in quantities sufficient to meet the Performance Objective.
  - The *Training and Exercise Table* identifies the essential tasks/learning objectives, which should be able to be demonstrated.
  - A jurisdiction or entity may not require all resource elements to achieve the Performance Objectives for its appropriate Class.

\*This document is intended to provide guidance to jurisdictions for building and measuring capabilities, as well as to help integrate the performance of preparedness activities. It is not meant to prescribe how to perform operations or to be viewed as a standard\*

## PROTECT CAPABILITY – MASS TRANSIT PROTECTION

The capability to maintain a risk management program, mitigate the consequences of a large-scale incident, educate the public on risk information, detect threats, deter and defend (interdict) threats, and prepare to respond and recover.

I. Classes: Lead Jurisdiction or Entity (may include a single agency or a set of agencies and systems) risk considerations for capability building. Classes can be defined by individual jurisdictions and entities or through a grouping of multiple jurisdictions.

Risk Factors	Class One	Class Two	Class Three	Class Four	Class Five
<b>A. Primary Risk Factors: Jurisdictions, entities, or groups of jurisdictions may identify their initial class designation by unlinked passenger miles and annual passenger miles, and may adjust their class based on one or more additional risk factors set forth in B.</b>					
Unlinked Passenger Trips	Jurisdictions or entities with annual unlinked passenger trips <b>greater than</b> 500 million	Jurisdictions or entities with annual unlinked passenger trips <b>between</b> 100 million and 500 million	Jurisdictions or entities with annual unlinked passenger trips <b>between</b> 10 million and 100 million	Jurisdictions or entities with annual unlinked passenger trips <b>between</b> 1million and 10 million	Jurisdictions or entities with annual passenger miles <b>less than</b> 1million
Annual Passenger Miles	Jurisdictions or entities with annual passenger miles <b>greater than</b> 1 billion	Jurisdictions or entities with annual passenger miles <b>between</b> 100 million and 1 billion	Jurisdictions or entities with annual passenger miles <b>between</b> 25 million and 100 million	Jurisdictions or entities with annual passenger miles <b>between</b> 5 million and 25 million	Jurisdictions or entities with annual passenger miles <b>less than</b> 5 million
<b>B. Additional Risk Factors: Jurisdictions, entities, or groups of jurisdictions may move up in Class based on one or more additional risk factors. Once a jurisdiction has identified their Class using primary risk factors, they should identify which additional risk factors they meet to determine Class placement.</b>					
Peak Operations	Jurisdiction or entity has a system that operates <b>greater than</b> 1,000 vehicles during peak operating hours	Jurisdiction or entity has a system that operates <b>between</b> 450 and 1,000 vehicles during peak operating hours	Jurisdiction or entity has a system that operates <b>between</b> 100 and 450 vehicles during peak operating hours	Jurisdiction or entity has a system that operates <b>between</b> 20 and 100 vehicles during peak operating hours	Jurisdiction or entity has a system that operates <b>less than</b> 20 vehicles during peak operating hours
Rail Operations	Jurisdiction or entity has a rail service with <b>over</b> 100 miles of subway track <b>and/or</b> over 100 stations	Jurisdiction or entity has a rail service with <b>between</b> 25 and 100 miles of track <b>and/or</b> between 50 and 100 stations	Jurisdiction or entity has a rail service with <b>between</b> 50 and 25 miles of track <b>and/or</b> less than 25 stations	Jurisdiction or entity has a rail service with <b>less than</b> 10 miles of track <b>and/or</b> less than 25 stations Jurisdiction or entity has a rail service	Jurisdiction or entity has a rail service
	Jurisdiction or entity has a rail service that possesses underground stations <b>and/or</b> elevated track	Jurisdiction or entity has a rail service that possesses underground track and elevated track	Jurisdiction or entity has a rail service that possesses elevated track		
Bus Operations	Jurisdiction or entity has a bus service with an active fleet <b>greater than</b> 2,500 vehicles	Jurisdiction or entity has a bus service with an active fleet <b>between</b> 1,000 vehicles and 2,500 vehicles	Jurisdiction or entity has a bus service with an active fleet <b>between</b> 150 and 1,000 vehicles	Jurisdiction or entity has a bus service with an active fleet <b>between</b> 50 and 150 vehicles	Jurisdiction or entity has a bus service with an active fleet <b>less than</b> 50 vehicles
	Jurisdiction or entity has a bus service possessing bus-only underground bus stops and tunnels, and possesses elevated bus-only infrastructure	Jurisdiction or entity has a bus service possessing bus-only elevated infrastructure	Jurisdiction or entity has a bus service possessing bus-only elevated infrastructure	Jurisdiction or entity has a bus service possessing bus-only elevated infrastructure	
Ferry Operations	Jurisdiction or entity has a public and/or private ferry service with annual passenger trips <b>greater than</b> 15 million	Jurisdiction or entity has a public and/or private ferry service with annual passenger trips <b>between</b> 1.5 million and 15 million	Jurisdiction or entity has a public and/or private ferry service with annual passenger trips <b>between</b> 500,000 and 1.5 million	Jurisdiction or entity has a public and/or private ferry service with annual passenger trips <b>between</b> 100,000 and 500,000	Jurisdiction or entity has a public and/or private ferry service with annual passenger trips <b>less than</b> 100,000
Intermodal interdependence relationships		Jurisdiction or entity possesses an Intermodal connection(s) between air and other forms of mass transit	Jurisdiction or entity has over _ weekly linked Intermodal connections between rail, bus, and/or ferry systems.	Jurisdiction or entity has Intermodal connections between rail, bus, and/or ferry systems.	
Relationship with non-transit critical infrastructure		Jurisdiction or entity has a system that services a DHS-designated Tier I CI/KR asset	Jurisdiction or entity has a system that services a DHS-designated Tier II CI/KR asset		

**II. Performance Objectives: Target outcomes and metrics are aligned by Class (Table I) and serve as guidance for capability building (outcomes are met through any combination of a jurisdiction or entity’s resources, mutual aid, and other assistance)**

	Performance Objectives	Class One	Class Two	Class Three	Class Four	Class Five
1	<b>Maintain Risk Management Program</b>	Adopt an all-hazards risk management program and conduct a risk assessment (including Transit Systems Vulnerability) every 2 years through a methodology formally adopted or consistent with the National Infrastructure Protection Plan, TSA or FTA.	Adopt an all-hazards risk management program and conduct a risk assessment (including Transit Systems Vulnerability) every 3 years through a methodology formally adopted or consistent with the National Infrastructure Protection Plan, TSA or FTA.	Adopt an all-hazards risk management program and conduct a risk assessment (including Transit Systems Vulnerability) every 5 years through a methodology formally adopted or consistent with the National Infrastructure Protection Plan, TSA or FTA.	Adopt an all-hazards risk management and conduct a risk assessment (including Transit Systems Vulnerability) every 5 years through a methodology formally adopted or consistent with the National Infrastructure Protection Plan, TSA or FTA.	Adopt an all-hazards risk management program; and conduct a risk assessment (including Transit Systems Vulnerability) every 5 years through a methodology formally adopted or consistent with the National Infrastructure Protection Plan, TSA or FTA..
2	<b>Mitigate Consequences</b>	Assign resource allocations and facility designs to priority risks in an improvement plan spanning the four mission areas of prevent, protect, respond, and recover; and update the improvement plan every fiscal cycle.	Assign resource allocations and facility designs to priority risks in an improvement plan spanning the four mission areas of prevent, protect, respond, and recover; and update the improvement plan every fiscal cycle.	Assign resource allocations and facility designs to priority risks in an improvement plan spanning the four mission areas of prevent, protect, respond, and recover; and update the improvement plan every other fiscal cycle.	Assign resource allocation and facility designs to priority risks in an improvement plan spanning the four mission areas of prevent, protect, respond, and recover; and update the improvement plan every other fiscal cycle.	Assign resource allocation sand facility designs to priority risks in an improvement plan spanning the four mission areas of prevent, protect, respond, and recover; and update the improvement plan every other fiscal cycle.
3	<b>Educate the Public on Risk Information</b>	Provide opportunities for 100% of the public to be educated on transit risks such as through the display of awareness information throughout the system, making public announcement messages in stations and vehicles, posting security awareness and emergency preparedness information on the transit agency website, varying the content and appearance of messages to retain public interest, and providing volunteer training to the public for system evacuations and emergency response.	Provide opportunities for 100% of the public to be educated on transit risks such as through the display of awareness information throughout the system, making public announcement messages in stations and vehicles, posting security awareness and emergency preparedness information on the transit agency website, varying the content and appearance of messages to retain public interest, and providing volunteer training to the public for system evacuations and emergency response.	Provide opportunities for 100% of the public to be educated on transit risks such as through the display of awareness information throughout the system, making public announcement messages in stations and vehicles, and posting security awareness and emergency preparedness information on the transit agency website.	Provide opportunities for 100% of the public to be educated on transit risks such as through the display of awareness information throughout the system and posting security awareness and emergency preparedness information on the transit agency website.	Provide opportunities for 100% of the public to be educated on transit risks such as through the display of awareness information throughout the system and posting security awareness and emergency preparedness information on the transit agency website.
4	<b>Detect Threats</b>	Employ a layered defense strategy for detecting threats, including the use of surveillance cameras throughout the system and the placement of available and approved (CBRNE) detection devices at the highest threat locations connected to a central command and security operations center, consistent with TSA and FTA guidance.	Employ a layered defense strategy for detecting threats, including the use of surveillance cameras throughout the system and the placement of available and approved (CBRNE) detection devices at the highest threat locations connected to a central command and security operations center, consistent with TSA and FTA guidance.	Employ a layered defense strategy for detecting threats, including the use of surveillance cameras at the highest threat locations connected to a central command and security operations center, consistent with TSA and FTA guidance.	Employ a layered defense strategy for detecting threats with feeds connected to a central security operations center consistent with TSA and FTA guidance.	Employ a layered defense strategy for detecting threats with feeds connected to a central security operations center consistent with TSA and FTA guidance.
5	<b>Deter and Defend (Interdict) Threats</b>	Employ integrated intrusion detection and alarms systems and physical barriers throughout key facilities, and adopt suspicious-activity reporting programs and counter-surveillance measures.	Employ integrated intrusion detection and alarms systems and physical barriers throughout key facilities, and adopt suspicious-activity reporting programs and counter-surveillance measures.	Employ physical barriers throughout all key facilities and adopt suspicious-activity reporting programs and counter-surveillance measures.	Employ physical barriers throughout all key facilities and adopt suspicious-activity reporting programs and counter-surveillance measures.	Employ physical barriers throughout all key facilities.
6	<b>Prepare to Respond and Recover</b>	Possess 24/7 monitoring connectivity between transit command/ emergency operations center and the jurisdiction’s emergency management agency’s emergency operations center.	Possess 24/7 monitoring connectivity between transit command/ emergency operations center and the jurisdiction’s emergency management agency’s emergency operations center.	Possess 24/7 connectivity between transit command staff and local law enforcement.	Possess 24/7 connectivity between transit command staff and local law enforcement.	Possess regular connectivity between transit command staff and local law enforcement.

### III. Resource Elements: Guidance for plans, personnel/teams, equipment, training, and exercises for meeting Performance Objectives (Table II) through any combination of a jurisdiction or entity's resources, mutual aid, and other assistance

*A jurisdiction or entity may not require all resource elements identified to achieve Performance Objectives.*

*Guidance on the resources to build a capability is applicable for use by a jurisdiction or entity in any Class unless otherwise indicated.*

#### PLANS

The *Planning Table* identifies industry standards Standard Operating Procedures (SOPs) or Emergency Operation Plans (EOPs) should include for ensuring that contingencies are in place for delivering the Mass Transit Protection capability. The Planning Table directs readers to guidance found in other industry standards and policy documents.

Jurisdictions and entities should reference their specific hazard and vulnerability analysis to develop planning requirements specific to their needs. EOPs should specify how an agency will obtain the personnel, teams, and equipment necessary to meet each Mass Transit Protection Performance Objective during a disaster.

#### Maintain Risk Management Program

1. TSA/FTA Security and Emergency Management Action Items for Transit Agencies [link](#)
2. FEMA 452- A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings [link](#)
3. TSA Transit Sector-Specific Plan Mass Transit Modal Annex [link](#)
4. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)
5. DHS National Infrastructure Protection Plan [link](#)
6. APTA Recommended Practice for Trash/Recycling Container Placement to Mitigate the Effects of an Explosive Event (p. 3 – 4) [link](#)
7. APTA First Responder Familiarization of Transit System Training [link](#)
8. Fiscal Year 2009 Transit Security Grant Program Guidance and Application Kit [link](#)
9. Security and Emergency Preparedness Plan Template [link](#)

#### Mitigate Consequences

1. FEMA 426- Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (Chapter 5) [link](#)
2. FEMA 452- A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings [link](#)
3. FEMA Continuity of Operations Planning Web-Based Course [link](#)
4. TSA Transit Sector-Specific Plan Mass Transit Modal Annex [link](#)
5. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)
6. APTA Recommended Practice for a Continuity of Operations Plan [link](#)
7. APTA Recommended Practice for Trash/Recycling Container Placement to Mitigate the Effects of an Explosive Event (p. 3 – 6) [link](#)

#### Educate the Public on Risk Information

1. TSA/FTA Security and Emergency Management Action Items for Transit Agencies [link](#)
2. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)

#### Detect Threats

1. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)
2. TSA Transit Sector-Specific Plan Mass Transit Modal Annex [link](#)
3. TSA/FTA Security and Emergency Management Action Items for Transit Agencies [link](#)
4. APTA Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities [link](#)

#### Deter and Defend (Interdict) Threats

1. FEMA 427- Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks (Chapter 5,6) [link](#)
2. TSA Transit Sector-Specific Plan Mass Transit Modal Annex [link](#)
3. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)
4. APTA Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities [link](#)

**Prepare to Respond and Recover**

1. DHS National Infrastructure Protection Plan: Transportation Systems Sector-Specific Plan [link](#)
2. APTA Recommended Practice for First Responder Familiarization of Transit Systems [link](#)
3. APTA Recommended Practice for Security & Emergency Management Aspects of Special Event Service [link](#)
4. APTA Recommended Practice for a Continuity of Operations Plan [link](#)
5. Transit Research Board (TRB) The Role of Transit in An Emergency Evacuation, Transportation Research Board, 2008 [link](#)

**PERSONNEL/TEAMS**

The *Personnel/Teams Table* identifies what baseline competencies and skill-sets personnel delivering a capability should possess. FEMA recommends that agencies also reference the *TSA/FTA Security and Emergency Management Action Items for Transit Agencies* when reviewing baseline competency requirements. This TSA/FTA document may be accessed here: [link](#)

**Maintain Risk Management Program**

1. Risk Evaluation
2. Pre-Incident Planning
3. Vulnerability Assessment
4. Application of Risk Assessment to Resource Decision Making
5. Facility Design

**Detect Threats**

1. Anomaly Detection
2. Surveillance/Monitoring
3. Familiarity with Key Facilities, System Components, Equipment, and Structures
4. VIPR Teams\*

**Mitigate Consequences**

1. Interagency Coordination
2. Continuity Planning
3. Information Sharing
4. Anomaly Detection
5. Familiarity with key facilities, system components, equipment, and structures

**Deter and Defend (Interdict) Threats**

1. Improvised Explosive Devices Identification
2. Physical Barrier Deployment
3. Patrol/Monitoring

**Educate the Public on Risk Information**

1. Media Outreach
2. Public Security and Emergency Awareness Program Management
3. Customer Outreach

**Prepare to Respond and Recover**

1. Post Incident Clean-Up and Recovery
2. Follow-Up Debriefing
3. After Action Report Creation and Utilization
4. Employee Crisis Counseling
5. Long Term Recovery Initiation
6. Familiarity with Key Facilities, System Components, Equipment, and Structures
7. Coordination with Law Enforcement and Incident Command Entities

\*For Class One only

**EQUIPMENT**

The *Equipment Table* details what Mass Transit Protection equipment an agency needs for steady-state operations. Steady state operations are defined as operations that an agency carries out on a regular basis, in the absence of a large-scale disaster. Equipment references are drawn from existing Federal guidance including the Standardized Equipment List (SEL), Authorized Equipment List (AEL), Public Transportation System Security and Emergency Preparedness Guide, and National Infrastructure Protection Plan's Mass Transit Modal Annex.

The complete DHS Authorized Equipment List (AEL) provides general categories and specific equipment allowable for funding under the DHS Homeland Security Grant Programs. Additional information on equipment, including applicable standards, manufacturing requirements and reviews, can be found at the Responder Knowledge Base (RKB) at [www.rkb.us](http://www.rkb.us).

**Maintain the Risk Management Program**

1. Database information technology
2. Risk management software (to facilitate capture, quantification, and management of risk factors involved in specific tasks, environments, or programs)

**Detect Threats**

1. Automatic vehicle location (AVL) systems
2. Mobile data terminal systems (to facilitate communication between the dispatcher and driver while allowing the driver to operate the vehicle)
3. Intrusion detection sensors (IDS)

**Mitigate Consequences**

1. System redundancies (control center, communications)
2. Blast-resistant trash cans
3. Tracking/identification software for CBRNE/commercial chemical hazards
4. Traffic modeling software (designed to depict traffic flow, identify congestion points, and predict impact of accidents or deliberate alterations of traffic patterns such as alterations of signal times, detours, closures, etc. Traffic flow may be for vehicular, maritime, aviation, pedestrian, or other flows)
5. Computer aided dispatch systems (to track and manage public safety incidents and resources)

4. Silent alarm and emergency signals
5. Information security technology
6. Data collection software, including data mining tools
7. Data and information-sharing system
8. Data exchange and interoperability equipment
9. Inspection systems (including cameras and surveillance equipment; ground/wall penetrating radar; personnel/package screening systems; scanner, sniffer, and sensor devices)

**Educate the Public on Risk Information**

1. Billboards, posters, and brochures
2. Reminding keepsakes, such as key chain flashlights disseminated by TSA in the WMATA system
3. Signage
4. Public notification and warning systems

**Deter and Defend (Interdict) Threats**

1. Access control and authentication devices for control centers, stations, and vehicles
2. Infrastructure hardening
3. Explosion Protection (including bomb-resistant trash receptacles and blast/shock/impact resistant building systems)
4. Surveillance, warning, access/intrusion control (including audio, data, and visual surveillance equipment; alarm systems/sensors; impact resistant doors and gates; fire extinguisher monitoring systems; fixed area lighting; physical access control systems; personnel identification systems; vehicle identification systems; security video assessment systems; barriers; and fences)
5. Waterfront surveillance, warning, access/intrusion control (including hull hardening equipment, radar systems, sonar systems, and vessel barriers)
6. Alert/notification systems (for real-time dissemination of information and intelligence among responders)

**Prepare to Respond and Recover**

1. Software for tracking of tangible equipment, including location and person(s)/organization(s) responsible
2. Interoperable communications equipment

**TRAINING AND EXERCISES**

The *Training and Exercise Table* identifies the essential tasks, or learning objectives, which personnel assigned to Mass Transit Protection operations must be able to complete. Learning objectives are consistent with the forthcoming FEMA [Training and Exercise Integration/Training Operations \(TEI/TO\)](#) Training Frameworks, which will emphasize the need for jurisdictions to build their capacity in relation to the capabilities noted in the TCL. Learning objectives reflect skills and abilities that can be observed during an operation and do not represent all related awareness and pre-requisite course requirements.

Learning objectives form the foundation for exercise conduct. The learning objectives listed below should form the foundation for how jurisdictions conduct operations-based exercises. Jurisdictions should ensure that personnel have taken courses that teach the ability to perform each listed learning objective. The list enables course developers to align existing courses to each Performance Objective, or as a starting point for establishing new courses.

The Learning Objectives for each capability will be integrated into the National Homeland Security Training Program (currently under development), which will oversee and coordinate homeland security training programs, increase training capacity, and ensure standardization across programs. Homeland Security Exercise and Evaluation Program (HSEEP) and the Exercise Evaluation Guides (EEGs) will also be updated. Information on HSEEP, including the latest version of the *EEG Builder* Web-based tool can be found at [www.hseep.dhs.gov](http://www.hseep.dhs.gov)

**Maintain Risk Management Program**

- |   |  |
|---|--|
| <ol style="list-style-type: none"> <li>1. Conduct a risk evaluation, adequately addressing the risk of various actions to both personnel and the public</li> <li>2. Conduct inventory and verify readiness of protective equipment</li> <li>3. Conduct pre-incident liaison and planning with Federal or other weapons of mass destruction (WMD) response organizations</li> <li>4. Establish preparedness plans and procedures</li> <li>5. Prioritize vulnerabilities</li> </ol> | <ol style="list-style-type: none"> <li>6. Establish a security and emergency response program</li> <li>7. Conduct employee background screenings</li> <li>8. Conduct vendor and contractor background screening</li> <li>9. Develop systems to address security issues</li> <li>10. Identify security vulnerabilities</li> </ol> |
|---|--|

**Mitigate Consequences**

- |  |   |
|--|---|
| <ol style="list-style-type: none"> <li>1. Coordinate with State, local and tribal government to address security concerns</li> <li>2. Implement life safety measures for protection of passengers and employees</li> </ol> | <ol style="list-style-type: none"> <li>6. Enhance response capabilities</li> <li>7. Establish regional law enforcement network (with Mass Transit law enforcement)</li> </ol> |
|--|---|

**Pre-Decisional Draft**

3. Enhance security systems and capabilities to identify CBRNE threats
4. Enhance response equipment inventory
5. Institute protective measures

8. Provide human/technical resources for anomaly detection
9. Address evacuation of vehicles and facilities
10. Address communication failures

**Educate the Public on Risk Information**

1. Incorporate security awareness program into public education activities
2. Install signage to aid public in reporting suspicious activity
3. Conduct public service announcements (PSAs)
4. Disseminate public awareness information

5. Ensure accuracy of evacuation routes
6. Instruct against unattended vehicles
7. Implement high visibility patrols

**Detect Threats**

1. Conduct surveillance of critical locations
2. Conduct surveillance detection activities
3. Monitor all external network connections
4. Implement personnel/vehicle inspection program
5. Ensure critical data backup

6. Conduct periodic inspections
7. Inspect unstaffed/remote areas
8. Conduct inspections of vehicles
9. Monitor fuel storage areas
10. Deploy canine detection teams, if available

**Deter and Defend (Interdict) Threats**

1. Increase electronic surveillance
2. Establish known, visible deterrence measures
3. Conduct regular and random patrol, both uniformed and plain clothed
4. Install/maintain video surveillance systems
5. Implement target-hardening measures

6. Increase security patrols
7. Increase security visibility
8. Deploy physical barriers
9. Monitor unattended packages

**Prepare to Respond and Recover**

1. Prepare to reestablish system operations following incident
2. Inform personnel of potential threat
3. Instruct key personnel to activate emergency operation plans
4. Monitor and redirect transportation systems
5. Limit route schedules and guard against secondary attacks

7. Reinforce personnel to increase vigilance
8. Manage mass casualty event
9. Limit access to facilities
10. Coordinate with regional response agencies to ensure collaborative response