Federal Transit Administration

Transit Agency Security and Emergency Management Protective Measures

November 2006

Prepared By

Battelle
TotalSecurity.US
Transportation Resource Associates

Distributed By
National Transit Institute

For additional copies of this report, please contact the National Transit Institute at: safety@nti.rutgers.edu or 732-932-1700 ext. 231

TRANSIT AGENCY SECURITY AND EMERGENCY MANAGEMENT PROTECTIVE MEASURES

FEDERAL TRANSIT ADMINISTRATION

NOVEMBER 2006

PREPARED BY

BATTELLE
TOTALSECURITY.US
TRANSPORTATION RESOURCE ASSOCIATES

Acknowledgments

This document was prepared for the Federal Transit Administration by Battelle under Project OH-26-5032. The Battelle Team includes Battelle, Transportation Resource Associates, and TotalSecurity.US. The authors gratefully acknowledge the participation from FTA, in particular Rick Gerhart, Bridget Zamperini and Mike Taborn.

The authors and FTA wish to acknowledge the participation, input, and comments from personnel at the Department of Homeland Security's Transportation Security Administration and Office of Grants and Training, VIA Metropolitan Transit (San Antonio), Washington Metropolitan Area Transit Authority, Metropolitan Atlanta Rapid Transit Authority, and the Chicago Transit Authority, as well as the American Public Transportation Association Committee on Public Safety.

Disclaimer

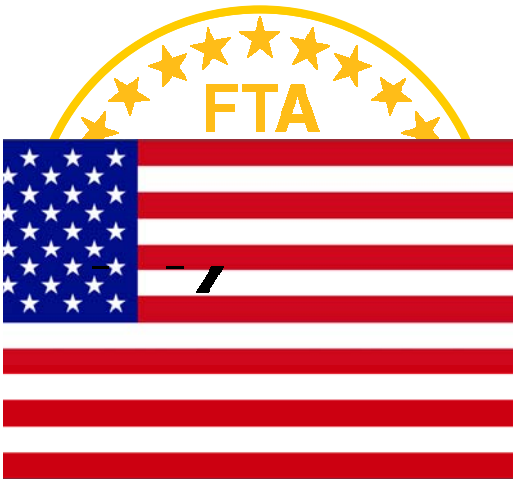


Table of Contents

List of Appendices

List of Tables

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

Acronyms and Abbreviations

APTA – American Public Transportation Association
CBRNE – Chemical, Biological, Radiological, Nuclear, or Explosive
CCTV – Closed Circuit Television
CPTED – Crime Prevention Through Environmental Design
DHS – Department of Homeland Security
DMZ – Demilitarized Zone (computing)
DOT – Department of Transportation
EOC – Emergency Operations Center
EOP – Emergency Operating Procedure
FBI – Federal Bureau of Investigation
FOIA – Freedom of Information Act
FRA – Federal Railroad Administration
FRAWG – Federal Risk Assessment Working Group
FTA – Federal Transit Administration
HAZMAT – Hazardous Materials
HSIN – Homeland Security Information Network
HSAS – Homeland Security Advisory System
HSPD – Homeland Security Presidential Directive
HVAC – Heating, Ventilation, and Air Conditioning
IAs – Immediate Actions
IT – Information Technology
JTTF – Joint Terrorism Task Force
K-9 – Dog patrol
MOA – Memorandum of Agreement
MOU – Memorandum of Understanding
NIPP – National Infrastructure Protection Plan
NRP – National Response Plan
OGT – Office of Grants and Training
PDD – Presidential Decision Directive
PM – Protective Measure
ROW – Right of Way
SC – Security Coordinator
SD – Security Directive
SOP – Standard Operating Procedure
SSI – Sensitive Security Information
ST-ISAC – Surface Transportation Information Sharing and Analysis Center

SVA – Security Vulnerability/Risk Assessment
TSA – Transportation Security Administration
TSOC – Transportation Security Operations Center
TVA – Threat and Vulnerability Analysis
WMD – Weapons of Mass Destruction
WTC – World Trade Center

Glossary of Highlighted Terms

(Note: where available, the definitions provided below are verbatim or summarized from the National Infrastructure Protection Plan (NIPP – July 2006) or the National Response Plan (NRP – December 2004) glossary definitions. For additional information regarding these definitions, please refer to the NIPP or NRP).

All Hazards – an approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

Attack or Active Incident – an actual emergency, which might include a terrorist attack, accident, or natural disaster.

Criminal Activity – an activity that violates the law.

Detection – the identification and validation of potential threat or attack that is communicated to an appropriate authority that can act. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security awareness programs.

Deterrence – an activity, procedure, or physical barrier that reduces the likelihood of an incident, attack, or criminal activity.

Emergency Incident – an incident where emergency response is required, specifically, an imminent threat to human life.

Graduated Security Response – a security response that increases in a modular or continuous fashion as the defined threat level increases in severity; protective measures implemented at lower threat levels build to the higher threat level protective measures in a cumulative fashion.

Mitigation – activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

Protective Measures – planned activities that reduce vulnerability, deny an adversary opportunity, or increase response capability during a period of heightened alert.

Recovery – the development, coordination, and execution of service- and site-restoration plans for impacted areas and operations.

Response – activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.

Risk – a measure of potential harm that encompasses threat, vulnerability, and consequence.

Security Vulnerability/Risk Assessment (SVA) – a systematic assessment approach for security vulnerability/risk and includes threat and vulnerability analysis (TVA).

Sensitive Security Information (SSI) – any information or records that the disclosure of the information may compromise safety or security of the traveling public and transit workers. The use of SSI is intended to restrict the material from automatic Freedom of Information Act (FOIA) disclosure.

Terrorist Attack – an intentional act of violence with intent to: inflict significant damage to property, inflict casualties, and produce panic and fear.

Threat – a potential action or situation that may cause harm to people or property.

Vulnerability – a weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.

Weapons of Mass Destruction (WMD) – weapons that can cause significant destruction of property and inflict significant numbers of casualties and deaths; typically considered to be a part of the group of weapons called chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons.

Executive Summary

This document has been developed by the Federal Transit Administration (FTA), in consultation with the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and Office of Grants and Training (OGT). This document provides an approach that integrates a transit agency's entire security and emergency management programs with the Department of Homeland Security (DHS) Homeland Security Advisory System (HSAS) threat conditions as an organizational framework.

The HSAS is made up of five graduated threat conditions.

- Severe – Red
- High – Orange
- Elevated – Yellow
- Guarded – Blue
- Low – Green

In addition to protective measures responsive to the HSAS threat conditions, this document also provides protective measures to be implemented in the event of an **Attack or Active Incident** (an actual emergency, which might include a terrorist attack, accident or natural disaster) and during the **Recovery** phase following an incident[1].

This document has been developed as a technical resource to transit agency executive management and senior staff assigned to implement protective measures for response to the HSAS threat conditions and emergencies that might affect a transit agency. This document includes a description of the HSAS and what it means for transit, a description of the approach described in this document, and a general protective measures implementation process, as shown in Figure ES-1.

Protective measures (PMs) are actions intended to reduce vulnerability, deny an adversary opportunity, or increase response capability during a period of heightened alert. Not all protective measures presented in this report are necessarily appropriate or applicable for all transit agencies, as transit agencies vary greatly in size and types of modes (bus, rail, paratransit, etc.) operated.

[1] Originally, FTA designated these two response conditions as Black and Purple. The protective measures are still, but these two color codes have been removed to stay consistent with the rest of the federal government.

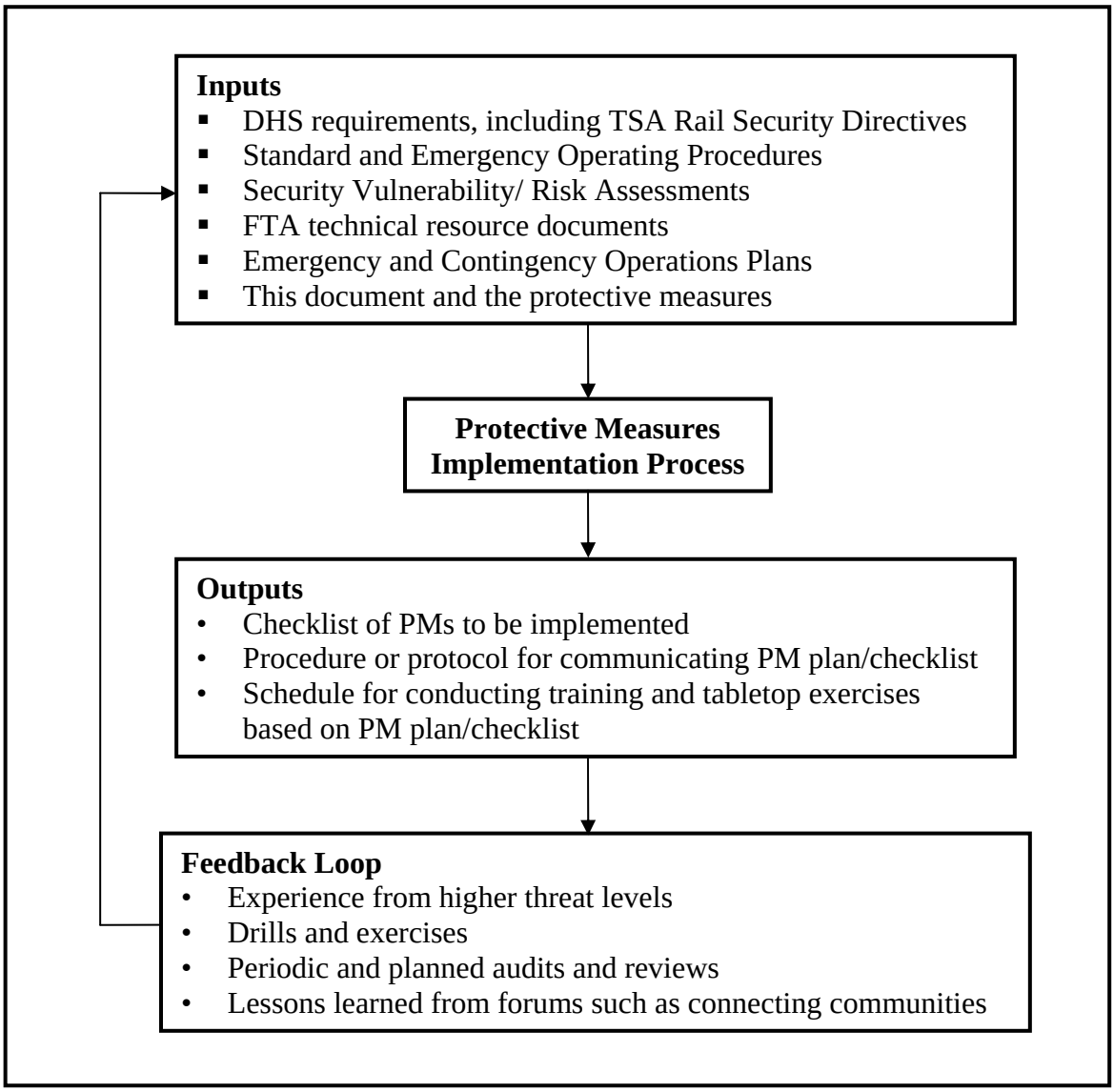


Figure ES-1. General Protective Measures Implementation Process

TECHNICAL RESOURCE DOCUMENT

Transit Agency Security and Emergency Management Protective Measures

Introduction

The federal government, including the Federal Transit Administration (FTA), and the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and Office of Grants and Training (OGT), and transit agencies continue to prepare for the occurrence of a terrorist attack or any other significant emergency. Efforts since 9/11 have included updating, developing, and implementing better procedures and plans, more training, and drills and exercises. Most of all, there are now better communications within each transit agency, as well as with other transit agencies, first responders, and regional and federal agencies. These efforts are reflected in the FTA/DHS Security and Emergency Management Program Action Items for Transit Agencies – a blueprint for a good security and emergency management program; details on this action items list can be found on the FTA Office of Safety and Security's website at: http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20/default.asp.

In September 2005, FTA along with TSA and OGT formalized their cooperative efforts via the Public Transportation Security Annex to the Department of Transportation/Department of Homeland Security Memorandum of Understanding on roles and responsibilities. The Annex identifies specific areas of coordination among the parties, including citizen awareness, training, exercises, risk assessments, and information sharing. The parties to the Annex have developed an implementation framework that leverages each agency's resources and capabilities. The implementation framework process is overseen by an Executive Steering Committee comprised of senior leadership from FTA, TSA and OGT. See Appendix A for a schematic representation of the Public Transportation Security MOU Annex implementation framework.

In the aftermath of the March 2004 attacks on the Madrid commuter trains, TSA issued rail security directives (SDs) applicable to rail transit and passenger rail systems. To ensure consistency and coordination, the rail SDs, which are required to be implemented by rail transit systems, are included in this document as protective measures, and are identified as such.

Purpose of this Document

This document provides a set of suggested protective measures and a systematic approach for their application to enhance transit security and emergency management. The protective measures align with the color-coded threat conditions used in the DHS Homeland Security Advisory System (HSAS). Beyond the graduated threat condition protective measures, additional protective measures are provided in two areas: (1) **Attack or Active Incident** – in the

event an attack occurs or an active incident (such as a natural disaster or HAZMAT accident) is ongoing affecting a transit system or in its area, and (2) **Recovery** – during recovery from such an attack, natural disaster or significant other incident.

Protective measures (PMs) are actions or activities that may have the ability to reduce vulnerability, deny an adversary opportunity, or increase response capability for the transit agency especially during a period of heightened alert, as reflected by the changing of the HSAS color-code conditions. This document provides a general approach to implementing protective measures that is an integration of the transit agency's entire security and emergency management program (including both normal and contingency operations) with the national framework of the HSAS threat conditions. In other words, with this approach, all aspects of the transit agency's security and emergency management activities should be planned and described in a manner that is consistent with the HSAS threat conditions.

This integrated approach allows for planning and communications inside and outside the transit agency. The approach also includes reviewing the wide range of capabilities and needs that the transit agency may want to consider implementing before the next emergency situation arises. Finally, the approach provides the transit agency with a process to transition current graduated security and emergency management protocol to one based on the HSAS threat conditions and the Active Incident and Recovery phases.

Traditionally, the transit agency's goals for the security and emergency management programs have been focused on the deterrence of and response to criminal activities and natural disasters. In the post 9/11 environment, transit agencies have added deterrence and response to terrorist threats and activities. A ***terrorist attack*** is an intentional act of violence that is intended to inflict significant damage to property, inflict casualties, and produce panic and fear. A ***threat*** is a potential action or situation that may cause harm to people or property.

The approach to HSAS threat condition preparation includes two major differences to the design of previously traditional security and emergency management programs:

- The availability of improved intelligence and threat information to provide advance warning to transit agencies to increase their security readiness.
- The inclusion of security readiness and response capabilities for potential threats such as chemical, biological, radiological, nuclear and explosive (CBRNE) ***weapons of mass destruction (WMD)*** into the planning process at the transit agency.

Through the implementation of the process described in this document, FTA encourages transit agencies to make cost effective and appropriate plans for responding to all types of threats and emergencies.

The increasing HSAS threat conditions (Green, Blue, Yellow, Orange, and Red) allow transit agencies to develop and apply graduated responses as part of their preparedness to handle potential terrorist and criminal activities directed against their property, employees and customers. This document provides a range of protective measures (categorized by color-coded

threat levels) that are intended to help transit agencies deter, respond and recover from terrorism and non-terrorist crime.

A ***graduated security response*** means that as the HSAS threat condition changes, the security response of the transit agency should be modified accordingly. As an example, under HSAS threat condition "Red", offices may be closed to the public, service delivery could be reduced, and facilities more closely guarded. The application of these restrictive measures would be an appropriate policy for a short period of time ("surge capacity") under an imminent threat level. As the threat level is lowered back to "Orange" or "Yellow", service delivery can return to normal and security could be adjusted to reflect the lowered threat condition.

Consistent with the National Response Plan's (NRP)[2] and National Infrastructure Protection Plan (NIPP)[3] **all-hazards** approach, the activities described in this report also help prepare the transit agency for any emergency, including those caused by natural disasters (e.g., snow/ice; earthquake; hurricane; flooding), major accidents, and criminal and terrorist activities. The systems approach presented in this document includes additional protective measures for the Attack or Active Incident condition and the Recovery condition, regardless of what caused the emergency (natural disaster, accident, terrorism or non-terrorism criminal act).

Objectives of this Document

Transit agencies have finite resources for security and emergency preparedness activities. In general, the objective of the transit agency security and emergency management program is to optimize deterrence and response capabilities based on those finite resources. The objectives of this protective measures document are to:

(1) Help the transit agency perform an agency-wide security and emergency preparedness gap analysis

(2) Help the transit agency assemble and prioritize a matrix of desired capabilities and resources for potential threats and emergencies

(3) Help the transit agency communicate across all of its departments what each department is expected to do at a given threat condition.

Document Organization

This document provides:

- A basic description of the HSAS threat conditions as well as the two response conditions of Attack or Active Incident and Recovery
- A general approach to integrating HSAS threat conditions into existing transit agency security and emergency management programs

[2] Department of Homeland Security, "National Response Plan," December 2004.

[3] Department of Homeland Security, "National Infrastructure Protection Plan," July 2006.

A listing of all of the protective measures is provided in Appendix B for transit agency use. Appendix C provides a more detailed implementation process that transit agencies may wish to use.

The general philosophy presented in this document is a layered approach that builds upon basic security and emergency management awareness by developing and implementing specific processes, procedures and activities for each department in the transit agency. This approach is described in the following three sections:

(1) HSAS for Transit – a basic description of the HSAS color-coded threat conditions and the two response conditions, and what they mean for transit agencies

(2) Protective Measures: Concepts – an approach to implementing protective measures for deterring terrorism and other criminal activities, as well as the response capabilities needed for day-to-day security operations and for responding to an emergency incident/event

(3) Protective Measures: Implementation Process – procedures and processes the transit agency can work through to implement a systematic approach to preparing for changing HSAS threat conditions and potential response and recovery from an actual emergency. (As mentioned above, a more detailed version is provided in Appendix C).

(1) HSAS for Transit

This section describes the DHS color-coded HSAS for preparedness related to a terrorist threat condition in the United States. The HSAS has been created as a means to "disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people[4]." The HSAS threat condition may be based on a general threat condition applicable to the entire country or it could be a threat to a specific industry or region.

As shown in Figure 1, each HSAS threat condition from Green to Red is built cumulatively on the lower level threat conditions and the protective measures employed at each of those lower level threat conditions. The transit agency security and emergency management activities for heightened HSAS alerts are often the same as those employed as part of increased preparations for scheduled major public events and natural disasters. It should also be remembered that a terrorist incident or any emergency/incident can occur at any time regardless of HSAS threat condition. Once an incident is under way, the transit agency (and the region) will respond (Active Incident) and over a period of time will recover (Recovery) from the incident.

An Attack or Active Incident may occur in the region and not specifically on the transit system. In this case, a transit system's resources may be needed for extended regional support, in addition to its own service delivery area. Also, an incident or emergency may be specific to a particular mode (such as a subway) or a critical asset (such as a major transit center) and may not include the entire transit system. Thus, some elements of a transit system may be under an

[4] Homeland Security Advisory System, Homeland Security Presidential Directive #3, March 11, 2002.

Active Incident condition or in the Recovery phase, while the rest of the transit system may be at another threat condition (most likely Red).

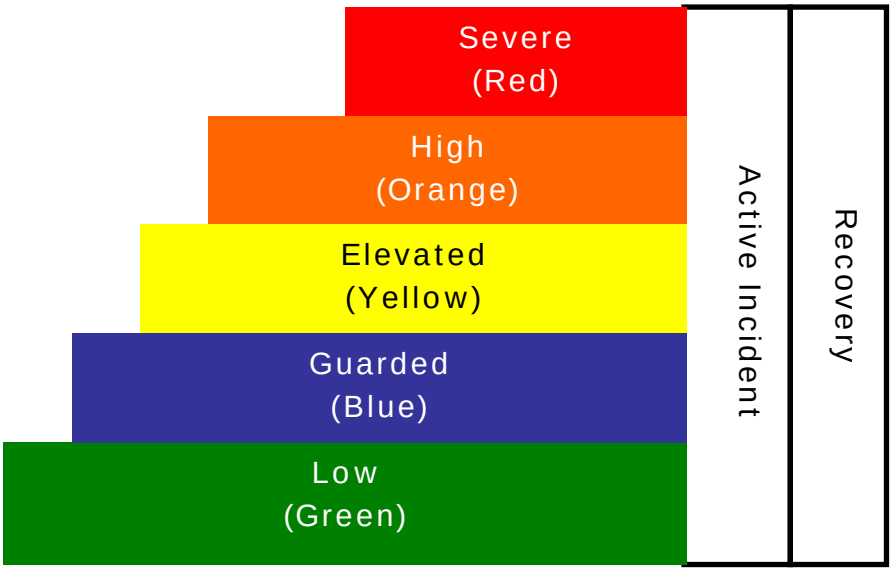


Figure 1. HSAS Threat Condition Connectivity

HSAS threat conditions and the additional two response conditions are defined as follows[5]:

- **Low (Green) –** At the Low or Green threat condition, transit agency activities revolve around preparation of plans and making sure that capabilities exist within the transit system for the implementation of higher threat condition activities. Security and emergency preparedness-related plans to be completed include standard operating procedures, emergency operating procedures, emergency response procedures, contingency planning, communications planning, information technology/disaster recovery planning, and others as needed. For each of these plans, departments within the transit agency will need to complete an inventory of their supplies, equipment, and other resources that may be needed to execute any portion of the plans. Training will need to be created and delivered based on these plans and procedures. A ***Security Vulnerability/Risk Assessment (SVA)*** process will need to be implemented to support the planning and preparations process.

- **Guarded (Blue)** – The Guarded or Blue threat condition is the first level of potential threat. Activities at this threat condition include practice all of the security and emergency preparedness plans and procedures as well as determine what steps should be undertaken in managing an incident. Equipment and systems need to be tested and any "found" problems need to be addressed in a timely manner. Inventories of supplies need

[5] HSAS color-coded threat condition definitions:
http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0046.xml

to be re-checked, maintenance logs inspected, and new supplies ordered. Drills and exercises should be designed and executed to practice emergency, disaster recovery, and contingency operations capabilities. Public awareness information for security and emergency preparedness needs to be developed and disseminated as appropriate. Security awareness messages that must be displayed during higher threat conditions need to be developed and planned. All of the plans and procedures need to be reviewed and updated on a regular basis. Any problems, shortcomings, or issues identified through drills and exercise after-action reports need to flow into revisions for the plans, procedures, and training as appropriate.

- **Elevated (Yellow)** – An Elevated or Yellow threat condition indicates a significant risk exists for some type of terrorist activity or attack. At this threat condition, the activities needed to be performed by a transit agency include increased surveillance, coordinating emergency plans and procedures, checking if other protective measures need to be put in place based on the threat information, and initiating contingency activities as appropriate (such as checking that equipment and alternate operating locations are available and equipment processes and procedures are operating properly).

- **High (Orange)** – A High or Orange threat condition indicates that a high risk of terrorist activity has been declared. Activities during an Orange threat condition include coordination of security efforts at the transit agency, local, state, and federal agencies as appropriate. Security related to scheduled public events and how the transit system plays a role needs to be addressed. Preparations for activating emergency and contingency plans need to become a higher priority. Additional restrictions for access to facilities may need to be put in place. The status for activities that are required based on the threat information should be communicated to the transit agency's management and other local/regional emergency response organizations, as appropriate.

- **Severe (Red)** – The Severe or Red threat condition represents the highest level of readiness that the transit agency can provide. This threat condition indicates that a severe risk of terrorist activity or an incident or emergency is imminent; however, this does not mean that the transit system is under attack or has an active emergency ongoing. At this threat condition, the transit agency would be expected to activate and deploy the maximum security and emergency preparedness processes, procedures and activities available. This may require significant resource redirection and may include closing facilities (to the public) or discontinuing non-essential activities for the duration of the Red threat condition.

- **Attack or Active Incident** – As stated above, this document also provides suggested protective measures to be implemented at the time that an attack or active incident (or another major emergency such as a natural disaster or accident) has occurred (or is occurring) against a specific transit agency or within the agency's service area, and during recovery from such an attack or active incident. When an attack or incident has actually occurred and transit services have been disrupted, protective measures implemented may have to be responsive to casualties, assisting in evacuations, inspecting

and securing transit facilities and infrastructure, or helping with other tasks as directed by an emergency management authority. It is important to remember that an attack or active incident may occur at any time, even while the transit system is at any of the other lower threat conditions.

- **Recovery** – During the recovery phase, transit agencies will be focused on restoring revenue service, repairing or reopening facilities, adjusting employee work schedules and assignments, responding to customer inquiries about services, and other activities necessary to fully restore transit service. The protective measures implemented during the recovery phase will coexist with the other prevailing threat condition. In other words, service and business recovery will be accomplished while maintaining the prevailing threat level readiness status (e.g., Orange protective measures) in other parts of the transit system's operations.

Color-coded threat information is provided to transit agencies to assist them in implementing protective measures for the appropriate threat condition. Guidance related to establishing the threat condition originates from the United States Attorney General in consultation with DHS. Threat information and guidance is transmitted to DHS' Transportation Security Administration (TSA) and DOT's Federal Transit Administration (FTA) for dissemination to transit agencies. Transit agencies may obtain threat information from other sources such as the FBI joint terrorism task force (JTTF), local law enforcement, emergency management organizations, or other state and local authorities. Each transit agency is responsible for determining the appropriate responses based on an assessment of the guidance received from all sources and the responses of local and regional jurisdictions within the transit agency's service area.

The threat condition established by DHS and the Attorney General is based on intelligence and threat information that may be gathered from a variety of sources. Threat information may be general in nature, or applicable to specific regions of the country, specific cities, transit agencies' specific modes (e.g., commuter rail, subway, or bus), or specific facilities (e.g., transit centers, stations, control centers). Transit agency response may vary depending on the nature of the information. For example, threat information focused on the northeastern region of the country may dictate that transit agencies in that region maintain a higher response than other regions of the country. If the information is modal-based, for example a threat to subways, transit agencies that operate subways may need to maintain a higher preparation level than agencies without subways. In fact, large multi-modal transit agencies may operate their different modes with different protective measures being implemented.

A transit agency is responsible for determining the appropriate threat condition for the transit agency's operation. The threat condition at a transit agency may be determined to be higher or lower than the current national threat condition suggested by DHS. For example, a major sporting event or high-profile convention occurring in the transit agency's service area may cause the transit agency to heighten its threat condition regardless of the threat condition for the rest of the nation.

(2) Protective Measures: Concepts

Protective measures were introduced as part of the Homeland Security Presidential Directive 3 (HSPD-3, March 2002). These protective measures were described alongside the HSAS threat conditions and defined as actions that reduce vulnerability or increase response capability. With this in mind, this document is focused on protective measures for transit agencies based on the HSAS threat conditions. The approach provided in this document is intended to be an "all hazards" approach that includes integration of the HSAS threat conditions with the transit agency's existing security and emergency management programs[6]. In addition, planning and preparing for each HSAS threat condition may necessitate that the transit agency significantly enhance or refresh its security and emergency management plans, procedures, training, drills and exercises.

This technical resource is not prescriptive. It is intended to provide a list of potential protective measures that a transit agency may want to employ. Some of the protective measures may not be appropriate for all transit agencies or for all modes operated (bus, rail, paratransit, etc.). Furthermore, this information has been provided with the recognition that there is an economic impact for the implementation of these protective measures and the transit agency will need to account for the resources required to execute them. This recognition of costs must include implementation as well as costs for the duration of any given threat condition. The responsibility of a transit agency is to deploy the best plans, processes, equipment and infrastructure upgrades and procedures that its current budget allows; and to prioritize additional identified improvements through its planning processes.

This approach to security and emergency management is systematic and is intended to reduce vulnerabilities, detect and deter potential attacks or other criminal activities, respond to active incidents or emergencies, and mitigate the consequences of an incident or emergency. As background, the following definitions are provided:

- ***Vulnerability*** – a weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.
- ***Deterrence*** – an activity, procedure, or physical barrier that reduces the likelihood of an incident, attack, or criminal activity.
- ***Detection*** – the identification and validation of potential threat or attack that is communicated to an appropriate authority that can act.
- ***Response*** – activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.
- ***Mitigation*** – activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences or an incident.

[6] Transit agencies should reference the National Infrastructure Protection Plan, National Response Plan (http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf), National Incident Management System (http://www.fema.gov/pdf/emergency/nims/nims_doc_full.pdf), and Incident Command System.

Reducing vulnerabilities and improving deterrence, detection, response, and mitigation are the foundation of the U.S. Policy on Counterterrorism as defined in Presidential Decision Directive 39 (PDD-39)[7]. This directive has also been updated to include strategies for computer security and other security-related activities in PDD-62[8]. Both PDD-39 and PDD-62 are classified; however, portions of both of these directives have been unclassified and are available on the internet. HSPD-7, titled "Critical Infrastructure Identification, Prioritization, and Protection", establishes a national policy for identifying and prioritizing critical infrastructure and key resources and to protect them from terrorism[9].

Knowledge of the threat type can allow concentration on strategies that are most appropriate for the specific threat. Specific threat types have different capacities for harm as illustrated by the historical exposure rate shown in Table 1.

Table 1. Specific Threat Types and Historical Exposure Rate

Specific Threat Type	Historical Exposure Rate per Incident (People Affected)
Chemical	5,000
Biological	1,500-5,000
Radiological	1,500-5,000
Explosives/ Incendiary	50-3,000 (WTC/Madrid/London/Mumbai)
Nuclear	50,000
Fire Arms/ Armed Assault	10-100
Hijack/ Hostage	10-100
Cyber/ Information Security	unknown

Source: multiple sources including the Mineta Transportation Institute

The most effective deterrence to a terrorist attack or other criminal activities/emergency condition on the transit system is based on a comprehensive set of security activities. This set of security activities, typically called "good housekeeping," is the basis for the FTA/DHS Security and Emergency Management Program Action Items for Transit Agencies: http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20/default.asp.

For non-specific threats, a transit agency must be prepared for the occurrence of all possible incidents/events or emergency circumstances that could disrupt transit services. Prioritizing the preparation for the potential occurrence of incidents and emergencies should be based on the

[7] PDD-39, U.S. Policy on Counterterrorism, June 21, 1995.

[8] PDD-62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998.

[9] HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003.

ongoing transit agency security vulnerability/risk assessment (SVA). This prioritization can help the transit agency manage and reduce vulnerabilities and risk.

Table 2 contains brief descriptions of protective strategies and their principal role in deterring, detecting or responding to criminal or terrorist activities, or mitigating the consequences resulting from the occurrence of these types of criminal activities or emergency incidents/events. Protective strategies are built through the use of protective measures, which are planned and executed by the departments within a transit agency. Since the protective strategies focus on providing deterrence against criminal or terrorist activities, most of the protective strategies have value for all types of threats and the occurrence of disruptive incidents/events within the area served by the transit system.

As part of the preparation of this document, an analysis of whether or not there would be different threat deterrence or strategies for the different threat types was conducted. The results of this work are shown in Table 3, and indicate very little difference exists in deterrence activities by threat type, except for cyber-security threats. The protective strategies that are intended to deter one threat type are generally effective in deterring all threat types.

While the strategies differ little by threat type, the indicators of an actual incident may differ substantially depending on the type of threat device employed in the incident/event. These indicators and the immediate actions necessary to protect transit passengers, employees, and property are important elements in the transit agency's security awareness and emergency response planning, awareness training, and drill/exercise programs and activities.

Immediate Actions (IAs)[10] is an important topic that FTA developed as a technical resource for transit agencies to use in preparing employees to react promptly and properly to suspicious activities, imminent threats, and actual attacks including those that employed WMD devices.

The process described in this guidance document is consistent with FTA's "Public Transportation System Security and Emergency Preparedness Planning Guide"[11]. For a transit agency to be prepared for security and emergency management, three major activities must be established in an ongoing fashion:

- Plans and procedures must be created and kept up to date
- Training materials must be created, disseminated, and updated on a regular basis
- Exercises must be conducted and critiqued to verify the ability to act according to the plans and procedures and based on the associated training

[10] FTA, "Immediate Actions (IAs) for Transit Agencies for Potential and Actual Life-Threatening Incidents," December 2003

[11] FTA, "The Public Transportation System Security and Emergency Preparedness Planning Guide," January 2003

Table 2. Protective Strategy Descriptions

Strategy	Protective Topic	Strategy Description (examples)
Deterrence and Detection	Intelligence/Information Sharing/Cooperation	Understanding threats, working as a team with local planners, law enforcement, and first responders.
	Access Control (perimeter and physical security)	Control of nonpublic places, locks & keys, identification badges, security patrols, visitors escorted.
	Screening	Background checks of employees, contractors, vendors and others with regular access.
	Training/Drills/Immediate Actions	Practicing how to deter, detect, respond, mitigate, and recover.
	Public Address System and Signage	Educating passengers and public of safe actions to take; safety and security awareness information; instructions in emergency situations.
	Surveillance with Force Response	Watching for suspicious activity, items out of place, packages, or other items – directly or from a remote location.
	High Visibility Patrols	Uniformed security patrols and postings, uniformed employees, reflective vests on all employees.
	Sweeps/Inspections	Looking for suspicious items, packages, on a regular or random schedule.
	K-9 Teams	Support for sweeps, inspections; aid for specific types of items; high visibility.
	Alter Operations	Changing regular routines or patterns, preparation for specific duties such as evacuation.
	Alarms with Force Response	Support to access control, intrusion awareness; possibly alert of an event in progress.
	Lighting	Support for inspections, patrols, passenger and employee awareness, deterrence for covert acts.
	Remote Sensors with Force Response	Support to surveillance and inspections; possible identification and alert of a specific type of event in progress.
Response	Evacuation and Assembly/Lockdown and Shelter in Place Capability	Life safety measure; protection of employees, passengers, and others until qualified responders arrive or until safe to evacuate.
	Control of HVAC Systems and Air Vents	Protecting against introduction or dispersal of hazardous materials in critical areas or in vehicles.
	Force Response	Supporting detection and reporting of threats/attacks. Attack may be deterred if in planning stages, defeated or consequences mitigated if in final active stage.
Mitigation	Fire Suppression Equipment	Mitigating or controlling the impact of an event in progress.
	Signage, Public Address and other Emergency Information	Promote an organized and safe response to an attack situation.
	Personal Protective Equipment	Protection for first responders; escape protection for employees.
	Decontamination	Reducing the consequences of attack; facilitating recovery of equipment and facilities.
	Mitigation Equipment	Reducing the impacts of attack; also deterrence.

Table 3. Protective Topics for Specific Threat Types

Protective Topics	Specific Threat Type							
	Chemical	Biological	Radiological	Explosives/ Incendiary	Nuclear	Fire Arms/ Armed Assault	Hijack/ Hostage	Cyber/ Info Security
Intelligence/Information Sharing/ Cooperation	X	X	X	X	X	X	X	X
Access Control	X	X	X	X	X	X	X	X
Screening	X	X	X	X	X	X	X	X
Training/Drills/ Immediate Actions	X	X	X	X	X	X	X	X
Public Address System and Signage	X	X	X	X	X	X	X	
Surveillance	X	X	X	X	X	X	X	X
High Visibility Patrols	X	X	X	X	X	X	X	
Sweeps/Inspections	X	X	X	X	X	X	X	
K-9 Teams			X	X		X	X	
Alter Operations	X	X	X	X	X	X	X	
Alarms	X	X	X	X	X	X	X	X
Lighting	X	X	X	X	X	X	X	
Remote Sensors	X	X	X	X	X			
Evacuation and Assembly/Lockdown and Shelter in Place Capability	X	X	X	X	X	X	X	
Control of HVAC Systems and Air Vents	X	X	X	X	X	X	X	
Fire Suppression Equipment	X	X	X	X				
Personal Protective Equipment	X	X	X	X	X	X	X	
Decontamination	X	X	X		X			
Mitigation Equipment			X[a]	X[a]			X[b]	

a. Explosive resistant container is an example of mitigation equipment for this threat.

b. Road spikes or stop strips are examples of mitigation equipment for this threat.

During the conduct of each of these three activities, knowledge is gained that affects the other activities as shown in Figure 2. The use and update of these three activities for security and emergency management (plan, train, and exercise) is a continuous process that can help a transit agency get prepared and stay prepared.

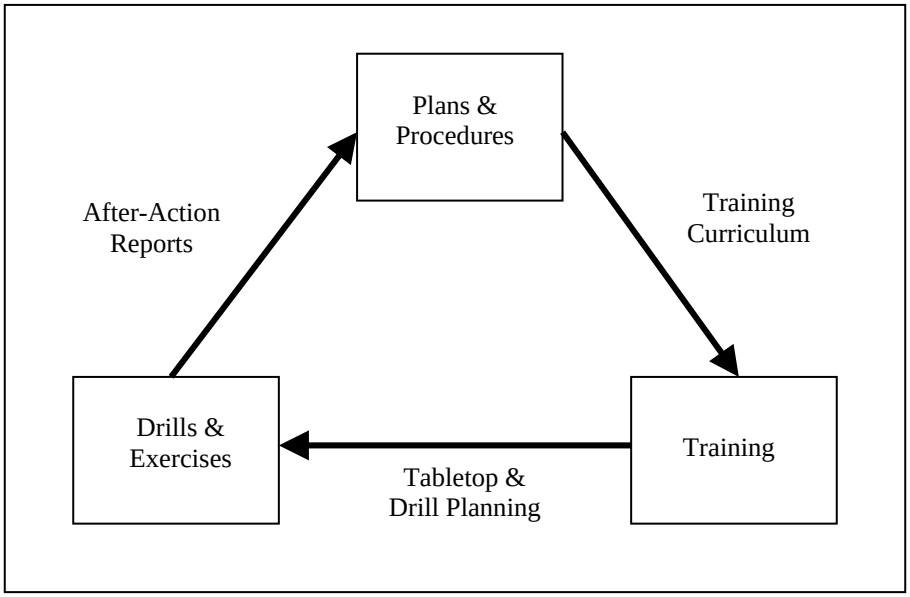


Figure 2. Relationships of Plans and Procedures, Training, and Drills and Exercises

(3) Protective Measures: Implementation Process

The general implementation process for integrating HSAS threat conditions into a transit agency's security and emergency management program starts with a review of the protective measures. ***Protective measures*** (PMs) are the preventive and tactical actions taken to reduce vulnerabilities, deny an adversary opportunity, or to increase response capabilities. The objective of this general implementation process is to integrate the HSAS threat conditions with a transit agency's security and emergency management program using an applicable subset of all the protective measures provided in this document (and additional protective measures as needed).

Protective measures are organized by transit agency security and emergency management function as the basis for developing and deploying specific implementation procedures. The provided lists of protective measures are candidate actions, not requirements. Specific implementation procedures and processes should be determined by a transit agency in light of its local and regional needs, conditions, capital and operations budgets and operating environment. This list of protective measures is not intended to be exhaustive and not all of these protective measures may be appropriate for every transit agency. The list is provided as a starting point for the process.

Protective measure implementation should be prioritized based on an analysis of the transit agency's specific vulnerabilities, intelligence information, potential consequences and remedial costs. Similar to the relationship of plans and procedures, training, and drills and exercises (Figure 2), the protective measures implementation process for a transit agency has been set up as a continuous process through a feedback loop, as shown in Figure 3. There are several inputs to the process including:

- TSA Rail Security Directives (SDs): RAILPAX-04-01
- Standard and emergency operating procedures (SOPs/EOPs)
- Security Vulnerability Assessments
- Threat information provided by Department of Homeland Security (DHS)
- Technical resources from the Transportation Security Administration (TSA), Office of Grants and Training (OGT) and Federal Transit Administration (FTA)
- Emergency and contingency operations plans
- Additional protective measures provided in this guidance document

The transit agency protective measures implementation process should produce, as output, a plan and/or procedural handbook that includes:

(1) A checklist of protective measures to be implemented for each HSAS color-coded threat level (and the Attack or Active Incident and Recovery conditions)

(2) A procedure or protocol for communicating the transit agency's HSAS protective measures plan (including notifying employees, coordinating with industry stakeholders and informing the media whenever the threat level is increased or decreased)

(3) A schedule for conducting HSAS threat level employee training and testing (tabletop exercises and regional drills)

The protective measures implementation process is iterative and intended to help improve security and emergency management programs at a transit agency, using the HSAS color-coded threat conditions as an organizational framework. The iterative process is accomplished through the feedback loop shown in Figure 3; it includes the following inputs:

- Documented experience and knowledge from actual operation during higher threat conditions
- Documented experience from drills and exercises based on scenarios with higher threat conditions (after-action reports)
- Periodic audits, reviews and updates of security and emergency management plans
- Lessons learned from security and emergency management forums, such as the FTA/DHS Connecting Communities Forums

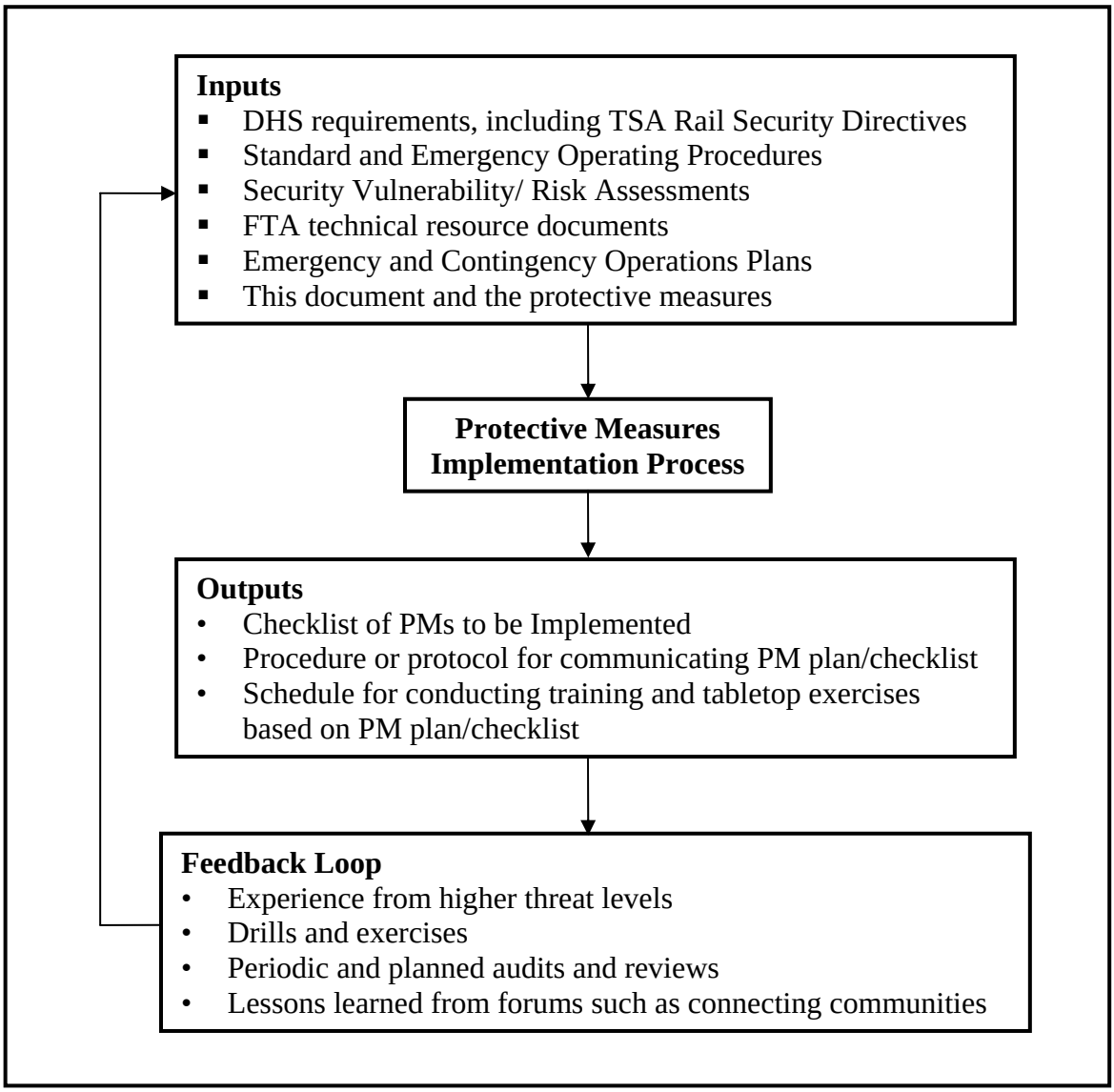


Figure 3. General Protective Measures Implementation Process

Appendix B provides a list of the suggested protective measures, which are categorized into six functional areas, as shown in Table 4. Each protective measure is assigned to one of the specific color-coded threat and response conditions, so that the connectivity of multiple protective measure activities can be seen and utilized.

Table 4. Categories of Protective Measures

Section/Category	Scope
1.0 Information & Intelligence	Information & intelligence gathering includes threat and vulnerability information collection and analysis, sharing information with and getting information from local, regional and federal sources such as DHS and the FBI
2.0 Security and Emergency Management	All aspects of creating, updating, and executing the security and emergency management plans and procedures for the transit agency
3.0 Regional Coordination	Participation of the transit agency in the region, including regional emergency response plans, relationships with other security-related organizations in the region and first responders, and conducting regional drills and exercises
4.0 Information Technology and Communications Systems	All aspects of creating, updating, and executing the information system plans and monitoring and operating the communications equipment for the transit agency
5.0 Employee and Public Communications	All aspects of creating, updating, and executing the employee and public information communications plans for the transit agency
6.0 Contingency and Continuity Plans	All aspects of creating, updating, and executing the transit agency's contingency and continuity of operations plans for emergency incidents/events within the transit system and in the region

This approach presented here is not required by FTA and is provided only as a technical resource document. In preparation for emergency operations, most transit agencies have already completed a process similar to the one described here. This information is being provided to help ensure that the process used at transit agencies is systematic and thorough. At a minimum, a transit agency should review the material in this report to ascertain if its use would benefit or add value to existing processes.

It is important to remember that once this process starts, the information that is discussed and collected will most likely be categorized as ***sensitive security information (SSI)***[7] and will need to be controlled and protected from inappropriate disclosure outside of the transit system.

[7] – FTA/DHS Security and Emergency Management Action Item #16, http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20

Appendix C provides a more detailed implementation process that transit agencies may be interested in using. The process in Appendix C provides a more robust, systematic approach that includes:

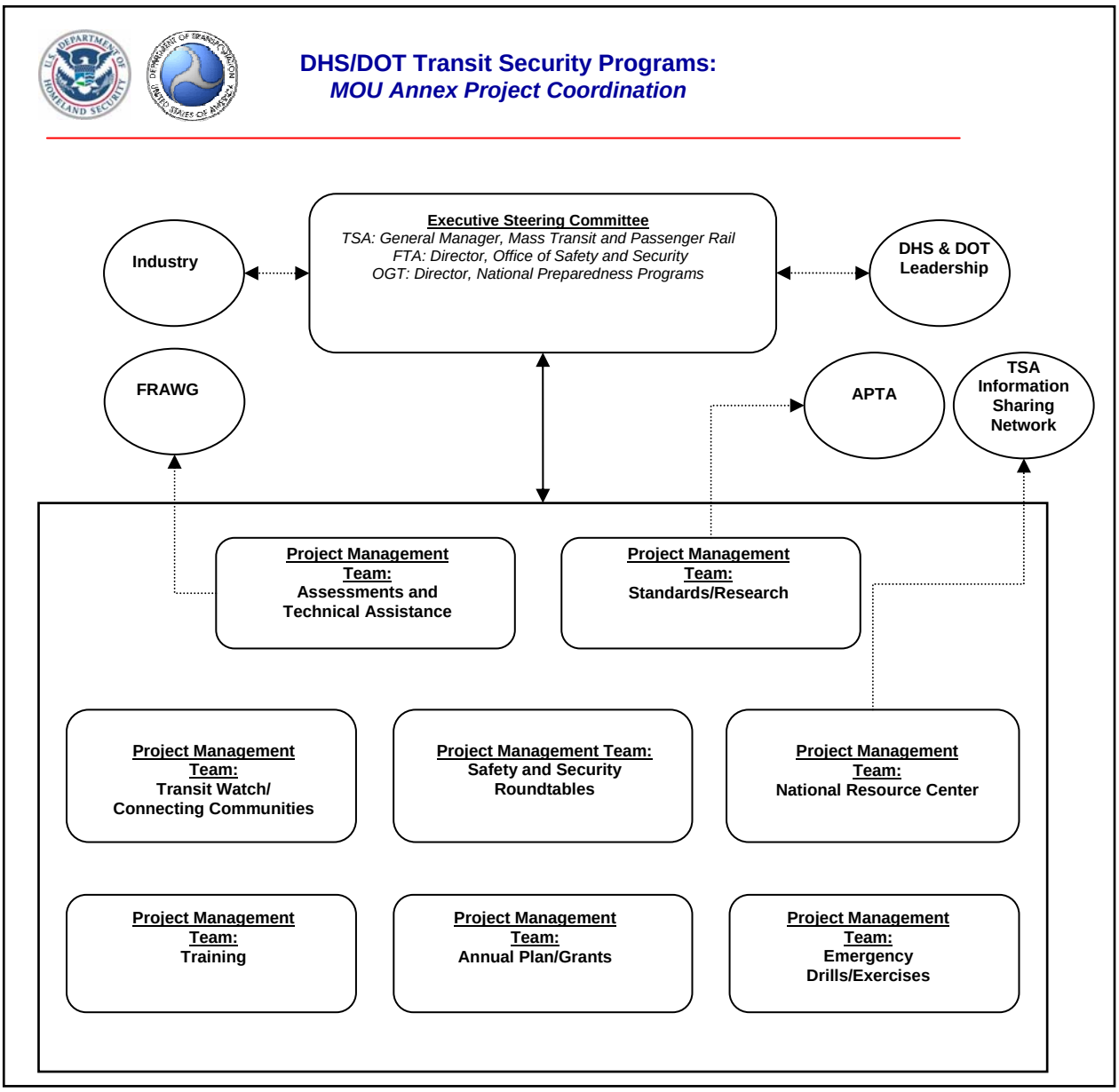
- An agency-wide assessment of existing security and emergency management capabilities
- Assigning individual departments responsibilities for implementing specific protective measures
- Prioritizing any resource needs emanating from the capabilities assessment
- Developing a database for tracking and communicating protective measure activities
- Conducting employee training/workshops and testing (tabletop exercises/drills) on the process

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

Schematic Representation of the Public Transportation Security MOU Annex

THIS PAGE INTENTIONALLY LEFT BLANK


DHS/DOT Transit Security Programs:
MOU Annex Project Coordination
Executive Steering Committee
TSA: General Manager, Mass Transit and Passenger Rail
FTA: Director, Office of Safety and Security
OGT: Director, National Preparedness Programs
Industry
DHS & DOT Leadership
FRAWG
APTA
TSA Information Sharing Network
Project Management Team: Assessments and Technical Assistance
Project Management Team: Standards/Research
Project Management Team: Transit Watch/ Connecting Communities
Project Management Team: Safety and Security Roundtables
Project Management Team: National Resource Center
Project Management Team: Training
Project Management Team: Annual Plan/Grants
Project Management Team: Emergency Drills/Exercises

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

Suggested Protective Measures

THIS PAGE INTENTIONALLY LEFT BLANK

Security and Emergency Management Protective Measures for Transit Agencies

This appendix provides the entire list of suggested security and emergency management protective measures for transit agencies organized into six categories as listed in the following table. Protective measures are organized by transit agency security and emergency management function as the basis for developing and deploying specific implementation procedures. The provided lists of protective measures are candidate actions, not requirements. Specific implementation procedures and processes should be determined by a transit agency in light of its local and regional needs, conditions, capital and operations budgets and operating environment. This list of protective measures is not intended to be exhaustive and not all of these protective measures may be appropriate for every transit agency. The list is provided as a starting point for the process.

Table B-1. Categories of Suggested Protective Measures

Section/Category	Scope
1.0 Information & Intelligence	Information & intelligence gathering includes threat and vulnerability information collection and analysis, sharing information with and getting information from local, regional and federal sources such as DHS and the FBI
2.0 Security and Emergency Management	All aspects of creating, updating, and executing the security and emergency management plans and procedures for the transit agency
3.0 Regional Coordination	Participation of the transit agency in the region, including regional emergency response plans, relationships with other security-related organizations in the region and first responders, and conducting regional drills and exercises
4.0 Information Technology and Communications Systems	All aspects of creating, updating, and executing the information system plans and monitoring and operating the communications equipment for the transit agency
5.0 Employee and Public Communications	All aspects of creating, updating, and executing the employee and public information communications plans for the transit agency
6.0 Contingency and Continuity Plans	All aspects of creating, updating, and executing the transit agency's contingency and continuity of operations plans for emergency incidents/events within the transit system and in the region

Suggested Protective Measures

1.0 Information and Intelligence

Seq No	Protective Measure	Action Required
1.1	Develop and implement a threat and vulnerability assessment process to assure that (a) all transit system facilities, support systems, and surrounding areas are regularly assessed for security threats, including terrorist attacks, and vulnerabilities, and (b) all reasonable measures are identified to mitigate these vulnerabilities.	
1.2	Establish priorities for protective measures and mitigation; Organize measures into specific actions to be taken at the appropriate threat condition	
1.3	Establish contact information with local and regional law enforcement and security intelligence units, state and federal regional offices	
1.4	Identify available security planning informational resources such as the FTA's website	
1.5	Develop, disseminate, and implement procedures for employees receiving information (e.g., phone calls, e-mails) that threaten harm to the transit system, employees, or customers	
1.6	Designate a primary and an alternate Security Coordinator (SC) and provide their contact information to the Transportation Security Administration (TSA). Immediately notify TSA (sd.masstransit@dhs.gov) of changes in SCs or contact information, e.g., telephone number(s)	RSD #1: Notification to TSA required for rail operators, per TSA SD Railpax-04-01
1.7	Designate responsibilities of primary and alternate SCs to: (a) serve as the transit agency's primary and immediate contact for intelligence information, security-related activities, and communications with TSA; (b) be available to TSA on a 24-hour basis; (c) review, as appropriate, all security-related functions to ensure they are effective and consistent with rail passenger security measures, including TSA's SD Railpax-04-01; (d) upon learning of non-compliance with TSA-required security measures, immediately initiate corrective action; (e) coordinate implementation of security measures with other organizations involved in security operations, including but not limited to, third party owners of rail passenger stations and freight railroads hosting the operations of parties to which TSA SD Railpax-04-01 applies. This includes follow up reporting on federal inquiries.	RSD # 2: Notification to TSA required for rail operators, per TSA SD Railpax-04-01
1.8	Report threats and security concerns to law enforcement authorities and to TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov	RSD # 3. Reporting to TSA required for rail operators, per TSA SD Railpax-04-01
1.9	Via e-mail to sd.masstransit@dhs.gov, notify TSA of the date of the most recent vulnerability assessment. Provide TSA access to the vulnerability assessment and corresponding security plan (if available). If no vulnerability assessment has been conducted, so advise	RSD # 4: Notification to TSA required for rail operators, per TSA SD Railpax-04-01

1.0 Information and Intelligence (cont.)

Seq No	Protective Measure	Action Required
1.10	Network with local and regional law enforcement and security intelligence units, Joint Terrorism Task Force, and the area TSA Federal Security Director or Surfact Transportation Security Inspector for assessments of current and security-related information.	
1.11	Review/re-issue procedures for employees reporting threatening communications (e.g., phone calls, e-mails)	
1.12	Include intelligence information in roll-call briefings of security and law enforcement units	
1.13	Review security vulnerability assessments and update regularly or whenever a new asset (i.e., a new facility such as an administrative building, bus depot, rail yard, or new type of revenue service) is added.	
1.14	Include security in special event planning to identify any unique requirements	
1.15	Join/participate in FBI Joint Terrorism Task Force (JTTF), Surface Transportation Information Sharing and Analysis Center (ST-ISAC) and Homeland Security Information Network (HSIN).	
1.16	Actively seek relevant intelligence with DHS, FTA, JTTF, ISAC, HSIN, state and local authorities, and other transit agencies.	
1.17	Assess the threat's characteristics. Determine the additional Protective Measures required.	
Active Incident		
1.18	Advise TSA via the TSOC (1-703-563-3237 or TSOC.ST@dhs.gov) immediately of all known information regarding the nature of the attack so that TSA can provide assistance and immediately disseminate the information to other transit and governmental agencies.	
1.19	Identify attacker(s) to law enforcement and security personnel. As appropriate, use witnesses or surveillance for timely and relevant information.	
Recovery		
1.20	Guard against secondary attacks	
1.21	Coordinate with external intelligence and information agencies to return to the appropriate HSAS threat level condition	
1.22	Prepare an After Action Report - Determine circumstances that led to successful attack. Evaluate response performance. Identify and implement corrective measures. Document actions and lessons learned	

2.0 Security and Emergency Management

Seq No	Protective Measure	Action Required
2.1	Develop system security and emergency response plans and standard and emergency operating procedures. In these plans and procedures, identify the responsibilities of employees by job function. Include preparedness for multiple concurrent events.	
2.2	Establish a security and emergency management team or task force, with designated alternates, that is responsible for implementing procedures appropriate to the emergency condition	
2.3	Review security and emergency management technical guidance on FTA's website	
2.4	Inventory emergency equipment and supplies. Verify that needed quantities at higher HSAS threat level conditions are adequately stocked and/or available	
2.5	Establish priorities for all outstanding maintenance and capital projects that could affect the security of facilities	
2.6	As part of the system security plan, develop and implement access control systems for employees, visitors, facilities, and vehicles. Develop access restrictions that allow for the implementation of recovery plans after an attack or emergency, but that prevent tampering with the incident scene. Implementation of access controls should be incremental in response to changing HSAS threat level conditions	
2.7	As part of the system security plan, develop and implement a document control system to identify and protect sensitive security information.	
2.8	Direct that all personal, transit, and contractor vehicles be secured when not in use	
2.9	Survey areas adjacent to and surrounding transit properties to determine activities that might increase security risks to the transit system (e.g., government buildings, airports, stadiums, convention centers, industrial plants, pipelines, railroads)	
2.10	Develop procedures for shutting down and evacuating facilities and/or the transit system	
2.11	Review/update all plans and procedures to ensure that they provide adequate assistance to employees and customers with disabilities	
2.12	Deploy neighborhood watch personnel, if available, for routine patrols	
2.13	Determine, map, and disseminate emergency evacuation route plans for transit system vehicles	
2.14	Determine and document factors that would require partial or full service shutdown	
2.15	Develop and implement a security and emergency management data collection system consistent with FTA national transit database reporting requirements. Use the system to analyze incidents and trends. Control sensitive security information per document control system (see sequence number 2.7)	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.16	Perform background checks on all employees and on contractors consistent with applicable law	
2.17	Apply concepts of crime prevention through environmental design (CPTED) in reviews of facilities and in new designs and modifications	
2.18	Insure transit agency employees have visible identification (and uniforms for designated job categories); and that on-site contractors and visitors are identifiable by an appropriate identification system, such as badges.	
2.19	Develop and implement policies and procedures for a key control management/inventory system	
2.20	Develop the procedure for a full inspection of public and non-public facilities including lockers and storage areas at higher threat conditions.	
2.21	Train all employees in security awareness, response plans, and individual roles and responsibilities.	
2.22	Train all employees on the Homeland Security Advisory System (HSAS) and on specific Protective Measures that the agency will implement at higher HSAS threat level conditions	
2.23	Plan and provide policing and security appropriate to DHS threat levels and threat advisories	RSD # 14: Action is required for rail operators, per TSA SD Railpax-04-01
2.24	Conduct emergency drills and exercises that include employees and customers with disabilities	
2.25	Develop training and testing to assess employee proficiency (e.g., table top and field drills with outside responders). Base training and testing, in part, on FTA's "Immediate Actions for Transit Agencies" guidance. For all table top and field drills, include a process for system improvements based on after action reports	
2.26	Participate in regional drills and exercises to support the response to attacks or other emergencies, such as natural disasters	
2.27	Insure that existing physical security and emergency measures (e.g., fencing, lighting, locks) are in good working order and adequately maintained. Conduct regular tests of security and emergency management equipment (e.g., emergency generators, communication and notification systems, surveillance and intrusion detection systems). Repair/replace any defective equipment.	
2.28	Insure coordination between the safety and the security departments (e.g., emergency procedures are regularly reviewed and updated as needed by a safety management team)	
2.29	Inspect all mail and package deliveries. Examine mail and packages for letter/parcel bombs and suspicious substances. Do not open suspicious letters or packages	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.30	Maintain accurate records for tracking all identification cards, badges, decals, and uniforms. Cancel access for any items lost or stolen. Require uniform vendors to verify identities of individuals seeking to purchase uniform articles	
2.31	Conduct immediate inventory sweep for all revenue and non-revenue vehicles, including contingency/spare vehicles. Search for any missing vehicles	
2.32	Immediately re-check all security systems (e.g., lighting, CCTV, and intrusion alarms). Install additional, temporary lighting if needed to provide desired lighting for key areas (e.g., underground stations, transit centers, rail yard and bus garage perimeters).	
2.33	Physically audit (at supervisory level)/enforce positive identification of all personnel. Make no exceptions.	
2.34	Identify and train employees who can assist as drivers of transit vehicles during emergencies	
2.35	Insure coordination between the security department and the operations and maintenance departments (e.g., jointly develop and approve standard operating procedures)	
2.36	Confirm availability of outside security resources to assist with intensified or increased span of coverage during peak periods	
2.37	Increase special patrols (e.g., foot patrols, bicycle patrols) and on-board vehicle patrols as appropriate.	
2.38	Reduce the number of access points for vehicles and personnel to minimum levels. Spot check contents of vehicles at access points. Watch for vehicles parked for long periods of time in or near any facility. Lock doors and check that all designated locked doors remain locked.	
2.39	Conduct frequent inspections of facilities, stations, terminals, and other critical assets, including public storage areas, for persons and items that do not belong.	RSD # 12: Action is required for rail operators, per TSA SD Railpax-04-01
2.40	At regular intervals, inspect each passenger vehicle for suspicious or unattended items.	RSD # 13: Action is required for rail operators, per TSA SD Railpax-04-01
2.41	If equipped with locking mechanisms, lock all doors that allow access to the engineer's or operator's cab or compartment. The TSA SD is not intended to supersede safety regulations concerning locking of certain types of doors on cards under DOT/FRA/FTA regulations.	RSD # 15: Action is required for rail operators, per TSA SD Railpax-04-01
2.42	Elevate the priority of security maintenance and repairs such as perimeter fencing, lighting, facility locks, and access points	
2.43	Limit visitor access to critical security areas. Confirm that visitors are expected and have a valid need to be in the area	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.44	Change appearance (e.g., orange/yellow vests) and patrol deployment strategies to disrupt terrorist planning	
2.45	Alert vendors and contractors to heighten security awareness and report suspicious activity. Inform vendors and contractors about heightened control measures, including access, parking, and identification	
2.46	Increase security spot checks of persons (employees, contractors and visitors) entering non-public facilities, including confirming identification and randomly checking bags	
2.47	Secure all buildings and storage areas not in regular use. Increase frequency of inspections and patrols in these areas	
2.48	Increase surveillance of critical infrastructure areas (e.g., control and communication centers, loading docks, parking lots and garages, bridges, tunnels, rights-of-way)	
2.49	Check designated unmanned and remote sites more frequently for signs of unauthorized entry, suspicious packages, and unusual activities	
2.50	Check all deliveries to facility loading docks to insure that the items received are as ordered and expected. Refuse any unexpected deliveries	
2.51	For passenger stations with identified, significant risks, to the extent practicable, remove trash receptacles and other non-essential containers, except for bomb-resistant receptacles and clear plastic containers. Install bomb-resistant receptacles to the extent that resources allow.	RSD # 8: Action is required for rail operators, per TSA SD Railpax-04-01
2.52	Use explosive detection canine teams, if available.	RSD # 9: Action is required for rail operators, per TSA SD Railpax-04-01
2.53	At any time or place, allow TSA-designated canine teams to conduct operations under the overall direction of the authority responsible for security of the transit property or operator.	RSD # 10: Action is required for rail operators, per TSA SD Railpax-04-01
2.54	At any time or location, allow TSA/DHS-designated Security Partnership Teams to work with the transit agency's Security Coordinator to perform inspections, evaluations, or tests, including copying records, for Security Directive Railpax-04-01	RSD # 11: Action is required for rail operators, per TSA SD Railpax-04-01
2.55	Review standard operating procedures for heating, ventilation, and air conditioning (HVAC) operations in various emergency conditions	
2.56	Maintain respiratory protection equipment immediately available to law enforcement and operations personnel while they are in the field	
2.57	Increase the frequency with which law enforcement/security personnel perform ad hoc security checks and sweeps of transit vehicles at ends of lines	
2.58	Consider random screening of passengers' bags, backpacks, briefcases, suitcases, etc. at station entrances. Provide overt warning to potential passengers prior to their entering stations.	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.59	Review procedures and prepare to establish/activate the Command Center(s). Prepare to dispatch Mobile Command Centers in the event of an actual emergency. Prepare to initiate the incident command system	
2.60	Put the Emergency Operations Center [EOC] on 'Stand-By' status with all systems operational. Verify that all systems are functioning	
2.61	Increase security postings and patrols to maximum sustainable levels	
2.62	Increase inspections of public storage areas, including bike and bag lockers	
2.63	Close and lock all gates and barriers except those needed for immediate entry and exit. Inspect perimenter fences on a frequent basis.	
2.64	Restrict visitors to essential business purposes. Require positive identification and inspect suitcases, packages, and other articles of significant size	
2.65	Limit access to designated facilities to personnel with a legitimate and verifiable need to enter.	
2.66	Implement higher threat level sweep and inspection procedures for transit vehicles in and out of facilities, and continue driver inspections of vehicles. Increase ad hoc security checks and sweeps of transit vehicles in revenue service (i.e., during revenue trips) by law enforcement/security personnel.	
2.67	Relocate authorized parked vehicles away from stations, terminals, and other critical buildings or areas, if possible. Consider implementing centralized parking and employee shuttle buses. Remove unauthorized parked vehicles	
2.68	Place backup/offsite operations control center on standby status. Test/verify its capability/readiness	
2.69	Erect barriers and obstacles to control traffic flows and protect stations, terminals, and other facilities and critical infrastructure from attack by parked or moving vehicles. Consider using company vehicles as barriers	
2.70	Increase presence/visibility of security and law enforcement personnel through consistent appearance (e.g., all patrols and posted security wearing vests, transit police in full uniform)	
2.71	Protect onsite or adjacent auxiliary facilities and services (e.g., day care center, homeless shelter, food service vendor) consistent with the agency's protective measures	
2.72	Postpone all non-vital construction work performed by contractors, or continuously monitor their work with agency personnel	
2.73	Limit administrative employee travel	
2.74	Close all public restrooms in underground stations	
2.75	Require service workers to empty trash receptacles more frequently	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.76	Review security camera stored disks/tapes to detect possible indicators of pre-operational surveillance.	
2.77	Monitor and inspect elevators more frequently	
2.78	Increase the frequency of late night/overnight security sweeps and inspections of key right-of-way infrastructure elements (e.g., underground rail lines, electrical substations)	
2.79	Implement transit emergency plans and procedures. Assign emergency response personnel, pre-position resources, and mobilize specially trained teams	
2.80	Activate the transit system's EOC	
2.81	Implement 100% sweep and inspection procedures for transit vehicles in and out of facilities in addition to the driver inspections. Implement 100% security inspection at out-of-service stops	
2.82	Augment security forces to ensure control of key command, control, and communications centers and other potential target areas. Establish surveillance points and reporting procedures	
2.83	Maximize patrols in areas without stationed security personnel. Conduct frequent checks of building exteriors and parking areas	
2.84	Implement surveillance in support of guarded and patrolled areas	
2.85	Reduce facility access points to an operational minimum and restrict access to essential personnel.	
2.86	At facility access points, inspect 100% of employee, contractor, and visitor briefcases, suitcases, bags, and other articles	
2.87	Minimize/eliminate administrative employee leave/travel	
2.88	Close visitor and employee parking lots, as appropriate	
2.89	Disable and lock out public storage areas such as bike and bag lockers	
2.90	Physically verify that vehicle gates, garage and building doors, and other gates and doors designated to be closed and locked at the "red" threat level are actually closed and locked	
2.91	Close all non-essential functions (e.g., sales offices, neighborhood outreach offices, onsite day care facilities)	
2.92	Transfer/deliver all mail and packages to a central remote location for inspection	
2.93	Close all public restrooms	
2.94	Consider implementing temporary revenue service restrictions and/or re-routes associated with serving higher-risk targets/icons (e.g., military bases, stadiums, convention centers)	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.95	Consider restricting or suspending bicycle transport (e.g., not allowing bicycles with bags or backpacks affixed to them to be carried on vehicles)	
2.96	Remove all non-explosive resistant trash cans (except clear plastic containers) at passenger facilities.	
2.97	Deploy on-duty vehicle cleaners to terminal stations during peak revenue hours. Remove or secure unattended newspaper vending machines in selected locations	
2.98	When operators exit their vehicles at an end-of-line layover point, require all riders to de-board. Secure/lock the vehicle. When operators return to vehicles, require them to conduct a sweep before allowing riders to board/re-board	
2.99	Staff backup/offsite operations control center. Prepare to assume control from primary operations control center if needed	
2.100	Perform Immediate Actions (IAs) for suspicious activities and imminent threats as necessary	
Active Incident		
2.101	Perform Immediate Actions (IAs) for attacks as necessary	
2.102	Designate the incident commander. Activate and operationalize the EOC. Implement emergency operating procedures to mitigate the effects of the attack	
2.103	Provide security for the site and other transit system assets during the emergency. Be alert for possible secondary attacks	
2.104	Mobilize and provide transit assets (communications links, equipment, facilities and personnel) in support of the overall response effort	
2.105	Assess immediate impacts of the attack on transit service and facilities, and reduce or cancel services as required	
2.106	Assist with response to casualties, as needed/requested	
2.107	Restrict/eliminate access to facilities by contractors, vendors, and visitors. Accept deliveries on a case-by-case basis only	
2.108	Position/park vehicles to block entrances to facilities, as appropriate	
2.109	Review security camera stored disks/tapes for operational activity.	
2.110	Provide security for the incident site. Allow access to incident area only to security, mitigation, and investigating personnel. Other access restrictions should allow the implementation of recovery plans, but prevent tampering with the incident scene until fully released	
2.111	Activate "on-call" external contractors and other special support, as required	
2.112	Implement plans to return to the appropriate threat level ("green" through "red")	

2.0 Security and Emergency Management (cont.)

Seq No	Protective Measure	Action Required
2.113	Inspect facilities and infrastructure for latent damage before reoccupying facilities or restoring operations	
2.114	Continue secure access control around affected area(s)	
2.115	Identify short and long-term capital replacement needs. Develop plans and detailed designs	
2.116	Recover facilities, infrastructure, and vehicles. Restore transit system capabilities. Restore the scene of attack to functionality	

3.0 Regional Coordination

Seq No	Protective Measure	Action Required
3.1	Participate in development and review of local and regional security and emergency response plans	
3.2	Establish local, regional, and system-wide threat and warning dissemination processes (consistent with federal level information sharing per protective measures in 1.0 Information and Intelligence)	
3.3	Establish emergency communications capability and coordinate notifications to emergency response organizations	
3.4	Coordinate with emergency response agencies (e.g., military, police, fire, HAZMAT, hospitals, federal agencies) to develop support systems to provide post-incident support to customers and employees	
3.5	Establish memoranda of agreement (MOAs) and other mutual aid agreements, as needed, to assure adequate regional emergency response coordination	
3.6	Participate in local and regional security and emergency response training, drills, and exercises. Coordinate transit system's role in local and regional emergency response. Include an after-action report-based process improvement system for all tabletop exercises and drills	
3.7	Coordinate security and emergency response awareness materials for transit employees and the public consistent with other local and/or regional transit agencies	
3.8	Periodically communicate with military, law enforcement units, emergency response organizations, hospitals, and other agencies and organizations (including federal agencies), as appropriate	
3.9	Identify and train other community personnel who can assist as drivers of transit vehicles during emergencies	
3.10	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit agency is at Elevated Condition (Yellow) and advise the protective measures being employed	
3.11	Coordinate emergency preparedness/response plans with nearby jurisdictions	
3.12	Participate in daily/weekly regional briefings	
3.13	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit system is at HSAS condition "orange," and advise them of the Protective Measures being employed	
3.14	Consult with local authorities about control of public roads and access that could make the transit system more vulnerable	

3.0 Regional Coordination (cont.)

Seq No	Protective Measure	Action Required
3.15	Take additional precautions at local and regional public events. Consider alternative venues or postponing or canceling the events.	
3.16	Implement regional emergency plans with nearby jurisdictions. Implement plans to assist in evacuations or respond to emergency management requests	
3.17	Coordinate with local authorities on the possible closing of public roads and facilities and the removal of unattended vehicles	
3.18	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit system is at HSAS condition "red," and advise them of the Protective Measures being employed	
3.19	Implement regional emergency preparedness plans with nearby jurisdictions. Implement plans to assist in evacuations or respond to emergency management requests	
3.20	Deploy liaisons to regional emergency operations centers (EOCs) to participate in unified command	
Active Incident		
3.21	Report the attack immediately to all local, regional, state, and federal emergency response organizations, including TSA's Transportation Security Operation n Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov (including those mentioned in protective measure 1.10)	
3.22	Designate the transit agency Incident Commander, as needed, and activate transit agency's EOC. Provide onsite technical support to the regional EOC's Incident Commander	
3.23	Mobilize and provide transit assets (communications links, equipment, facilities and personnel) to support of the response, as requested by the Regional EOC Incident Commander	
Recovery		
3.24	Coordinate local and regional plans to return to appropriate threat level ("green" though "red")	
3.25	Coordinate funding and other needs for transit system restoration with federal, state, and local agencies	

4.0 Information Technology and Communication Systems

Seq No	Protective Measure	Action Required
4.1	Develop and implement hardware, software and communications security and disaster recovery/business continuity plans and procedures, including (a) data management; (b) access partitions and permissions; (c) external communication links; (d) internal activity monitoring; (e) configuration management (hardware, software, network descriptions and locations); (f) vehicle control systems. Provide for incremental responses to changing threat level conditions. Coordinate with systems security plans. Develop and implement plans for business, operations, and security	
4.2	Inventory existing emergency response infrastructure, equipment, supplies and service contracts, and compare against current requirements. Assign work/prepare purchase orders based on the inventory. Consider: (a) frequency management (e.g., allocation and assignment of frequencies, license renewals, tower capacity); (b) contracts for backup communications systems (e.g., cell phones); (c) procurement and assignment of backup communications systems (e.g., distribution of phones and phone numbers to assigned personnel); (d) interoperability with local and/or regional emergency responder organizations (e.g., update/implementation of frequency management with responder organizations, purchase/acquisition of translation equipment). Purchase and/or install items needed to implement protective measures at higher threat levels	
4.3	Limit transit operations data communications to outbound information only. Install firewalls and DMZ environment. Block or control internet access. Establish private networks	
4.4	Use 'push' technology for anti-virus and software security updates	
4.5	Develop a computer incident response plan and team that includes representatives from various user groups	
4.6	Develop information technology (IT) administrative and operational procedures to identify and respond to IT and communications related incidents in a timely and controlled manner	
4.7	Configure IT infrastructure to provide fault tolerances across physical locations and within a single physical location	
4.8	Secure employee and customer information (e.g., personal information, account data, credit card information) from unauthorized electronic access	
4.9	Assess the impact on transit agency operations if all essential computer system resources (command, control, and financial computer systems) are disconnected from the internet and public access during higher HSAS threat level conditions. Manage external transit fare vending machines so that they cannot be compromised/hacked	

4.0 Information Technology and Communication Systems (cont.)

Seq No	Protective Measure	Action Required
4.10	Perform daily incremental and weekly full backups of electronic data required for security, payroll, scheduling, operations, and business continuity. Transport backup(s) to a secure remote location weekly or more often for critical data. Practice data file restoration on a regular basis, including retrieval from offsite storage and return to offsite storage. Practice full System restoration on an annual or more frequent basis	
4.11	Test primary emergency communications and notification systems. Order maintenance as necessary. Update emergency communications frequencies for interoperability with emergency responders	
4.12	Test the network, servers, databases, and Web servers to ensure that they can handle increasing transaction loads	
4.13	Test to assure that the IT infrastructure is protected against unauthorized manipulation of website applications	
4.14	Test IT systems for single points of failure	
4.15	Secure command, control, and financial IT systems and communication networks from outside tampering	
4.16	Inspect and test all closed circuit television (CCTV), video camera/recording equipment, intercoms, emergency telephones, radios, and satellite communication devices to assure that all communication equipment is in place and operational	
4.17	Update system software (servers, switches, routers, firewalls, DMZs) for Information security protection. Enter all changes into the configuration management system	
4.18	Test/exercise primary and backup communications equipment and procedures with essential personnel to ensure that an agency or facility response can be mobilized appropriate to an incident or increased security requirement	
4.19	Test/exercise external communications equipment and procedures used with designated emergency response or command locations	
4.20	Monitor all digital communications links for security. Test alternate paths	
4.21	Perform daily incremental backups of electronic data required for security, payroll, scheduling, operations, and business continuity. Maintain copies on-site and transport backup(s) to secure remote location	
4.22	Develop and implement a procedure to identify vulnerabilities and patches for known viruses and "denial of service" attacks	
4.23	Provide and test redundancy in emergency communications to contact security officials, law enforcement agencies, and field incident commanders	

4.0 Information Technology and Communication Systems (cont.)

Seq No	Protective Measure	Action Required
4.24	Coordinate with all IT and communications vendors and contractors to heighten security awareness and reporting of suspicious activity. Inform vendors and contractors of control measures, including access, parking, and identification	
4.25	Check that offsite, stored backups for "as built" facility drawings and related engineering and capital projects information that might be needed in an emergency are readily available	
4.26	Implement and test backup hardware and software systems at the Emergency Operations Center (EOC). Implement and test emergency web site and network links to alternate sites	
4.27	Check that current backup copies of critical operations software are available to load onto backup servers	
4.28	Keep all essential personnel on call. Establish and verify primary and alternate phone numbers. Issue backup communications equipment to essential personnel. Implement the use of restricted frequencies for critical communications	
4.29	Practice restoring capability for critical data weekly. Recall tapes, verify correct labeling, and implement restoration procedures on main and alternate systems for selected critical business files	
4.30	Issue backup communications equipment to essential personnel	
4.31	Implement the use of restricted frequencies for critical communications	
4.32	Implement 100% sweep and inspection procedures for all IT vendor service vehicles and off-site backup tape delivery vehicles	
4.33	Disconnect all command, control, and financial computer systems) from the Internet and public access. Allow internal/intranet access, as appropriate	
4.34	Apply intrusion detection tools to detect and deter outside attempts to access the private network	
4.35	Activate emergency web site from alternate, secure location	
Active Incident		
4.36	Provide communication links and IT equipment resources to support the response effort	

4.0 Information Technology and Communication Systems (cont.)

Seq No	Protective Measure	Action Required
Recovery		
4.37	Replace damaged communication infrastructure and IT infrastructure elements.	
4.38	Discontinue use of emergency radio frequencies, as appropriate	
4.39	Recall tapes, verify correct labeling, and implement restoration procedures on main and alternate systems for selected critical business and operations files	
4.40	Perform system and critical file restoration for all essential computer systems. Verify that systems restorations are correct and complete	

5.0 Employee and Public Communications

Seq No	Protective Measure	Action Required
5.1	Develop emergency communications plans and procedures (including announcement types, frequency, and message based on threat condition). Establish points of contact for all internal and external communications. Develop emergency evacuation plans as appropriate.	
5.2	Incorporate security and emergency preparedness information into employee, customer, and general public education programs. Use the intranet to inform employees and the internet site to inform customers and the public of current conditions, awareness campaigns, and regional plans and activities. Refresh employee postings, public signs and broadcast messages at station platforms and on-board vehicles	
5.3	Develop specific provisions for disabled individuals in plans and procedures (e.g., employee and customer communications, security and emergency preparedness awareness campaigns)	
5.4	Establish contingency plans to provide for the welfare of employees and their families, such as assistance with overnight shelter and food. Include contingency and continuity plan information, as appropriate, in employee communications	
5.5	Develop a database of employee emergency contact information and next of kin for use during response and recovery activities	
5.6	Provide resource materials (e.g., brochures, websites) to employees to help with family preparedness planning activities	
5.7	Schedule periodic reviews/updates for all operations plans, personnel assignments, and logistics requirements that pertain to implementing employee, customer, and public communications activities	
5.8	Periodically contact liaisons with each station or facility served to maintain lines of communication. Use transit police or security personnel to routinely patrol stations/facilities	
5.9	Develop and disseminate emergency response, contingency and continuity, and security awareness materials	
5.10	Periodically update and test contact databases, calling trees, notification/recall lists, and other communications lists used during emergencies and heightened threat condition levels. Verify primary and secondary employee telephone numbers	
5.11	Review with all employees the elements of security and emergency management plans and personal safety pertaining to implementing increased security levels. Insure that all employees receive a security briefing regarding current and emerging threat conditions	
5.12	Periodically test public emergency communications plans using tabletop drills and exercises with regional emergency response partners	
5.13	Develop and issue quick reference emergency guidelines pocket cards to all employees	

5.0 Employee and Public Communications (cont.)

Seq No	Protective Measure	Action Required
5.14	Review U.S. Postal Service "Suspicious Mail Alert" and "Bombs by Mail" publications with all employees involved in receiving mail and package deliveries	
5.15	Remind employees and on-site contractors to always lock/secure their vehicles and personal spaces (e.g., personal vehicles, company-assigned vehicles, personal storage lockers, tool chests)	
5.16	Notify all transit agency employees, via briefings, e-mail, voice mail or signage, of any changes in HSAS threat level conditions and Protective Measures. Reinforce employee and rider Transit Watch programs	RSD # 5: Actions is required for rail operators, per TSA SD Railpax-04-01 #5
5.17	Direct employees to be alert and immediately report any suspicious activity or potential threat. To the extent resources allow, use surveillance systems to monitor for suspicious activity.	RSD # 6: Action is required for rail operators, per TSA SD Railpax-04-01 #6
5.18	Re-check adequacy of emergency evacuation signage posted on board vehicles and at stations, transit centers, and administrative and maintenance facilities. Post signs and/or make routine public announcements emphasizing the need for all passengers to closely control baggage and packages. Increase the frequency of announcements, especially during peak hours.	
5.19	Regularly inform staff and contractors of the general security situation and additional threat information as available. Provide periodic updates on security measures being implemented	
5.20	Instruct employees working alone at remote locations or on the ROW to check-in on a periodic basis	
5.21	Communicate information on heightened security measures to passengers in stations, where practicable, and on vehicles. Ask passengers to report unattended property or suspicious behavior to uniformed crew members and/or law enforcement personnel (suggested per Transit Watch - announcement frequency every 30 minutes). Increase the frequency of announcements and distribution of security awareness materials to passengers in stations and on-board revenue service vehicles	RSD # 7: Action is required for rail operators, per TSA SD Railpax-04-01 #7
5.22	Implement leave restrictions as necessary so that staff required to implement security plans are readily available (on call). Insure that all essential personnel, including employees with access to building plans and area evacuation plans, are available at all times	
5.23	Provide periodic updates to all staff on security measures being deployed	
5.24	Brief the Board of Directors and executive management, as necessary, on possible emergencies and protective measures being taken per the threat level condition	
5.25	Include Immediate Actions (IAs) for Transit Employees' guidance in procedures and protocols, and ensure that employees receive adequate IA training and testing	

5.0 Employee and Public Communications (cont.)

Seq No	Protective Measure	Action Required
5.26	Limit number of employees working alone in non-public areas to minimum. Increase the frequency of call-ins for isolated assignments	
5.27	Prepare and issue press releases to local media on transit system states of readiness, including restrictions related to carry-on articles, modifications to service or schedules, and other actions that may impact the riding public	
5.28	Increase the frequency of public address announcements (suggested Transit Watch frequency is every 5-10 minutes). Increase distribution of security awareness materials to passengers and the public	
5.29	Notify labor unions of threat level condition to assist/increase security coordination	
5.30	Use "all calls" to vehicle operators (Bus Dispatch/Radio Room to Bus Operators, Rail Control to Rail Operators, Paratransit Dispatch to Paratransit Drivers) to inform operators of threat level condition and related security needs/measures	
5.31	Make public address announcements and post signage to inform passengers that bags, packages, and other carry-on articles may be subject to inspection	
5.32	Schedule announcements and responses to local/regional media inquiries, and issue press releases on transit system states of readiness	
5.33	Inform/prepare employees to perform Immediate Actions (IAs) as needed.	
5.34	Increase frequency of public address announcements (suggested Transit Watch frequency is every 5 minutes).	
Active Incident		
5.35	Provide internal briefings and transit system status information to the public as soon as possible	
Recovery		
5.36	Use all available media to make frequent announcements about restoration of service, transit security, and the transit system's state of readiness.	
5.37	Work to restore public confidence by reporting available incident and law enforcement information	

6.0 Contingency and Continuity Plans

Seq No	Protective Measure	Action Required
6.1	Develop contingency and business continuity plans that address changes in HSAS threat level conditions. Develop contingency plans for loss of electrical power and loss of communications systems. Develop plans for revenue service continuation/restoration/recovery	
6.2	Identify alternative sites where the human resources department can adequately staff the agency, if necessary	
6.3	Develop plans to provide for the welfare of employees and their families (e.g., assistance with overnight shelter and food) in case of attack or major emergency.	
6.4	Develop and implement training based on contingency and continuity plans	
6.5	Prepare emergency response, continuity and contingency, and security awareness materials. Coordinate and disseminate materials within the transit agency	
6.6	Conduct drills and exercises of emergencies that require execution of contingency and continuity plans and procedures	
6.7	Implement contingency and continuity plans, as appropriate	
6.8	Modify standard contract terms and conditions to reflect the necessity of suspension of work for higher HSAS threat level conditions, including special requirements for jobsite configuration during work and non-work periods	
6.9	Prepare to execute continuity of operations procedures, such as moving to an alternate site or dispersing the workforce	
6.10	Prepare to execute specific contingency procedures (e.g., relocation of incident command or the Board of Directors' office to alternative sites, dispersion of the workforce)	
6.11	Activate alternative location for the Board of Directors' office	
Active Incident		
6.12	Assess the immediate impacts of the attack/emergency on the transit system, and prepare to implement contingency, continuity, and recovery plans as needed	
Recovery		
6.13	Activate contingency plan, disaster recovery, business continuity/recovery plan, and/or other continuity of operations plan(s), as needed	

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

Detailed Protective Measures Implementation Process and Worksheets

THIS PAGE INTENTIONALLY LEFT BLANK

Detailed Protective Measures Implementation Process

The implementation process for integrating HSAS threat conditions into a transit agency's security and emergency management program starts with a review of the protective measures. ***Protective measures*** (PMs) are the preventive and tactical actions taken to reduce vulnerabilities, deny an adversary opportunity, or to increase response capabilities. The objective of this general implementation process is to integrate the HSAS threat conditions with a transit agency's security and emergency management program using an applicable subset of all the protective measures provided in this document (and additional protective measures as needed).

A transit agency needs to first define its own specific procedures and processes, in order to implement the appropriate set of protective measures. Each protective measure is assigned to specific departments within the transit agency. Once developed, these implementation procedures and processes must be coordinated with the other emergency service resources/providers that are active within a transit agency's service area.

Protective measures are organized by transit agency security and emergency management function as the basis for developing and deploying specific implementation procedures. The provided lists of protective measures are candidate actions, not requirements. Specific implementation procedures and processes should be determined by a transit agency in light of its local needs, conditions, capital and operations budgets and operating environment. This list of protective measures is not intended to be exhaustive and not all of these protective measures may be appropriate for every transit agency. The list is provided as a starting point for the process.

Protective measure implementation should be prioritized based on an analysis of the transit agency's specific vulnerabilities, intelligence information, potential consequences and remedial costs. Similar to the relationship of plans and procedures, training, and drills and exercises, the protective measures implementation process for a transit agency has been set up as a continuous process through a feedback loop, as shown in Figure C-1. There are several inputs to the process including:

- TSA Rail Security Directives (SDs): RAILPAX-04-01
- Standard and emergency operating procedures (SOPs/EOPs)
- Security Vulnerability Assessments
- Threat information provided by Department of Homeland Security (DHS)
- Technical resources from the Transportation Security Administration (TSA), Office of Grants and Training (OGT) and Federal Transit Administration (FTA)
- Emergency and contingency operations plans
- Additional protective measures provided in this guidance document

The transit agency protective measures implementation process should produce, as output, a plan and/or procedural handbook that includes:

(1) A checklist of protective measures to be implemented for each HSAS color-coded threat level (and the Attack or Active Incident and Recovery conditions)

(2) A procedure or protocol for communicating the transit agency's HSAS protective measures plan (including notifying employees, coordinating with industry stakeholders and informing the media whenever the threat level is increased or decreased)

(3) A schedule for conducting HSAS threat level employee training and testing (tabletop exercises and regional drills)

The protective measures implementation process is iterative and it is intended to help improve security and emergency management programs at a transit agency, using the HSAS color-coded threat conditions as an organizational framework. The iterative process is accomplished through the feedback loop shown in Figure C-1; it includes the following inputs:

- Documented experience and knowledge from actual operation during higher threat conditions
- Documented experience from drills and exercises based on scenarios with higher threat conditions (after-action reports)
- Periodic audits, reviews and updates of security and emergency management plans
- Lessons learned from security and emergency management forums, such as the FTA/DHS Connecting Communities Forums

This process for implementing protective measures allows for a coordinated response from a transit agency, and ensures that the departments within a transit agency consistently communicate and coordinate with one another. The protective measures implementation process for developing the transit agency's response to the HSAS threat conditions should be set up with the following steps/activities:

(1) Creating a working group to coordinate the implementation

(2) Assigning departments the responsibility for implementing specific protective measures;

(3) Prioritizing the capability needs

(4) Developing a database for tracking and communicating protective measure activities, as a function of the HSAS threat conditions

(5) Testing readiness through tabletop exercises

(6) Implementing changes based on ongoing experience from actual events, drills and exercises.

To provide a structured framework, the protective measures are categorized into six functional areas, as shown in Table C-1. This table also provides a column suggesting the lead department for each category of protective measures.

Following this detailed implementation process description is a set of worksheets with the protective measures, categorized and numbered by functional areas. Each protective measure is assigned to one of the specific color-coded threat and response conditions, so that the connectivity of multiple protective measure activities can be seen and utilized. The worksheets are intended to be used within the transit agency to determine at a detailed level what each protective measure means to each department. Each department should decide which protective measures apply to them and how they should be implemented.

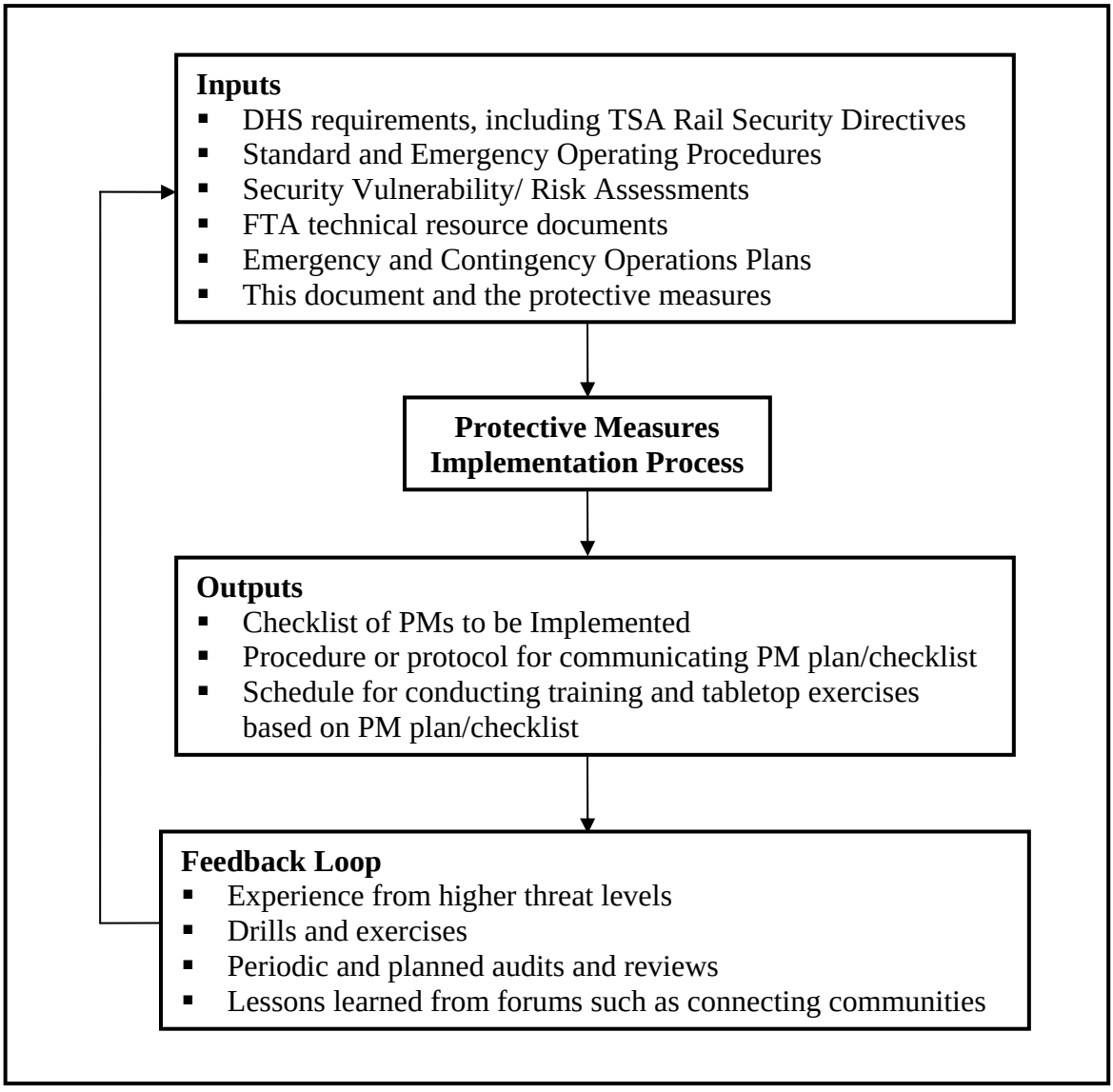


Figure C-1. Protective Measures Implementation Process

This approach presented here is not required by FTA and is provided only as a technical resource document. In preparation for emergency operations, most transit agencies have already completed a process similar to the one described here. This information is being provided to help ensure that the process used at transit agencies is systematic and thorough. At a minimum, a transit agency should review the material in this report to ascertain if its use would benefit or add value to existing processes.

It is important to remember that once this process starts, the information that is discussed and collected will most likely be categorized as ***sensitive security information (SSI)*** and will need to be controlled and protected from inappropriate disclosure outside of the transit system.

Table C-1. Categories of Protective Measures

Section/Category	Scope	Suggested Lead Department
1.0 Information & Intelligence	Information & intelligence gathering includes threat and vulnerability information collection and analysis, sharing information with and getting information from local, regional and federal sources such as DHS and the FBI	Security
2.0 Security and Emergency Management	All aspects of creating, updating, and executing the security and emergency management plans and procedures for the transit agency	Security
3.0 Regional Coordination	Participation of the transit agency in the region, including regional emergency response plans, relationships with other security-related organizations in the region and first responders, and conducting regional drills and exercises	Operations
4.0 Information Technology and Communications Systems	All aspects of creating, updating, and executing the information system plans and monitoring and operating the communications equipment for the transit agency	Information Technology
5.0 Employee and Public Communications	All aspects of creating, updating, and executing the employee and public information communications plans for the transit agency	Public Relations/ Marketing
6.0 Contingency and Continuity Plans	All aspects of creating, updating, and executing the transit agency's contingency and continuity of operations plans for emergency incidents/events within the transit system and in the region	Operations/ General Manager's Office

Protective measures implementation steps:

1. **Create a working group** – Executive management should assign staff to direct, design, and execute the protective measures implementation process. The transit agency staff assigned to this process should coordinate with all departments of a transit agency. At most transit agencies, the Security Department (or Office) typically will be tasked to lead this effort. However, it is extremely important that all of the transit agency's departments participate or are at least represented in this process.

2. **Assign Protective Measures to Departments** – Each protective measure should be assigned to the appropriate department(s) that needs to consider the implementation of the protective measure for their operations and functions within the transit agency. For convenience, the protective measures have been grouped by functional category as described in Table C-1 and listed here:

   1.0 Information & Intelligence
   2.0 Security and Emergency Management
   3.0 Regional Coordination
   4.0 Information Technologies and Communications Systems
   5.0 Employee and Public Communications
   6.0 Contingency and Continuity Plans

   Table C-2 presents a transit agency departmental organization structure, to facilitate which departments might be directly involved in the protective measures process. The suggested lead department is marked for each functional category of protective measures. The assigned lead department for each functional category should then facilitate the review of the protective measures by the other transit agency departments.

   Once assigned, the transit agency departments participate in filling out the appropriate protective measures category worksheets. The first actions should be focused on using the worksheets in to develop the detailed activities each department might employ, in order to establish their capability to implement each of the appropriate protective measures. Having appropriate departmental management and staff working on this assignment is critical to properly creating the detailed activities required to implement the protective measures.

   Figure C-2 illustrates how the protective measures worksheets should be completed. Each protective measure should be used as a performance standard, with department personnel determining what resources and capabilities currently exist, and what, if any, additional resources and capabilities are required to meet that performance standard. In order to be complete and accurate, it may be required that some of the protective measures that do not apply to the transit agency be removed, and/or some new protective measures that are determined to be necessary may be added.

Table C-2. Assignments of Transit Agency Departments to PM Worksheets

Department	1.0	2.0	3.0	4.0	5.0	6.0
Office of the General Manager						◆
Internal Audit						
Legal						
Legislative Affairs						
Media and Public Affairs					◆	
Engineering						
Capital Programs						
Program Planning						
Facilities/Infrastructure Maintenance						
Accounting						
Budgeting						
Procurements and Contracts						
Risk Management						
Human Resources						
Training/Organizational Development						
Information Technology				◆		
Marketing and Customer Service						
Transportation (by Mode)			◆			◆
Vehicle Maintenance (by Mode)						
Scheduling and Service Planning						
Safety and Security	◆	◆				
Operations Training						

◆ - suggested lead department for worksheet group

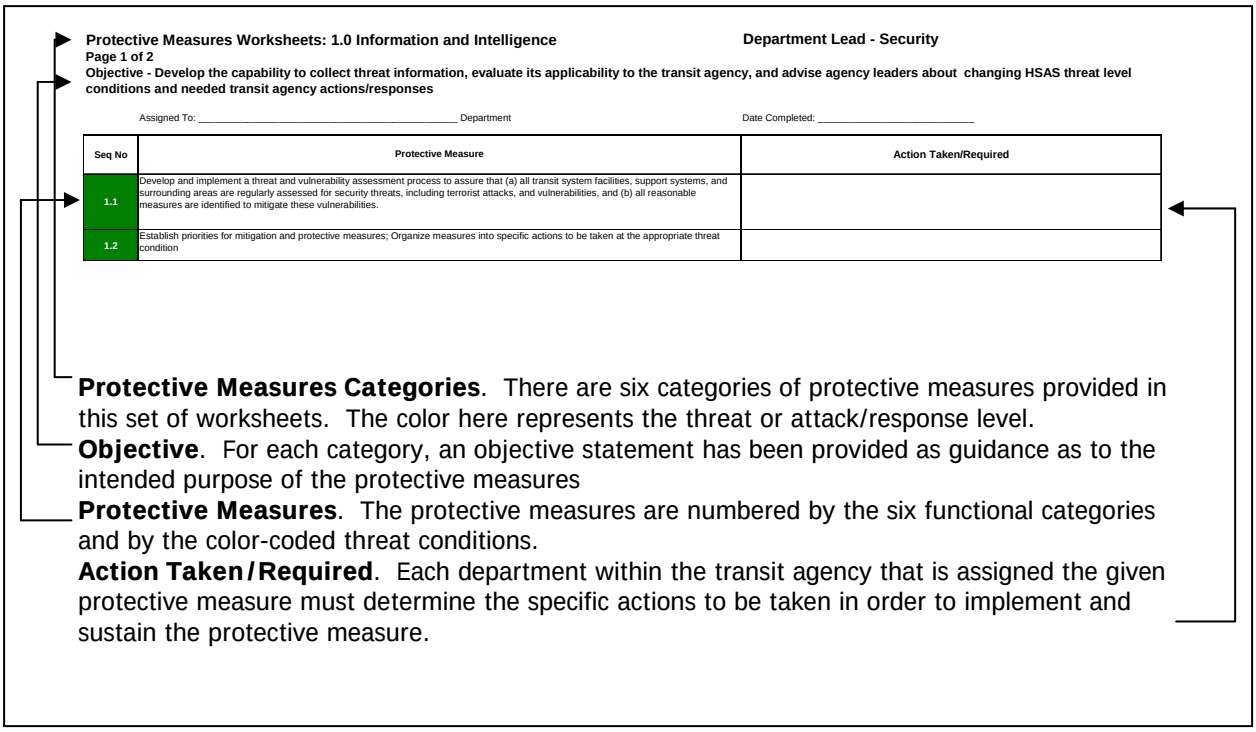


Figure C-2. Page from Protective Measures Worksheets

3. **Prioritizing Capability Needs and Reporting** – Once the worksheets are completed by the departments, existing capabilities versus needed capabilities can be assessed. Any identified missing capabilities (such as updated procedures, training, and equipment/supplies) should be prioritized. This prioritization process may significantly benefit from an understanding of a current security vulnerability assessment (SVA) for the transit agency. In some cases, operational procedures and additional training may be needed to bridge a gap of time required for needed capital procurement(s) to be completed.

4. **Developing a Database for Tracking and Communicating Protective Measure Activities by Departments** – A transit agency may want to create a database for tracking and internally communicating the completed protective measures worksheets. A database tool may be extremely helpful because each protective measure may have more than one department responding with activities to support that protective measure, and this may become difficult to keep organized. Executive and departmental management of a transit agency need to know what protective measure activities are planned at each color-coded HSAS threat level condition, across all departments, and this database can serve that function. Reports could be generated from the database to provide summaries of protective measure activities by department. These reports could also be used by departments to make changes and updates to that information as well as request replacement and new resources for capabilities required to execute those planned activities. A transit agency may also want to consider having the capability of creating these reports by facility as well.

5. **Testing Readiness Through Tabletop Exercises** – Tabletop exercises should be planned to test the activation of the planned protective measure actions for the entire transit agency. Preparedness is an iterative process of creating plans and procedures, developing and providing training, and then testing whether or not the plans, procedures, and training are having the desired effect. In this case, the departments of the transit agency should test their responses to potential threats and actual emergencies to determine if their plans are adequate and appropriate.

   There are many ways that these capabilities can be tested. One approach is to develop a tabletop scenario that requires the transit agency to respond to an emergency. The participants should first consider how they would react to this emergency scenario with only their existing capabilities. The next step is to then respond to the same emergency scenario with (hypothetical) access to any needed capabilities. The participants could then assess the gap in the capabilities that would be desired for that emergency and other potential emergencies. This gap analysis would then be fed back into the protective measures implementation process.

6. **Implement Changes** – These changes will typically be based on results from the exercises in Step 5 or the occurrence of actual incidents/events. The multi-step protective measures implementation process should be updated on a regular basis, preferably annually. This update could also follow any regularly scheduled exercises. Updates may also be needed after an actual emergency situation has occurred at the transit agency based on after-action reports from that emergency.

Protective Measures Worksheets: 1.0 Information and Intelligence **Department Lead - Security**

Page 1 of 2

Objective - Develop the capability to collect threat information, evaluate its applicability to the transit agency, and advise agency leaders about changing HSAS threat level conditions and needed transit agency actions/responses

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
1.1	Develop and implement a threat and vulnerability assessment process to assure that (a) all transit system facilities, support systems, and surrounding areas are regularly assessed for security threats, including terrorist attacks, and vulnerabilities, and (b) all reasonable measures are identified to mitigate these vulnerabilities.	
1.2	Establish priorities for protective measures and mitigation; Organize measures into specific actions to be taken at the appropriate threat condition	
1.3	Establish contact information with local and regional law enforcement and security intelligence units, state and federal regional offices	
1.4	Identify available security planning informational resources such as the FTA's website	
1.5	Develop, disseminate, and implement procedures for employees receiving information (e.g., phone calls, e-mails) that threaten harm to the transit system, employees, or customers	
1.6	Designate a primary and an alternate Security Coordinator (SC) and provide their contact information to the Transportation Security Aministration (TSA). Immediately notify TSA (sd.masstransit@dhs.gov) of changes in SCs or contact information, e.g., telephone number(s)	RSD #1: Notification to TSA required for rail operators, per TSA SD Railpax-04-01
1.7	Designate responsibilities of primary and alternate SCs to: (a) serve as the transit agency's primary and immediate contact for intelligence information, security-related activities, and communications with TSA; (b) be available to TSA on a 24-hour basis; (c) review, as appropriate, all security-related functions to ensure they are effective and consistent with rail passenger security measures, including TSA's SD Railpax-04-01; (d) upon learning of non-compliance with TSA-required security measures, immediately initiate corrective action; (e) coordinate implementation of security measures with other organizations involved in security operations, including but not limited to, third party owners of rail passenger stations and freight railroads hosting the operations of parties to which TSA SD Railpax-04-01 applies. This includes follow up reporting on federal inquiries.	RSD # 2: Notification to TSA required for rail operators, per TSA SD Railpax-04-01
1.8	Report threats and security concerns to law enforcement authorities and to TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov	RSD # 3. Reporting to TSA required for rail operators, per TSA SD Railpax-04-01
1.9	Via e-mail to sd.masstransit@dhs.gov, notify TSA of the date of the most recent vulnerability assessment. Provide TSA access to the vulnerability assessment and corresponding security plan (if available). If no vulnerability assessment has been conducted, so advise	RSD # 4: Notification to TSA required for rail operators, per TSA SD Railpax-04-01
1.10	Network with local and regional law enforcement and security intelligence units, Joint Terrorism Task Force, and the area TSA Federal Security Director or Surfact Transportation Security Inspector for assessments of current and security-related information.	
1.11	Review/re-issue procedures for employees reporting threatening communications (e.g., phone calls, e-mails)	
1.12	Include intelligence information in roll-call briefings of security and law enforcement units	
1.13	Review security vulnerability assessments and update regularly or whenever a new asset (i.e., a new facility such as an administrative building, bus depot, rail yard, or new type of revenue service) is added.	
1.14	Include security in special event planning to identify any unique requirements	
1.15	Join/participate in FBI Joint Terrorism Task Force (JTTF), Surface Transportation Information Sharing and Analysis Center (ST-ISAC) and Homeland Security Information Network (HSIN).	
1.16	Actively seek relevant intelligence with DHS, FTA, JTTF, ISAC, HSIN, state and local authorities, and other transit agencies.	
1.17	Assess the threat's characteristics. Determine the additional Protective Measures required.	

Protective Measures Worksheets: 1.0 Information and Intelligence **Department Lead - Security**

Objective - Develop the capability to collect threat information, evaluate its applicability to the transit agency, and advise agency leaders about changing HSAS threat level conditions and needed transit agency actions/responses

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
	Active Incident	
1.18	Advise TSA via the TSOC (1-703-563-3237 or TSOC.ST@dhs.gov) immediately of all known information regarding the nature of the attack so that TSA can provide assistance and immediately disseminate the information to other transit and governmental agencies.	
1.19	Identify attacker(s) to law enforcement and security personnel. As appropriate, use witnesses or surveillance for timely and relevant information.	
	Recovery	
1.20	Guard against secondary attacks	
1.21	Coordinate with external intelligence and information agencies to return to the appropriate HSAS threat level condition	
1.22	Prepare an After Action Report - Determine circumstances that led to successful attack. Evaluate response performance. Identify and implement corrective measures. Document actions and lessons learned	

Protective Measures Worksheets: 2.0 Security and Emergency Management

Department Lead - Security

Page 1 of 5

Objective - Develop, test, and maintain internal and external security and emergency management plans, procedures, and capabilities within the transit agency, area of operation, and region

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
2.1	Develop system security and emergency response plans and standard and emergency operating procedures. In these plans and procedures, identify the responsibilities of employees by job function. Include preparedness for multiple concurrent events.	
2.2	Establish a security and emergency management team or task force, with designatied alternates, that is responsible for implementing procedures appropriate to the emergency condition	
2.3	Review security and emergency management technical guidance on FTA's website	
2.4	Inventory emergency equipment and supplies. Verify that needed quantities at higher HSAS threat level conditions are adequately stocked and/or available	
2.5	Establish priorities for all outstanding maintenance and capital projects that could affect the security of facilities	
2.6	As part of the system security plan, develop and implement access control systems for employees, visitors, facilities, and vehicles. Develop access restrictions that allow for the implementation of recovery plans after an attack or emergency, but that prevent tampering with the incident scene. Implementation of access controls should be incremental in response to changing HSAS threat level conditions	
2.7	As part of the system security plan, develop and implement a document control system to identify and protect sensitive security information.	
2.8	Direct that all personal, transit, and contractor vehicles be secured when not in use	
2.9	Survey areas adjacent to and surrounding transit properties to determine activities that might increase security risks to the transit system (e.g., government buildings, airports, stadiums, convention centers, industrial plants, pipelines, railroads)	
2.10	Develop procedures for shutting down and evacuating facilities and/or the transit system	
2.11	Review/update all plans and procedures to ensure that they provide adequate assistance to employees and customers with disabilities	
2.12	Deploy neighborhood watch personnel, if available, for routine patrols	
2.13	Determine, map, and disseminate emergency evacuation route plans for transit system vehicles	
2.14	Determine and document factors that would require partial or full service shutdown	
2.15	Develop and implement a security and emergency management data collection system consistent with FTA national transit database reporting requirements. Use the system to analyze incidents and trends. Control sensitive security information per document control system (see sequence number 2.7)	
2.16	Perform background checks on all employees and on contractors consistent with applicable law	
2.17	Apply concepts of crime prevention through environmental design (CPTED) in reviews of facilities and in new designs and modifications	
2.18	Insure transit agency employees have visible identification (and uniforms for designated job categories); and that on-site contractors and visitors are identifiable by an appropriate identification system, such as badges.	
2.19	Develop and implement policies and procedures for a key control management/inventory system	
2.20	Develop the procedure for a full inspection of public and non-public facilitites including lockers and storage areas at higher threat conditions.	
2.21	Train all employees in security awareness, response plans, and individual roles and responsibilities.	
2.22	Train all employees on the Homeland Security Advisory System (HSAS) and on specific Protective Measures that the agency will implement at higher HSAS threat level conditions	
2.23	Plan and provide policing and security appropriate to DHS threat levels and threat advisories	RSD # 14: Action is required for rail operators, per TSA SD Railpax-04-01

Protective Measures Worksheets: 2.0 Security and Emergency Management (cont) **Department Lead - Security**

Page 2 of 5

Objective - Develop, test, and maintain internal and external security and emergency management plans, procedures, and capabilities within the transit agency, area of operation, and/or region

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
2.24	Conduct emergency drills and exercises that include employees and customers with disabilities	
2.25	Develop training and testing to assess employee proficiency (e.g., table top and field drills with outside responders). Base training and testing, in part, on FTA's "Immediate Actions for Transit Agencies" guidance. For all table top and field drills, include a process for system improvements based on after action reports	
2.26	Participate in regional drills and exercises to support the response to attacks or other emergencies, such as natural disasters	
2.27	Insure that existing physical security and emergency measures (e.g., fencing, lighting, locks) are in good working order and adequately maintained. Conduct regular tests of security and emergency management equipment (e.g., emerency generators, communication and notification systems, surveillance and intrusion detection systems). Repair/replace any defective equipment.	
2.28	Insure coordinatin between the safety and the security departments (e.g., emergency procedures are regularly reviewed and updated as needed by a safety management team)	
2.29	Inspect all mail and package deliveries. Examine mail and packages for letter/parcel bombs and suspicious substances. Do not open suspicious letters or packages	
2.30	Maintain accurate records for tracking all identification cards, badges, decals, and uniforms. Cancel access for any items lost or stolen. Require uniform vendors to verify identities of individuals seeking to purchase uniform articles	
2.31	Conduct immediate inventory sweep for all revenue and non-revenue vehicles, including contingency/spare vehicles. Search for any missing vehicles	
2.32	Immediately re-check all security systems (e.g., lighting, CCTV, and intrusion alarms). Install additional, temporary lighting if needed to provide desired lighting for key areas (e.g., underground stations, transit centers, rail yard and bus garage perimeters).	
2.33	Physically audit (at supervisory level)/enforce positive identification of all personnel. Make no exceptions.	
2.34	Identify and train employees who can assist as drivers of transit vehicles during emergencies	
2.35	Insure coordination between the security department and the operations and maintenance departments (e.g., jointly develop and approve standard operating procedures)	
2.36	Confirm availability of outside security resources to assist with intensified or increased span of coverage during peak periods	
2.37	Increase special patrols (e.g., foot patrols, bicycle patrols) and on-board vehicle patrols as appropriate.	
2.38	Reduce the number of access points for vehicles and personnel to minimum levels. Spot check contents of vehicles at access points. Watch for vehicles parked for long periods of time in or near any facility. Lock doors and check that all designated locked doors remain locked.	
2.39	Conduct frequent inspections of facilities, stations, terminals, and other critical assets, including public storage areas, for persons and items that do not belong.	RSD # 12: Action is required for rail operators, per TSA SD Railpax-04-01
2.40	At regular intervals, inspect each passenger vehicle for suspicious or unattended items.	RSD # 13: Action is required for rail operators, per TSA SD Railpax-04-01
2.41	If equipped with locking mechanisms, lock all doors that allow access to the engineer's or operator's cab or compartment. The TSA SD is not intended to supersede safety regulations concerning locking of certain types of doors on cards under DOT/FRA/FTA regulations.	RSD # 15: Action is required for rail operators, per TSA SD Railpax-04-01
2.42	Elevate the priority of security maintenance and repairs such as perimeter fencing, lighting, facility locks, and access points	
2.43	Limit visitor access to critical security areas. Confirm that visitors are expected and have a valid need to be in the area	

Protective Measures Worksheets: 2.0 Security and Emergency Management (cont) **Department Lead - Security**

Objective - Develop, test, and maintain internal and external security and emergency management plans, procedures, and capabilities within the transit agency, area of operation, and/or region

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
2.44	Change appearance (e.g., orange/yellow vests) and patrol deployment strategies to disrupt terrorist planning	
2.45	Alert vendors and contractors to heighten security awareness and report suspicious activity. Inform vendors and contractors about heightened control measures, including access, parking, and identification	
2.46	Increase security spot checks of persons (employees, contractors and visitors) entering non-public facilities, including confirming identification and randomly checking bags	
2.47	Secure all buildings and storage areas not in regular use. Increase frequency of inspections and patrols in these areas	
2.48	Increase surveillance of critical infrastructure areas (e.g., control and communication centers, loading docks, parking lots and garages, bridges, tunnels, rights-of-way)	
2.49	Check designated unmanned and remote sites more frequently for signs of unauthorized entry, suspicious packages, and unusual activities	
2.50	Check all deliveries to facility loading docks to insure that the items received are as ordered and expected. Refuse any unexpected deliveries	
2.51	For passenger stations with identified, significant risks, to the extent practicable, remove trash receptacles and other non-essential containers, except for bomb-resistant receptacles and clear plastic containers. Install bomb-resistant receptacles to the extent that resources allow.	RSD # 8: Action is required for rail operators, per TSA SD Railpax-04-01
2.52	Use explosive detection canine teams, if available.	RSD # 9: Action is required for rail operators, per TSA SD Railpax-04-01
2.53	At any time or place, allow TSA-designated canine teams to conduct operations under the overall direction of the authority responsible for security of the transit property or operator.	RSD # 10: Action is required for rail operators, per TSA SD Railpax-04-01
2.54	At any time or location, allow TSA/DHS-designated Security Partnership Teams to work with the transit agency's Security Coordinator to perform inspections, evaluations, or tests, including copying records, for Security Directive Railpax-04-01	RSD # 11: Action is required for rail operators, per TSA SD Railpax-04-01
2.55	Review standard operating procedures for heating, ventilation, and air conditioning (HVAC) operations in various emergency conditions	
2.56	Maintain respiratory protection equipment immediately available to law enforcement and operations personnel while they are in the field	
2.57	Increase the frequency with which law enforcement/security personnel perform ad hoc security checks and sweeps of transit vehicles at ends of lines	
2.58	Consider random screening of passengers' bags, backpacks, briefcases, suitcases, etc. at station entrances. Provide overt warning to potential passengers prior to their entering stations.	
2.59	Review procedures and prepare to establish/activate the Command Center(s). Prepare to dispatch Mobile Command Centers in the event of an actual emergency. Prepare to initiate the incident command system	
2.60	Put the Emergency Operations Center [EOC] on 'Stand-By' status with all systems operational. Verify that all systems are functioning	
2.61	Increase security postings and patrols to maximum sustainable levels	
2.62	Increase inspections of public storage areas, including bike and bag lockers	
2.63	Close and lock all gates and barriers except those needed for immediate entry and exit. Inspect perimenter fences on a frequent basis.	
2.64	Restrict visitors to essential business purposes. Require positive identification and inspect suitcases, packages, and other articles of significant size	
2.65	Limit access to designated facilities to personnel with a legitimate and verifiable need to enter.	

Protective Measures Worksheets: 2.0 Security and Emergency Management (cont)

Department Lead - Security

Page 4 of 5

Objective - Develop, test, and maintain internal and external security and emergency management plans, procedures, and capabilities within the transit agency, area of operation, and/or region

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
2.66	Implement higher threat level sweep and inspection procedures for transit vehicles in and out of facilities, and continue driver inspections of vehicles. Increase ad hoc security checks and sweeps of transit vehicles in revenue service (i.e., during revenue trips) by law enforcement/security personnel.	
2.67	Relocate authorized parked vehicles away from stations, terminals, and other critical buildings or areas, if possible. Consider implementing centralized parking and employee shuttle buses. Remove unauthorized parked vehicles	
2.68	Place backup/offsite operations control center on standby status. Test/verify its capability/readiness	
2.69	Erect barriers and obstacles to control traffic flows and protect stations, terminals, and other facilities and critical infrastructure from attack by parked or moving vehicles. Consider using company vehicles as barriers	
2.70	Increase presence/visibility of security and law enforcement personnel through cosistent appearance (e.g., all patrols and posted security wearing vests, transit police in full uniform)	
2.71	Protect onsite or adjacent auxillary facilities and services (e.g., day care center, homeless shelter, food service vendor) consistent with the agency's protective measures	
2.72	Postpone all non-vital construction work performed by contractors, or continuously monitor their work with agency personnel	
2.73	Limit administrative employee travel	
2.74	Close all public restrooms in underground stations	
2.75	Require service workers to empty trash receptacles more frequently	
2.76	Review security camera stored disks/tapes to detect possible indicators of pre-operational surveillance.	
2.77	Monitor and inspect elevators more frequently	
2.78	Increase the frequency of late night/overnight security sweeps and inspections of key right-of-way infrastructure elements (e.g., underground rail lines, electrical substations)	
2.79	Implement transit emergency plans and procedures. Assign emergency response personnel, pre-position resources, and mobilize specially trained teams	
2.80	Activate the transit system's EOC	
2.81	Implement 100% sweep and inspection procedures for transit vehicles in and out of facilities in addition to the driver inspections. Implement 100% security inspection at out-of-service stops	
2.82	Augment security forces to ensure control of key command, control, and communications centers and other potential target areas. Establish surveillance points and reporting procedures	
2.83	Maximize patrols in areas without stationed security personnel. Conduct frequent checks of building exteriors and parking areas	
2.84	Implement surveillance in support of guarded and patrolled areas	
2.85	Reduce facility access points to an operational minimum and restrict access to essential personnel.	
2.86	At facility access points, inspect 100% of employee, contractor, and visitor briefcases, suitcases, bags, and other articles	
2.87	Minimize/eliminate administrative employee leave/travel	
2.88	Close visitor and employee parking lots, as appropriate	
2.89	Disable and lock out public storage areas such as bike and bag lockers	
2.90	Physically verify that vehicle gates, garage and building doors, and other gates and doors designated to be closed and locked at the "red" threat level are actually closed and locked	

Protective Measures Worksheets: 2.0 Security and Emergency Management (cont) **Department Lead - Security**

Objective - Develop, test, and maintain internal and external security and emergency management plans, procedures, and capabilities within the transit agency, area of operation, and/or region

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
2.91	Close all non-essential functions (e.g., sales offices, neighborhood outreach offices, onsite day care facilities)	
2.92	Transfer/deliver all mail and packages to a central remote location for inspection	
2.93	Close all public restrooms	
2.94	Consider implementing temporary revenue service restrictions and/or re-routes associated with serving higher-risk targets/icons (e.g., military bases, stadiums, convention centers)	
2.95	Consider restricting or suspending bicycle transport (e.g., not allowing bicycles with bags or backpacks affixed to them to be carried on vehicles)	
2.96	Remove all non-explosive resistent trash cans (except clear plastic containers) at passenger facilities.	
2.97	Deploy on-duty vehicle cleaners to terminal stations during peak revenue hours. Remove or secure unattended newspaper vending machines in selected locations	
2.98	When operators exit their vehicles at an end-of-line layover point, require all riders to de-board. Secure/lock the vehicle. When operators return to vehicles, require them to conduct a sweep before allowing riders to board/re-board	
2.99	Staff backup/offsite operations control center. Prepare to assume control from primary operations control center if needed	
2.100	Perform Immediate Actions (IAs) for suspicious activities and imminent threats as necessary	
	Active Incident	
2.101	Perform Immediate Actions (IAs) for attacks as necessary	
2.102	Designate the incident commander. Activate and operationalize the EOC. Implement emergency operating procedures to mitigate the effects of the attack	
2.103	Provide security for the site and other transit system assets during the emergency. Be alert for possible secondary attacks	
2.104	Mobilize and provide transit assets (communications links, equipment, facilities and personnel) in support of the overall response effort	
2.105	Assess immediate impacts of the attack on transit service and facilities, and reduce or cancel services as required	
2.106	Assist with response to casualties, as needed/requested	
2.107	Restrict/eliminate access to facilities by contractors, vendors, and visitors. Accept deliveries on a case-by-case basis only	
2.108	Position/park vehicles to block etrances to facilities, as appropriate	
2.109	Review security camera stored disks/tapes for operational activity.	
	Recovery	
2.110	Provide security for the incident site. Allow access to incident area only to security, mitigation, and investigating personnel. Other access restrictions should allow the implementation of recovery plans, but prevent tampering with the incident scene until fully released	
2.111	Activate "on-call" external contractors and other special support, as required	
2.112	Implement plans to return to the appropriate threal level ("green" through "red")	
2.113	Inspect facilities and infrastructure for latent damage before reoccupying facilities or restoring operations	
2.114	Continue secure access control around affected area(s)	
2.115	Identify short and long-term capital replacement needs. Develop plans and detailed designs	
2.116	Recover facilities, infrastructure, and vehicles. Restore transit system capabilities. Restore the scene of attack to functionality	

Protective Measures Worksheets: 3.0 Regional Coordination

Department Lead - Security

Page 1 of 2

Objective - Develop, test, and maintain local and regional security coordination, including regional emergency response plans and coordination with area security-related and first-response organizations

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
3.1	Participate in development and review of local and regional security and emergency response plans	
3.2	Establish local, regional, and system-wide threat and warning dissemination processes (consistent with federal level information sharing per protective measures in 1.0 Information and Intelligence)	
3.3	Establish emergency communications capability and coordinate notifications to emergency response organizations	
3.4	Coordinate with emergency response agencies (e.g., military, police, fire, HAZMAT, hospitals, federal agencies) to develop support systems to provide post-incident support to customers and employees	
3.5	Establish memoranda of agreement (MOAs) and other mutual aid agreements, as needed, to assure adequate regional emergency response coordination	
3.6	Participate in local and regional security and emergency response training, drills, and exercises. Coordinate transit system's role in local and regional emergency response. Include an after-action report-based process improvement system for all tabletop exercises and drills	
3.7	Coordinate security and emergency response awareness materials for transit employess and the public consistent with other local and/or regional transit agencies	
3.8	Periodically communicate with military, law enforcement units, emergency response organizations, hospitals, and other agencies and organizations (including federal agencies), as appropriate	
3.9	Identify and train other community personnel who can assist as drivers of transit vehicles during emergencies	
3.10	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit agency is at Elevated Condition (Yellow) and advise the protective measures being employed	
3.11	Coordinate emergency preparedness/response plans with nearby jurisdictions	
3.12	Participate in daily/weekly regional briefings	
3.13	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit system is at HSAS condition "orange," and advise them of the Protective Measures being employed	
3.14	Consult with local authorities about control of public roads and access that could make the transit system more vulnerable	
3.15	Take additional precautions at local and regional public events. Consider alternative venues or postponing or canceling the events.	
3.16	Implement regional emergency plans with nearby jurisdictions. Implement plans to assist in evacuations or respond to emergency management requests	
3.17	Coordinate with local authorities on the possible closing of public roads and facilities and the removal of unattended vehicles	
3.18	Advise local agencies, law enforcement, security officials with an operational need to know, and TSA's Transportation Security Operation Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov, that the transit system is at HSAS condition "red," and advise them of the Protective Measures being employed	
3.19	Implement regional emergency preparedness plans with nearby jurisdictions. Implement plans to assist in evacuations or respond to emergency management requests	
3.20	Deploy liaisons to regional emergency operaions centers (EOCs) to participate in unified command	

Protective Measures Worksheets: 3.0 Regional Coordination **Department Lead - Security**

Objective - Develop, test, and maintain local and regional security coordination, including regional emergency response plans and coordiation with area security-related and first-response organizations

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
	Active Incident	
3.21	Report the attack immediately to all local, regional, state, and federal emergency response organizations, incluidng TSA's Transportation Security Operation n Center (TSOC) at 1-703-563-3237 or TSOC.ST@dhs.gov (including those mentioned in protective measure 1.10)	
3.22	Designate the transit agency Incident Commander, as needed, and activate transit agency's EOC. Provide onsite technical support to the regional EOC's Incident Commander	
3.23	Mobilize and provide transit assets (communications links, equipment, facilities and personnel) to support of the response, as requested by the Regional EOC Incident Commander	
	Recovery	
3.24	Coordinate local and regional plans to return to appropriate threat level ("green" though "red")	
3.25	Coordinate funding and other needs for transit system restoration with federal, state, and local agencies	

Protective Measures Worksheets: 4.0 Information Technology and Communications Systems

Department Lead - IT

Objective - Develop, test, and maintain information systems and communications plans, procedures, and capabilities appropriate for the transit agency to operate and to maintain communication under each HSAS threat level and FTA response condition

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
4.1	Develop and implement hardware, software and communications security and disaster recovery/business continuity plans and procedures, including (a) data management; (b) access partitions and permissions; (c) external communication links; (d) internal activity monitoring; (e) configuration management (hardware, software, network descriptions and locations); (f) vehicle control systems. Provide for incremental responses to changing threat level conditions. Coordinate with systems security plans. Develop and implement plans for business, operations, and security	
4.2	Inventory existing emergency response infrastructure, equipment, supplies and service contracts, and compare against current requirements. Assign work/prepare purchase orders based on the inventory. Consider: (a) frequency management (e.g., allocation and assignment of frequencies, license renewals, tower capacity); (b) contracts for backup communications systems (e.g., cell phones); (c) procurement and assignment of backup communications systems (e.g., distribution of phones and phone numbers to assigned personnel); (d) interoperability with local and/or regional emergency responder organizations (e.g., update/implementation of frequency management with responder organizations, purchase/acquisition of translation equipment). Purchase and/or install items needed to implement protective measures at higher threat levels	
4.3	Limit transit operations data communications to outbound information only. Install firewalls and DMZ environment. Block or control internet access. Establish private networks	
4.4	Use 'push' technology for anti-virus and software security updates	
4.5	Develop a computer incident response plan and team that includes representatives from various user groups	
4.6	Develop information technology (IT) administrative and operational procedures to identify and respond to IT and communications related incidents in a timely and controlled manner	
4.7	Configure IT infrastructure to provide fault tolerances across physical locations and within a single physical location	
4.8	Secure employee and customer information (e.g., personal information, account data, credit card information) from unauthorized electronic access	
4.9	Assess the impact on transit agency operations if all essential computer system resources (command, control, and financial computer systems) are disconnected from the internet and public access during higher HSAS threat level conditions. Manage external transit fare vending machines so that they cannot be compomised/hacked	
4.10	Perform daily incremental and weekly full backups of electronic data required for security, payroll, scheduling, operations, and business continuity. Transport backup(s) to a secure remote location weekly or more often for critical data. Practice data file restoration on a regular basis, including retrieval from offsite storage and return to offsite storage. Practice full System restoration on an annual or more frequent basis	
4.11	Test primary emergency communications and notification systems. Order maintenance as necessary. Update emergency communications frequencies for interoperability with emergency responders	
4.12	Test the network, servers, databases, and Web servers to ensure that they can handle increasing transaction loads	
4.13	Test to assure that the IT infrastructure is protected against unauthorized manipulation of website applications	
4.14	Test IT systems for single points of failure	
4.15	Secure command, control, and financial IT systems and communication networks from outside tampering	
4.16	Inspect and test all closed circuit television (CCTV), video camera/recording equipment, intercoms, emergency telephones, radios, and satellite communication devices to assure that all communication equipment is in place and operational	

Protective Measures Worksheets: 4.0 Information Technology and Communications Systems

Department Lead - IT

Objective - Develop, test, and maintain information systems and communications plans, procedures, and capabilities appropriate for the transit agency to operate and to maintain communication under each HSAS threat level and FTA response condition

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
4.17	Update system software (servers, switches, routers, firewalls, DMZs) for Information security protection. Enter all changes into the configuration management system	
4.18	Test/exercise primary and backup communications equipment and procedures with essential personnel to ensure that an agency or facility response can be mobilized appropriate to an incident or increased security requirement	
4.19	Test/exercise external communications equipment and procedures used with designated emergency response or command locations	
4.20	Monitor all digital communications links for security. Test alternate paths	
4.21	Perform daily incremental backups of electronic data required for security, payroll, scheduling, operations, and business continuity. Maintain copies on-site and transport backup(s) to secure remote location	
4.22	Develop and implement a procedure to identify vulnerabilities and patches for known viruses and "denial of service" attacks	
4.23	Provide and test redundancy in emergency communications to contact security officials, law enforcement agencies, and field incident commanders	
4.24	Coordinate with all IT and communications vendors and contractors to heighten security awareness and reporting of suspicious activity. Inform vendors and contractors of control measures, including access, parking, and identification	
4.25	Check that offsite, stored backups for "as built" facility drawings and related engineering and capital projects information that might be needed in an emergency are readily available	
4.26	Implement and test backup hardware and software systems at the Emergency Operations Center (EOC). Implement and test emergency web site and network links to alternate sites	
4.27	Check that current backup copies of critical operations software are available to load onto backup servers	
4.28	Keep all essential personnel on call. Establish and verify primary and alternate phone numbers. Issue backup communications equipment to essential personnel. Implement the use of restricted frequencies for critical communications	
4.29	Practice restoring capability for critical data weekly. Recall tapes, verify correct labeling, and implement restoration procedures on main and alternate systems for selected critical business files	
4.30	Issue backup communications equipment to essential personnel	
4.31	Implement the use of restricted frequencies for critical communications	
4.32	Implement 100% sweep and inspection procedures for all IT vendor service vehicles and off-site backup tape delivery vehicles	
4.33	Disconnect all command, control, and financial computer systems) from the Internet and public access. Allow internal/intranet access, as appropriate	
4.34	Apply intrusion detection tools to detect and deter outside attempts to access the private network	
4.35	Activate emergency web site from alternate, secure location	
	Active Incident	
4.36	Provide communication links and IT equipment resources to support the response effort	
	Recovery	
4.37	Replace damaged communication infrastructure and IT infrastructure elements.	
4.38	Discontinue use of emergency radio frequencies, as appropriate	
4.39	Recall tapes, verify correct labeling, and implement restoration procedures on main and alternate systems for selected critical business and operations files	
4.40	Perform system and critical file restoration for all essential computer systems. Verify that systems restorations are correct and complete	

Protective Measures Worksheets: 5.0 Employee and Public Communications

Department Lead - PR/Marketing

Objective - Develop, test, and maintain employee and public communications policies, plans, procedures, and capabilities so that the transit agency can communicate effectively under each HSAS threat level and FTA response condition

Assigned To: _____ Department

Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
5.1	Develop emergency communications plans and procedures (including announcement types, frequency, and message based on threat condition). Establish points of contact for all internal and external communications. Develop emergency evacuation plans as appropriate.	
5.2	Incorporate security and emergency preparedness information into employee, customer, and general public education programs. Use the intranet to inform employees and the internet site to inform customers and the public of current conditions, awareness campaigns, and regional plans and activities. Refresh employee postings, public signs and broadcast messages at station platforms and on-board vehicles	
5.3	Develop specific provisions for disabled individuals in plans and procedures (e.g., employee and customer communications, security and emergency perparedness awareness campagins)	
5.4	Establish contingency plans to provide for the welfare of employees and their families, such as assistance with overnight shelter and food. Include contingency and continuity plan information, as appropriate, in employee communications	
5.5	Develop a database of employee emergency contact information and next of kin for use during response and recovery activities	
5.6	Provide recource materials (e.g., brochures, websites) to employees to help with family preparedness planning activiities	
5.7	Schedule periodic reviews/updates for all operations plans, personnel assignments, and logistics requirements that pertain to implementing employee, customer, and public communications activities	
5.8	Periodically contact liaisons with each station or facility served to maintain lines of communication. Use transit police or security personnel to routinely patrol stations/facilities	
5.9	Develop and disseminate emergency response, contingency and continuity, and security awareness materials	
5.10	Periodically update and test contact databases, calling trees, notification/recall lists, and other communications lists used during emergencies and heightened threat condition levels. Verify primary and secondary employee telephone numbers	
5.11	Review with all employees the elements of security and emeergency management plans and personal safety pertaining to implementing increased security levels. Insure that all employees receive a security briefing regarding current and emerging threat conditions	
5.12	Periodically test public emergency communications plans using tabletop drills and exercises with regional emergency response partners	
5.13	Develop and issue quick reference emergency guidelines pocket cards to all employees	
5.14	Review U.S. Postal Service "Suspicious Mail Alert" and "Bombs by Mail" publications with all employees incolved in receiving mail and package deliveries	
5.15	Remind employees and on-site contractors to always lock/secure their vehicles and personal spaces (e.g., personal vehicles, company-assigned vehicles, personal storage lockers, tool chests)	

Protective Measures Worksheets: 5.0 Employee and Public Communications (cont) **Department Lead - PR/Marketing**

Objective - Develop, test, and maintain employee and public communications policies, plans, procedures, and capabilities so that the transit agency can communicate effectively under each HSAS threat level and FTA response condition

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
5.16	Notify all transit agency employees, via briefings, e-mail, voice mail or signage, of any changes in HSAS threat level conditions and Protective Measures. Reinforce employee and rider Transit Watch programs	RSD # 5: Actions is required for rail operators, per TSA SD Railpax-04-01 #5
5.17	Direct employees to be alert and immediately report any suspicious activity or potential threat. To the extent resources allow, use surveillance systems to monitor for suspicious activity.	RSD # 6: Action is required for rail operators, per TSA SD Railpax-04-01 #6
5.18	Re-check adequacy of emergency evacuation signage posted on board vehicles and at stations, transit centers, and administrative and maintenance facilities. Post signs and/or make routine public announcements emphasizing the need for all passengers to closely control baggage and packages. Increase the frequency of announcements, especially during peak hours.	
5.19	Regularly inform staff and contractors of the general security situation and additional threat information as available. Provide periodic updates on security measures being implemented	
5.20	Instruct employees working alone at remote locations or on the ROW to check-in on a periodic basis	
5.21	Communicate information on heightened security measures to passengers in stations, where practicable, and on vehcles. Ask passengers to report unattended property or suspicious behavior to uniformed crew members and/or law enforcement personnel (suggested per Transit Watch - announcement frequency every 30 minutes). Increase the frequency of announcements and distribution of security awareness materials to passengers in stations and on-board revenue service vehicles	RSD # 7: Action is required for rail operators, per TSA SD Railpax-04-01 #7
5.22	Implement leave restrictions as necessary so that staff required to implement security plans are readily available (on call). Insure that all essential personnel, including employees with access to building plans and area evacuation plans, are available at all times	
5.23	Provide periodic updates to all staff on security measures being deployed	
5.24	Brief the Board of Directors and executive management, as necessary, on possible emergencies and protective measures being taken per the threat level condition	
5.25	Include Immediate Actions (IAs) for Transit Employees' guidance in procedures and protocols, and ensure that employees receive adequate IA training and testing	
5.26	Limit number of employees working alone in non-public areas to minimum. Increase the frequency of call-ins for isolated assignments	
5.27	Prepare and issue press releases to local media on transit system states of readiness, including restrictions related to carry-on articles, modifications to service or schedules, and other actions that may impact the riding public	
5.28	Increase the frequency of public address announcements (suggested Transit Watch frequency is every 5-10 minutes). Increase distribution of security awareness materials to passengers and the public	
5.29	Notify labor unions of threat level condition to assist/increase security coordination	
5.30	Use "all calls" to vehicle operators (Bus Dispatch/Radio Room to Bus Operators, Rail Control to Rail Operators, Paratransit Dispatch to Paratransit Drivers) to inform operators of threat level condition and related security needs/measures	
5.31	Make public asddress announcements and post signage to inform passengers that bags, packages, and other carry-on articles may be subject to inspection	

Protective Measures Worksheets: 5.0 Employee and Public Communications (cont) **Department Lead - PR/Marketing**

Objective - Develop, test, and maintain employee and public communications policies, plans, procedures, and capabilities so that the transit agency can communicate effectively under each HSAS threat level and FTA response condition

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
5.32	Schedule announcements and responses to local/regional media inquiries, and issue press releases on transit system states of readiness	
5.33	Inform/prepare employees to perform Immediate Actions (IAs) as needed.	
5.34	Increase frequency of pulic address announcements (suggested Transit Watch frequency is every 5 minutes).	
	Active Incident	
5.35	Provide internal briefings and transit system status information to the public as soon as possible	
	Recovery	
5.36	Use all available media to make frequent announcements about restoration of service, transit security, and the transit system's state of readiness.	
5.37	Work to restore public confidence by reporting available incident and law enforcement information	

Protective Measures Worksheets: 6.0 Contingency and Continuity Plans **Lead - Operations/GM**

Page 1 of 1

Objective - Develop, maintain, and test contingency and continuity plans, procedures, and capabilities appropriate so that the transit agency can operate as effectively as possible under each HSAS threat level and FTA response condition

Assigned To: _____ Department Date Completed: _____

Seq No	Protective Measure	Action Taken/Required
6.1	Develop contingency and business continuity plans that address changes in HSAS threat level conditions. Develop contingency plans for loss of electrical power and loss of communications systems. Develop plans for revenue service continuation/restoration/recovery	
6.2	Identify alternative sites where the human resources department can adequately staff the agency, if necessary	
6.3	Develop plans to provide for the welfare of employees and their families (e.g., assistance with overnight shelter and food) in case of attack or major emergency.	
6.4	Develop and implement training based on contingency and continuity plans	
6.5	Prepare emergency response, continuity and contingency, and security awareness materials. Coordinate and disseminate materials within the transit agency	
6.6	Conduct drills and exercises of emergencies that require execution of contingency and continuity plans and procedures	
6.7	Implement contingency and continuity plans, as appropriate	
6.8	Modify standard contract terms and conditions to reflect the necessity of suspension of work for higher HSAS threat level conditions, including special requirements for jobsite configuration during work and non-work periods	
6.9	Prepare to execute continuity of operations procedures, such as moving to an alternate site or dispersing the workforce	
6.10	Prepare to execute specific contingency procedures (e.g., relocation of incident command or the Board of Directors' office to alternative sites, dispersion of the workforce)	
6.11	Activate alternative location for the Board of Directors' office	
	Active Incident	
6.12	Assess the immediate impacts of the attack/emergency on the transit system, and prepare to implement contigency, continuity, and recovery plans as needed	
	Recovery	
6.13	Activate contingency plan, disaster recovery, business continuity/recovery plan, and/or other continuity of operations plan(s), as needed	

THIS PAGE INTENTIONALLY LEFT BLANK