

**NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY**

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.



**Transportation
Security
Administration**

MASS TRANSIT & PASSENGER RAIL

COUNTERTERRORISM GUIDE



FOR OFFICIAL USE ONLY

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

WHAT IS TERRORISM?

The Department of Homeland Security (DHS) defines terrorism as a “premeditated threat or act of violence against noncombatant persons, property and environmental or economic targets to induce fear or to intimidate, coerce or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological or religious objectives.”

Terrorists often use threats to create fear among the public, to try to convince citizens that their government is powerless to prevent terrorism and to get immediate publicity for their causes.

Most terrorist incidents involve small, compartmentalized extremists. Terrorist cells can blend into a community and remain dormant for extended periods of time. Local, state and federal law enforcement officials all work together to prevent or protect against potential attacks but face the difficult challenge of identifying these small cells.

A terrorist attack can take several forms, depending on the resources available to the cell, the nature of the political issue motivating the attack and the points of weakness of the terrorists' target.

TSA'S MISSION

The Transportation Security Administration (TSA) protects the nation's transportation systems to ensure freedom of movement for people and commerce.

WHAT IS TERRORISM?

WARNING

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need to know” without prior approval of an authorized DHS official.

2

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

PRE-INCIDENT INDICATORS

The following pre-incident indicators can alert officials to a potential terrorist attack if properly reported. It is important to understand that the presence of one or two indicators does not presume terrorist activity, but the presence of several indicators should be reported immediately.

Eight Signs of Terrorism

1. Surveillance	5. Acquiring Supplies
2. Elicitation	6. Impersonation
3. Tests of Security	7. Rehearsal
4. Funding	8. Deployment

1. **Surveillance** of a potential target to determine:

- Its strengths and weaknesses
- How well it is protected
- What security measures are in place
- Emergency/law enforcement response patterns and times

Suspicious surveillance activity may include the following:

- Recording or monitoring activities
- Drawing diagrams, making notes or taking photographs
- Using vision enhancement equipment
- Acquiring blueprints/floor plans
- Showing interest in security and access points to facilities

2. **Elicitation:** Attempts to gain information about operations and security from people or organizations:

- By mail, email, phone and/or in person
- By gaining employment to monitor day-to-day activities

3

TERRORISM
INDICATORS

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

3. Tests of Security: Testing security procedures and response times, for example:

- Leaving unattended bags or suspicious items in potential target areas to test how long it takes for people/security to respond
- Trespassing into restricted areas to test security
- Possible use of bomb threats or false alarms to test response and timing

4. Funding: Not only do terrorists need to raise money to fund their operations, they need to transfer and spend it in a way that does not draw attention. Typical crimes for funding may include but are not limited to the following:

- Drug and human trafficking
- Burglary/theft
- Selling of illegal merchandise
- Funneling money from charitable organizations and legitimate businesses

Signs to watch out for:

- An unusually large transaction paid for with cash or gift cards
- Donations to unknown charities

5. Acquiring Supplies: To carry out an attack, terrorists may acquire a variety of supplies legally or illegally. Examples of supplies:

- Weapons
- Transportation
- Communications systems
- Abnormal amounts of chemical precursors such as acids

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

5

TERRORISM
INDICATORS

Suspicious activities that should be reported include:

- Suspicious vehicles in strange or restricted areas
- Storage of large quantities of fertilizer, odd machinery or supplies that can be made into weapons
- Fraudulent IDs, passports or credentials
- Stealing or attempts to acquire uniforms in nonconventional ways

6. Impersonation: Terrorists may impersonate law enforcement, mail carriers, utility workers or company employees to gain information. Other signs to look for:

- Individuals who do not belong or who look out of place
- Suspicious actions
- Suspicious conversations

7. Rehearsal: Terrorists will sometimes rehearse an impending attack to ensure their operations run smoothly. This may include the following:

- Putting their operatives into position
- Monitoring police or first responder radio channels
- Dry runs using simulated improvised explosive device (IED) components
- Measuring emergency response times of area police and firefighters

8. Deployment: The phase in which terrorists are:

- Arranging their assets
- Getting into position
- In the midst of an attack

Note that the recommendations in this guide concerning the reporting of pre-incident indicators are not intended to alter or conflict with the requirement in 49 CFR §1580.203 that passenger railroads and rail transit systems report significant security concerns to DHS/TSA.

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

TARGETS

Terrorist groups have demonstrated the ability to plan and execute complex attacks simultaneously against multiple targets.

Terrorists have used assault teams equipped with small arms, vehicle-borne improvised explosive devices (VBIEDs) and suicide bombers against a myriad of hard and soft targets.

These targets could include the following:

- Key assets (e.g., nuclear power plants, dams, government facilities)
- The energy sector (e.g., power-generating facilities, fuel farms, gas stations)
- Mass transit and passenger rail critical infrastructure (e.g., stations, trains, bus and rail terminals) and other critical key resources
- Financial institutions (e.g., banks, credit unions)
- Places that host large crowds (e.g., shopping malls, sporting events, convention centers, large hotels)

Terrorists are opportunistic. They exploit vulnerabilities, choosing the time, place and method of attack according to the weaknesses they observe or perceive. Increasing and layering security around potential targets and assets may mitigate or eliminate a possible terrorist attack.



**NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY**

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

THREATS BY MASS TRANSIT & PASSENGER RAIL

7

TARGETS
THREATS

Transnational terrorist groups and violent extremists continue to demonstrate the intent to attack surface transportation, both overseas and in the homeland.

Violent Islamic extremists (ISIL, al-Qa'ida and its affiliates), homegrown violent extremists (HVEs), lone offenders and anarchist groups pose the primary threat to U.S. mass transit and passenger rail. Improvised explosive devices (IEDs) or assaults would likely play a role in an attack against mass transit in the U.S.

Examples of mass transit and passenger rail terrorist attacks include:

- The March 22, 2016, Brussels metro explosion at 9:11 local time. A bomb exploded in the second car of a train leaving the Maelbeek station, killing 20 people and injuring over 100 more.
- The August 21, 2015, thwarted train attack on a high-speed train from Amsterdam to Paris.
- The July 7, 2005, London bombings – a series of coordinated suicide bomb attacks in central London that targeted civilians using the public transit system during the morning rush hour.
- The March 11, 2004, commuter train coordinated bombings in Madrid, Spain.

Threats covered in this section include:

- Insider threat
- Suspicious devices
- Cloned vehicles
- Suspicious substances
- Suspicious packages
- Suspicious people

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

INSIDER THREAT

The following list contains examples of behaviors that may signify an individual's vulnerability to divulge sensitive information, and may alert colleagues that the individual is in need of assistance. Early reporting often allows intervention that will assist the employee in getting the help he or she needs.

Not all behaviors are actionable. However, in combination or at severe levels and left unchecked, they could pose a risk to the individual's well-being or to national security.

Examples of reportable behaviors:

- Alcohol or other substance abuse or dependence
- Mental health issues
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Poor financial conduct or unexplained or sudden affluence
- Unreported foreign travel, contacts or relationships
- Inappropriate, unusual or excessive interest in security sensitive information (outside current assignment)
- Mishandling of sensitive company information
- Misuse of computers
- Divided loyalty or allegiance to the U.S.

Employers may reduce or prevent insider threat by performing regular screening and background checks on employees and contractors.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

CLONED VEHICLES

The use of “cloned” vehicles remains a popular way for criminals and terrorists to gain access to restricted or high-profile areas. Cloned vehicles and those impersonating legitimate businesses, law enforcement or first responder personnel, or other federal or private entities, pose a significant threat to security.

Companies should train their employees to recognize and report suspicious vehicles and people who do not belong.

Possible indicators of a cloned vehicle:

- Missing or improperly displayed vehicle registrations/ tags
- Registered to a person and not a specific company
- Personalized license plates
- Very low service vehicle numbers
- Display of names belonging to rival companies
- Display of several company names but only one contact number
- Phone numbers listed on the vehicle that have no connection with the company name displayed
- Dark-tinted windows
- Aftermarket accessories (CD player, hubcaps, etc.)
- Attached equipment that doesn't appear to have been used in a long time
- Excessive number of decals
- Misspelled words



NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

SUSPICIOUS PACKAGES

Unattended packages impose a tremendous burden on security. Although unattended packages are rarely linked to explosive devices, they all represent a potential threat and need to be examined systematically.

To minimize potential confusion, threats and incidents, do not allow anyone to leave any unattended parcels, packages or bags with you or on your vehicle.

An **unattended package** is one that is left:

- On or next to a vehicle or waiting area.
- Next to a phone booth or vending machine.
- In a restroom.

A **suspicious package** is an unattended package that:

- Is left or placed in an out-of-the-way area (e.g., under or behind a seat or trash container).
- Is an out-of-place or abandoned container (e.g., fire extinguisher, propane canister, thermos).
- Matches something described in a threat.
- Has a threatening message attached.

SUSPICIOUS DEVICES

Suspicious devices may have:

- Unusual wires and batteries.
- Some sort of visible tank, bottle or bag.
- A clock or timer attached to the object.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

SUSPICIOUS SUBSTANCES

Chemical, Biological and Radiological (CBR) Agents

- Chemical agent symptoms are generally immediate and widespread.
- Biological and radiological agents' effects are generally delayed.

Quite often, the observation of two or more people with the same symptoms will be the first indication of an attack or exposure.

Signs of CBR agent release:

- An unexplainable pungent odor
- A suspicious package emitting a vapor or odor
- Abandoned, out-of-place aerosol or manual spray device (e.g., fire extinguisher, garden sprayer)
- A cloud, mist, fine powder, dust, liquid or fog with no identifiable or suspected source

Symptoms of CBR agent exposure:

- Difficulty breathing or uncontrollable coughing
- Collapse or seizure
- Nausea
- Blurred vision



Always protect yourself. If you become a victim, you cannot help others, and you add to the problem.

TARGETS
THREATS

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

SUSPICIOUS PEOPLE

Keep an eye out for people in the wrong place or wandering aimlessly around agency property. Remember that terrorists shadow their targets before they attack. Be leery of individuals expressing an unusual level of interest in various aspects of operations.

Quite often, people casing an area are looking for system vulnerabilities to exploit. These suspicious individuals may pose as members of the media. Never submit to interviews and/or photographs without prior approval from management.

A **suspicious person** is someone who is:

- In an unauthorized area.
- In the wrong place or appears lost.
- Overdressed for the weather conditions.
- Loitering and/or watching customers and employees.
- Pacing, nervous or jumpy.
- Acting in a disorderly manner that alarms or disturbs others.
- A repair, utility or delivery person or other “trusted employee” who is out of place.
- Expressing an unusual level of interest in operations, personnel, equipment or facilities.
- On property without proper identification, uniform or safety gear.

What to Do About a Suspicious Person

- When approaching a suspicious person in a restricted area, calmly ask if you can help.
- Request identification; ask what the person's business is or whom he or she is there to see.
- Notify police if there is no explanation for the person's presence.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

- Avoid approaching people who are threatening or dangerous.
 - Do not become confrontational, abusive or offensive.
 - Do not try to detain or hold a person by any means.
- If you have observed an unfamiliar person in a restricted or unauthorized area or engaged in suspicious activity, check the areas in which they were seen for signs of tampering or suspicious packages, devices or substances.
 - Try to keep the person in sight at all times and observe and report his or her location, activity, behavior and physical characteristics.

Physical Characteristics

When you observe a suspicious person, based upon his or her location and/or activity, you should take note of the person's physical description.

Details about the following characteristics will help police identify the person should he or she leave the area.

- **Eyes:** color, glasses
- **Hair/facial hair:** color, length, style, clean-shaven/beard/mustache
- **Size/body shape:** height, weight, build
- **Complexion:** skin color, acne, rashes
- **Markings:** tattoos, scars, birthmarks
- **Hat:** color, style
- **Shirt/blouse:** color, style, sleeves, collar
- **Coat:** color, style, length
- **Pants/skirts/shorts:** color, style
- **Shoes:** color, style
- **Appearance:** neat/sloppy, clean/dirty
- **Accessories:** bags, backpack, purse, briefcase

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

TACTICS

Al-Qa'ida, the Islamic State of Iraq and the Levant (ISIL/ISIS), homegrown violent extremists (HVEs) and their operatives have proven that they will use a myriad of tactics, including improvised explosive devices (IEDs), active shooters and vehicle-borne improvised explosive devices (VBIEDs), to carry out their attacks.

IEDs

An IED attack is the use of a “homemade” bomb and/or destructive device to destroy, incapacitate, harass or distract. IEDs are used by criminals, vandals, terrorists, suicide bombers and insurgents.

Precautions

- Be cautious of any item that arouses curiosity; exterior inspection does not ensure its safety.
- Keep in mind the components required for an IED and make note of any that are present upon initial observation (from a safe distance):
 - Power source (battery or similar device)
 - Initiator (blasting cap, switches)
- Beware of items/containers with electronic components that are not in their normal configuration and are connected to containers that could hold explosives or other hazmat. Examples:
 - Circuit boards
 - Cell phones
 - Antennas
- Beware of items with such components as fuses, fireworks, match heads, black or smokeless powder, or other unusual materials or liquids.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

15

IED RESPONSE

TACTICS

- Note the addition of attached items such as nails, bolts, drill bits, marbles or ball bearings used for fragmentation.
- Beware of obvious items such as blasting caps, detcords, military explosives, commercial explosives or grenades.

Response to an IED

- Do not approach or touch any suspicious device.
- Do not activate radios or cell phones within 300 feet/ 91 meters of the device.
- If a suspect item is identified, evacuate to a minimum safe distance of 300 feet/91 meters unless the threat is clearly a large vehicle bomb (LVB), and then go immediately to the exclusion area recommended by the FBI/ATF.
- Notify **911** immediately.
- Follow company reporting and response procedures.



COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

ACTIVE SHOOTER EVENTS

An active shooter is an individual who is engaged in killing or attempting to kill people in a confined and populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims.

- Victims are selected at random.
- The event is unpredictable and evolves quickly.
- Knowing what to do can save lives.

When an active shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation. The following are instructions from the Department of Homeland Security (DHS).

You have three options:



RUN

- Have an escape route and a plan in mind.
- Leave your belongings behind.
- Evacuate regardless of whether others agree to follow.
- Help others escape if possible.
- Do not attempt to move the wounded.
- Prevent others from entering an area where the active shooter may be.
- Keep your hands visible.
- Call **911** when you are safe.



HIDE

- Hide in an area out of the shooter's view.
- Lock the door or block entry to your hiding place.
- Silence your cell phone (including vibrate mode) and remain quiet.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.



FIGHT

- Fight as a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the shooter.
- Act with as much physical aggression as possible.
- Improvise weapons or throw items at the shooter.
- Commit to your actions – your life depends on it.

The first officers to arrive on scene will not stop to help the injured. Expect rescue teams to follow the initial officers. These rescue teams will treat and remove the injured.

Once you have reached a safe location, you will likely be held in that area by law enforcement until the situation is under control and all witnesses have been identified and questioned. Do not leave the area until law enforcement authorities have instructed you to do so.

When law enforcement arrives:

- Remain calm and follow instructions.
- Drop any items in your hands (e.g., bags, jackets).
- Raise your hands and spread your fingers.
- Keep your hands visible at all times.
- Avoid quick movements toward the officers, such as holding on to them for safety.
- Avoid pointing, screaming or yelling.
- Do not ask questions when evacuating.

Source: DHS Active Shooter Event Quick Reference Guide

INFORMATION TO PROVIDE TO 911 OPERATIONS

- Location of the active shooter
- Number of shooters
- Physical description of the shooter(s)
- Number and type of weapons each shooter has
- Number of potential victims at the location

17

ACTIVE SHOOTER

TACTICS

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

VBIEDs

Vehicle bombs are a common terrorist method of attack. Prior to September 11, 2001, the two most destructive terrorist attacks carried out on U.S. soil involved large truck VBIEDs (World Trade Center and Oklahoma City). Attacks overseas have included the use of an accelerant (e.g., gasoline, cooking oil) to increase the destructive effects of VBIEDs.

Some potential indicators of VBIEDs:

- Rental/delivery/utility vehicles, limos or other vehicles parked in unusual locations
- A driver who operates a vehicle in an overly cautious manner, attempts to abandon the vehicle or acts nervously
- A driver who displays noncompliant behavior, such as insisting on parking close to a building or crowded area
- Excessive vehicle weight or unusually uneven weight distribution (e.g., the vehicle appears overloaded or loaded by someone unfamiliar with proper cargo weight distribution)
- Smoke or strong chemical or fuel odors emanating from a vehicle
- Recent theft of explosives in the area, including blasting caps, fuses or chemicals used in the manufacture of explosives
- Rental of self-storage space for the purpose of storing chemicals or mixing apparatuses
- Delivery of chemicals directly from the manufacturer to a self-storage facility, or unusual deliveries of chemicals to residential or rural addresses
- Chemical fires, toxic odors, brightly colored stains or rusted metal fixtures in apartments, hotel/motel rooms or self-storage units

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

- Modification of a truck or van with heavy-duty springs to handle heavier loads
- Small test explosions in remote rural areas
- Treatment of chemical burns or missing hands/fingers
- Untreated chemical burns or missing hands/fingers
- Reported attempts to gain access to restricted areas or to park closer than usual to buildings, storage sites or other infrastructure locations
- Consumer rental trucks or vehicles being used to pick up chemicals or volatile supplies



19

VBIEDS

TACTICS

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BOMB THREAT DISTANCES

20



BOMB THREAT STAND-OFF CARD



THREAT DESCRIPTION	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
 Pipe Bomb	5 lbs	70 ft	71-1,199 ft	+1,200 ft
 Suicide Vest	20 lbs	110 ft	111-1,699 ft	+1,700 ft
 Briefcase/Suitcase	50 lbs	150 ft	151-1,849 ft	+1,850 ft
 Car	500 lbs	320 ft	321-1,899 ft	+1,900 ft
 SUV/Van	1,000 lbs	400 ft	401-2,399 ft	+2,400 ft
 Small Delivery Truck	4,000 lbs	640 ft	641-3,799 ft	+3,800 ft
 Container/Water Truck	10,000 lbs	860 ft	861-5,099 ft	+5,100 ft
 Semi-Trailer	60,000 lbs	1,570 ft	1,571-9,299 ft	+9,300 ft

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

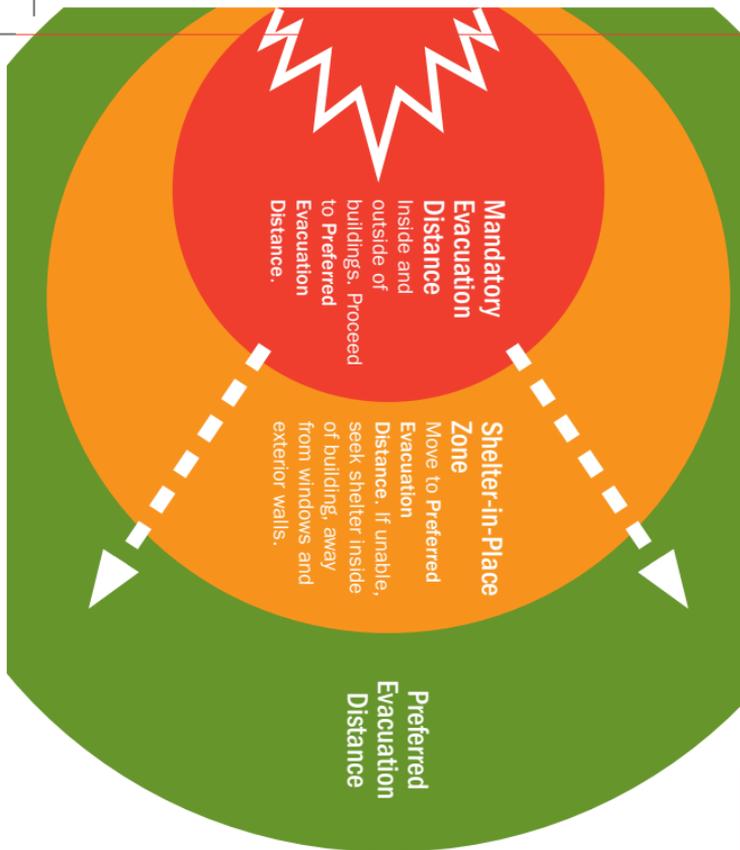
NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

21

EVACUATION

TACTICS



CAUTION!

- Do not touch suspicious item.
- Notify proper authorities.
Call 911.
- Ensure all witnesses are available to brief first responders.
- Recommended stand-off data should be used in conjunction with your emergency evacuation plan.

Sources: Department of Homeland Security,
Office for Bombing Prevention, Arlington, VA;
FBI, Bomb Data Center, Quantico, VA;
Technical Support Working Group, Arlington, VA

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

PREVENTION/MITIGATION

NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)

DHS issues NTAS advisories to communicate information about terrorist threats. These advisories provide timely, detailed information to the public, government agencies, first responders, public sector organizations, airports and other transportation hubs.

NTAS consists of two types of advisories:

1. Bulletins have been added to the advisory system to communicate current developments or general trends regarding threats of terrorism. Bulletins provide critical terrorism information that, while not necessarily indicative of a specific threat against the U.S., can reach homeland security partners or the public quickly, thereby allowing recipients to implement necessary protective measures.

2. Alerts will be issued when there is specific, credible information about a terrorist threat against the U.S. Alerts may include specific information, if available, about the nature of the threat, including geographic region, mode of transportation or critical infrastructure potentially affected by the threat, as well as steps individuals and communities can take to protect themselves and help prevent, mitigate or respond to the threat.

Elevated Alert: DHS has credible threat information, but only general information about timing and target, making it reasonable to recommend implementation of protective measures to thwart or mitigate an attack.

Imminent Alert: DHS believes the threat is credible, specific and impending in the very near term.

For more information, go to:

www.dhs.gov/national-terrorism-advisory-system

NTAS

22

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

PROTECTIVE MEASURES

TSA strongly recommends that, to the extent possible and based on threat information and agency capabilities, public transportation and passenger railroad owner/operators implement the following voluntary security measures associated with all hazards and with the more specific enumerated categories. These measures will be updated every six months or as necessary.



As well as implementing these protective measures, random and unpredictable security activity is always encouraged.

General All Hazard

1. Direct all employees, contractors and vendors, as appropriate, to be alert and follow emergency notification procedures as appropriate to immediately report any situation that appears to constitute a threat or suspicious activity.
2. Consider the use of law enforcement, security or other designated personnel to perform surveillance at or in the following:
 - Key entrances and areas of high consequence and/or high pedestrian traffic
 - Terminals and stations
 - Railcars and buses
 - Rail and bus yards
 - Other locations

Also, increase monitoring of closed-circuit television (CCTV) cameras.

23

GENERAL ALL HAZARD

PREVENTION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

General All Hazard (Cont'd)

3. Consider requesting assistance from state or local law enforcement agencies to increase the presence of marked vehicles and uniformed security personnel.
4. Increase the frequency of inspections of the following for suspicious or unattended items:
 - Passenger railcars and buses
 - Rail and bus terminals
 - Rail and bus stations
 - Rail and bus yards
 - Right-of-ways
5. Maintain open lines of communication and law enforcement intelligence gathering.
6. Coordinate necessary security efforts, based on the nature of the perceived threat, with federal, state, local and tribal law enforcement agencies.
7. Communicate security awareness information to passengers in stations and on trains and buses.
 - Ask employees and passengers to report unattended property or suspicious behavior to uniformed crew members and/or law enforcement.
 - Increase the frequency of announcements and distribution of security awareness materials.
 - When possible, leverage programmable reader board signs and public address systems installed in multimodal locations.

In regions where there are multiple public transportation and passenger railroad owner/operators, coordinate general hazard information messaging across public information outlets.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

25

GENERAL ALL HAZARD

8. Increase the frequency that designated unmanned and remote sites and security equipment are checked for signs of unauthorized entry, suspicious items or unusual activities. Additionally, maintain heightened vigilance in areas where objects can be concealed or hidden, such as in trash receptacles.
9. Maximize available canine patrols. The mobility of explosives detection canine teams, especially when employed in a visible, random and unpredictable manner, provides a heightened deterrent.
10. Consistent with current conditions, provide regular awareness briefings and updates on the prevailing threat situation to local law enforcement, transit, rail and bus employees and security personnel.
11. Review emergency action plans, evacuation procedures and shelter-in-place policies with facility employees.
12. Review or update security assessments to determine the facility's vulnerability to threats and review the relevant emergency response procedures with agency personnel.
13. Designate a point of contact with knowledge of the facility's security procedures and floor plan to liaise with police and other emergency agencies in the event of an attack.



PREVENTION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

General All Hazard (Cont'd)

14. When conditions warrant, restrict access and use of facilities to transportation only (e.g., shut down portions of the facility that include food courts and vendors, and other areas).
15. Ensure employees have visible identification.
16. Maintain effective communication with local labor representatives to ensure:
 - Awareness of a specific or credible threat to rail/bus operations.
 - Understanding of the rationale for heightened security measures.
 - Effective means to resolve concerns.
17. Deploy law enforcement and/or security officials, or other designated personnel, to conduct random patrols of buses, railcars, transit vehicles and infrastructure.
18. Review standard operating procedures (SOPs) for prevention, protection and response.



NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

27

IED / ACTIVE SHOOTER THREAT

Improvised Explosive Device (IED) Threat

1. Consistent with law, statute and agency policy, randomly inspect passengers' containers or bags.
2. Ensure open lines of communication with local explosive-detection and canine-response police officers.
3. Consider establishing a perimeter security stand-off distance from targeted facilities and stations.
4. Inspect and secure luggage/storage areas.

Active Shooter Threat

1. Review and re-brief local law enforcement on tactics for handling active shooter scenarios.
2. Establish appropriate perimeters (inner and outer) at target sites to deny access or intercept potential assailants, and ensure security personnel and security measures are in place at all access points.
3. Ensure blueprints, floor plans and other documents containing sensitive security information are available to responding law enforcement.
4. Review plainclothes recognition protocols by law enforcement.



PREVEN-
TION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Sabotage

1. Coordinate with other public transportation agencies and railroads that operate on adjacent routes to inform staff about awareness of the sabotage threat and concern. There should be heightened vigilance for, and reporting of, suspicious activities and objects along or on key routes.
2. Increase the presence and visibility of security, law enforcement and operations personnel in and around stations, rail yards and other critical infrastructure along the right-of-way, such as switches, curves, bridges and tunnels.
3. When the situation warrants, limit/reduce train speeds so as to improve stopping capability.
4. Increase random track inspections.

Chemical, Biological and Radiological (CBR) Agents

1. Review SOPs for heating, ventilation and air-conditioning operations in various emergency conditions.
2. Ensure that first responder personnel have recently reviewed their response tactics to be used in the event of a chemical/biological attack affecting the infrastructure and operations of the public transportation agency or railroad.
3. Maintain open lines of communication with public health officials about the threat.
4. Ensure that personal protective equipment (PPE) and portable detection devices are fully functional and ready to be issued and deployed as needed.
5. Increase monitoring of CCTV cameras for indicators of debilitating effects on passengers or other symptoms exhibited by passengers.
6. Increase monitoring of the operating status and sampling results for all deployed chemical, biological and radiological alarms and sensors.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

29

Hijacking

1. Review and re-brief transit personnel and local law enforcement agencies on hijacking prevention and response procedures.
2. Implement remote kill switches, driver authentication systems and panic buttons on buses.
3. Increase monitoring capabilities of deployed buses and establish procedures for making deviations from the assigned routes.
4. Review procedures with 911 dispatch centers to relay an influx of 911 calls in response to a hijacking to local law enforcement agencies.



HIJACKING

PREVENTION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

SECURITY MEASURES

The following information is intended for federal, state, local and tribal government agencies and authorities, private sector critical infrastructure owners and operators, and other entities. It is meant to assist in developing protective and support measures relating to an existing or emerging threat to homeland security.

Bus Operators

Be alert to things that are suspicious or out of place at garages, rail stations, transit centers and shelters. Also be observant of activity, people and vehicles along bus routes.

Make quick and efficient vehicle inspections part of your normal routine. The few minutes you spend doing it may save lives. During pre-trip inspections, layovers or when your bus has been unattended, look for suspicious packages, devices, wires, substances and signs of tampering.

Security sweep checklist:

- Floors
- Above, on and below seats
- Operator's area
- Steps
- Wheelchair lift mechanism
- Compartments
- Lights
- Wheel wells
- Engine compartments
- Bus frame and underbody
- Exhaust system
- Fuel and air tanks
- Rooftop

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Bus Mechanics and Hostlers

When receiving or releasing vehicles, look for suspicious packages, devices, wires, substances and signs of tampering.

Quite often, if something is intentionally “planted” on a vehicle or in a facility, the mechanic or hostler will be the first to notice.

If something seems out of the ordinary during an inspection, report it to your supervisor. In particular, check the engine compartment for foreign objects, a false compartment in the air filter area, additional wires from the battery and unusually clean components and devices. Inspect the fuel and air tanks for inconsistent and missing connections.

Signs of vehicle tampering:

- Scratches or marks made by tools
- Unusually clean or dirty compartments
- Items attached to vehicles or objects with magnets or duct tape
- Open or disturbed compartments and cabinets

Security sweep checklist:

- | | |
|--|--|
| <input type="checkbox"/> Floors | <input type="checkbox"/> Wheel wells |
| <input type="checkbox"/> Above, on and below seats | <input type="checkbox"/> Bus frame and underbody |
| <input type="checkbox"/> Operator's area | <input type="checkbox"/> Engine compartments |
| <input type="checkbox"/> Steps | <input type="checkbox"/> Exhaust system |
| <input type="checkbox"/> Internal lift mechanism | <input type="checkbox"/> Rooftop area |
| <input type="checkbox"/> Compartments | <input type="checkbox"/> External lift mechanism |
| <input type="checkbox"/> Lights | <input type="checkbox"/> Fuel and air tanks |

31

BUS

PREVENTION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Train Operators

Be alert and proactive in looking for suspicious people, vehicle activities, packages, devices and conditions along the right-of-way, in stations and facilities and on the trains.

Security sweep checklist:

- Stations
 - Vending machines
 - Trash containers
 - Turnstiles
 - Booths
 - Stairs/escalators
 - Elevators
 - Pay phones
 - Benches
 - Lights and signs
 - Restrooms
 - Service rooms and cabinets
- Right-of-ways
 - Between and under rails and switches
 - Fences and retaining walls
 - Electrical system components
 - Sign cabinets, poles and lines
 - Communication lines equipment
 - Culverts and overpasses
- Railcars
 - Floors and floor compartments
 - Space between cars
 - Operator's area
 - Undercar equipment area
 - Above, on and below seats
 - Interior compartments and lights

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Rail Mechanics and Hostlers

When receiving or releasing vehicles, look for suspicious packages, devices, wires, substances and signs of tampering.

Quite often, if something is intentionally “planted” on a vehicle or in a facility, the mechanic or hostler will be the first to notice.

If something seems out of the ordinary during an inspection, report it to your supervisor. In particular, check the engine compartment for foreign objects, a false compartment in the air filter area, additional wires from the battery and unusually clean components and devices. Inspect the fuel and air tanks for inconsistent and missing connections.

Signs of vehicle tampering:

- Scratches or marks made by tools
- Unusually clean or dirty compartments
- Items attached to vehicles or objects with magnets or duct tape
- Open or disturbed compartments and cabinets

Security sweep checklist:

- Floor and floor compartments
- Operator’s area
- Undercarriage equipment
- Space between cars (couplers and cables)
- Electrical and other compartments
- Interior compartments and lights
- Above, on and below seats
- Rooftop equipment

33

TRAIN

PREVENTION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

BOMB THREATS

All bomb threats should be addressed in accordance with your company's security plan. It is essential that every precaution be taken to ensure the safety of passengers and employees and to prevent damage to property.

Under no circumstances should any employee or customer touch, handle or move any suspicious package or object they discover.

There are two types of bomb threats:

Specific: The threat gives the location of a bomb and the time it will explode.

Non-Specific: The threat just states there is a bomb placed on the property and does not give a location or the time the bomb will explode.

Notification and Action

Employees receiving a direct call from a person reporting a bomb on the property should attempt to hold the person on the phone as long as possible and obtain as much information as the caller will divulge.

The employee should try to ascertain:

- The exact location of the bomb.
- What time the bomb is scheduled to explode.
- In what kind of container the bomb is located.
- How large the bomb is and whether it will do much damage.
- The caller's name and why he or she is calling to warn about the bomb.
- When the bomb was placed on the property.
- Any other information from the caller.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

IMPORTANT

The person who received the bomb threat must immediately notify police and give all available information.

If a bomb threat is received via letter, email or method other than a telephone call, immediately notify police. Do not handle, erase or alter the document or communication. It is important not to contaminate or alter this kind of evidence.

Specific Bomb Threat at a Station or Building (Time of Detonation and Location Given)

- Notify police and/or **911**.
- Police shall search the target location by utilizing employees, preferably supervisors, who are familiar with the site.
 - Concentrate on those areas accessible to the public.
 - During the inspection, look for any items or objects that appear out of place or suspicious by their presence.
- If a suspicious package/object or bomb is found, or if there has been an explosion, beware of secondary devices. Establish a 300-foot/91-meter perimeter (minimum) and conduct a prompt and orderly evacuation of the area according to the building emergency plan.
- After assurance by police that the area is safe, resume normal operation.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Specific Bomb Threat on a Train or Bus (Time of Detonation and Location Given)

- Notify police and/or **911**.
- Notify the operator to immediately inspect the train/bus. **If a suspicious object is located**, immediately arrange for passengers to be discharged at the nearest station. Avoid causing alarm to passengers.
- If possible, move the train/bus to an isolated track or to an open area with a 300-foot/91-meter (minimum) clear zone.
- If it is not possible to move to an open or isolated area, move to an area clear of people and as far away as possible from critical structures.
- Suspend service in the area where the train/bus is being isolated for inspection.
- For a train, cut traction power by lowering the pantograph/powering down the third rail, and inspect the train. For a bus, turn off the engine and inspect the bus.
 - The inspection is to be done by police and supervisors.
- If the train/bus is parked in a station or other facility, evacuate the passengers and close the station or facility.
- After assurance by police personnel that the train/bus is safe, resume normal operation.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Non-Specific Bomb Threat (No Location or Time Given)

- Notify police and/or **911**.
- Continue normal operation of all service.
- Alert all personnel to be on the lookout for any suspicious packages or objects and to report anything immediately.
- If any suspicious package or object is found on the system, immediately notify police.
- Police will make a systematic inspection of the system.
- Police will make a determination about the stoppage of service resulting from a **non-specific bomb threat**. Command Center will reactivate bus and rail service when cleared by police.



PASSENGER SAFETY

- In any emergency, inform the passengers of the conditions and that help is on the way.
- Assist emergency personnel.

37

BOMB THREATS

PREVEN-
TION

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

SECURITY EXERCISES

Security exercises (either discussion-based or operations-based) should be conducted annually to identify strengths, weaknesses, disconnects and security gaps. Exercises should include the appropriate company representatives and local, state and federal agencies, and should focus on prevention, protection, response and recovery.

Exercises should relate to the organization's security plan and the appropriate countermeasures and mitigation strategies that will be implemented during a heightened level of security or a transportation security incident.

TSA Exercise Assistance

The **Intermodal Security Training and Exercise Program (I-STEP)** enhances the preparedness of U.S. surface transportation systems. It does this through a facilitated exercise program that partners with transportation systems to conduct seminars, workshops, tabletops, games/drills and functional and/or full-scale exercises to address unique transportation security issues and strengthen an organization's security posture.

I-STEP:

- Promotes sound principles and performance-based standards.
- Provides guidance documents.
- Identifies lessons learned and best/effective practices.



NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

I-STEP improves the intermodal transportation industry's ability to prepare for, protect against and respond to a transportation security incident (TSI) by doing the following:

- Increasing awareness
- Improving processes
- Creating partnerships
- Delivering relevant transportation security training exercises

The **Exercise Information System (EXIS)** tool is provided at no cost by TSA as an integral part of I-STEP.

EXIS takes a step-by-step approach as it guides users through exercise planning to execution.

1. **It directs users** to identify the exercise planning schedule and modal focus.
2. **It enables users** to select specific objectives and scenario elements.
3. **It allows users** to plan evaluation criteria, share best practices and lessons learned, and create post-exercise reports.

EXIS communities facilitate information sharing among users. Users can create private communities and sub-communities to delegate tasks to other planning team members or share lessons learned between exercise teams and transportation partners.

EXIS provides transportation stakeholders with resources to design, document and evaluate exercises, and it provides access to transportation security lessons learned and best practices.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

EXIS users have access to more than:

- 120 objectives
- 100 scenario elements
- 20 customized documents

Contact Information

I-STEP Program Office: **571-227-5150**

Email: **ISTEP@dhs.gov**

To become a member of the EXIS community, register at:
<http://exis.tsa.dhs.gov>

CYBERSECURITY

Recognizing that the national and economic security of the U.S. depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. It directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure.

The “Framework for Improving Critical Infrastructure Cybersecurity,” created through collaboration between industry and government, consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risks.



NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

Delivery of the Framework to stakeholders is a measurable National Strategy for Transportation Security (NSTS) goal for DHS, TSA and TSA Surface Division, developed with TSA's Surface Division industry partners.

For more information, contact a TSA Security Specialist at:

TSA.MassTransit@tsa.dhs.gov

The Framework may be found at:

www.nist.gov/cyberframework

The Stop.Think.Connect. Campaign

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.

Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

For more information about Stop.Think.Connect. and a resource tool kit, go to: www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™

EVACUATION

Business continuity plans are critical to consider when conducting exercises on evacuation plans.

Evacuation plans should include sheltering-in-place; primary and secondary muster points; telework capabilities; system requirements; care and needs of employees' families; and operational relationships with support organizations in the same situation locally, regionally or nationally.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

FEDERAL POCs

The **Department of Homeland Security's** overriding and urgent mission is to lead the unified national effort to secure the country and preserve our freedoms.

www.dhs.gov

Homeland Security Information Network (HSIN): HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified (SBU) information. Federal, state, local, territorial, tribal, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

For more information, contact: HSIN.Outreach@hq.dhs.gov

First Observer is a national security program whose mission is to administer an antiterrorism security awareness message to all transportation professionals in support of the National Preparedness Guidelines. The program offers security awareness training to transportation workers engaging in highway, mass transit, freight rail and pipeline modes, recruiting them to act as "First Observers" by reporting suspicious activities of a criminal or terrorist nature.

For training information, go to: www.tsa.gov/firstobserver

Transportation Security Operations Center (TSOC): The TSOC provides 24-hour-a-day, 7-day-a-week, 365-day-a-year coordination, communications, intelligence and domain awareness for all DHS transportation-related security activities worldwide.

NOT FOR DISTRIBUTION FOR REVIEW PURPOSES ONLY

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

TSOC also provides continuous domain and operational awareness for TSA Headquarters of special events, incidents and/or crises; furnishes real-time alerting and reporting to field security organizations; fuses actionable intelligence with operational information across all modes of transportation; and coordinates with federal, state and local homeland security entities.

To report suspicious activities, call TSOC (also known as the Freedom Center) at **1-866-615-5150** or **1-844-TSA-FRST (844-872-3778)**.

The **FBI – Joint Terrorism Task Forces (JTTFs)** are small cells of highly trained, locally based investigators, analysts, linguists, SWAT experts and other specialists from dozens of U.S. law enforcement and intelligence agencies.

www.fbi.gov/about-us/investigate/terrorism/national-joint-terrorism-task-force

STATE & LOCAL POCs

Agency

Phone Number

Local FBI-JTTFs	
State/Local Hazmat Response Team	
State Police	
Local Police Department	
Local Fire Department	
State/Local Fusion Center	
TSA Federal Security Director	
State DOT	
Local DOT	

43

FEDERAL, STATE & LOCAL POCs

POCs

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

**NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY**

You may not copy, distribute, transmit, e-mail, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

MASS TRANSIT & PASSENGER RAIL

COUNTERTERRORISM GUIDE

This guide is intended to provide an awareness of specific issues that should be considered when developing and implementing your organization's security plan.

Company personnel should follow their specific company policies and procedures to prevent, protect and respond to a security incident.



For more information on TSA Mass Transit & Passenger Rail programs or to request additional complimentary guides, contact TSA at: TSA.MassTransit@tsa.dhs.gov



© 2016 QuickSeries Publishing
1-800-361-4653 | www.quickseries.com

01-0808-051-02 | 0808-001
ISBN 978-1-62350-696-4 | Printed in Canada

COPYRIGHTED MATERIAL

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.