Transportation
Security
Administration

HIGHWAY
TRANSPORTATION
INFRASTRUCTURE
COUNTERTERRORISM GUIDE

FOR OFFICIAL USE ONLY

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."

TSA'S MISSION

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

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.

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.

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. 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

4

Suspicious activities that should be reported include the following:

- → 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, highway 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

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)

→ Highway infrastructure (e.g., bridges, tunnels, traffic management centers [TMCs], key intersections)

→ 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.

6

THREATS BY HIGHWAY

International and domestic terrorist groups, as well as unaffiliated individuals, have proven that they will use our highways and vehicles to deliver their attacks.

> In the 1993 World Trade Center bombing, a rented truck was used to deliver a vehicle-borne improvised explosive device (VBIED), killing six people and injuring over 1,000 more.

> A rented truck was used in the 1995 Oklahoma City bombing of the Alfred P. Murrah Federal Building. This is one of the most catastrophic domestic terrorism events in U.S. history. The bombing was responsible for the death of 168 people and injuring hundreds more.

> On April 10, 2015, an attempted homegrown terrorist plot against a U.S. Army post was foiled. An attacker described as a "lone wolf" obtained materials to create a vehicle bomb with the intent to use it against soldiers at Fort Riley, Topeka, KS. The attacker was arming the device for detonation near Fort Riley when he was arrested by the FBI.

Threats covered in this section include:

- → Insider threat
- → Cloned vehicles
- → Hijacking
- → Suspicious packages

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. (Flip to the "ID & Credentialing" tab, page 34, for more information on this.)

8

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

HIJACKING PREVENTION

Hijackers may target trucks, buses or other commercial vehicles to use the vehicle for other illegal purposes, such as for committing robberies, transporting explosives or other materials of destruction, or perpetrating various types of terrorist activities.

Employers should practice safety procedures to prevent hijacking:

→ Increased use of high-quality seals and padlocks

→ "No stop" policy for drivers when possible, especially within two to three hours of the trip origin

→ En route tracking and communications protocols

Drivers should be trained to adhere to strict security measures to prevent hijacking:

→ Do not assume technology such as the Global Positioning System (GPS) will not fail, and identify a backup plan in case of failure.

→ Be aware of safe areas in case you are being targeted. Park in secure areas with ample lighting.

→ Carry a 24-hour emergency telephone number at all times.

→ If you are carrying cargo, make sure you know what it is, especially when carrying a potentially hazardous or high-value load.

→ Check the load when possible to make sure that what is in the vehicle is what is supposed to be there.

→ Inform the dispatcher of your route and then follow it. If the route changes, inform appropriate personnel.

→ Remember, there is safety and security in motion. The most dangerous time for hijacking is when a vehicle is stopped.

10

- → Lock the vehicle every time you make a stop.
  - ▪ Lock the vehicle and close the windows when parked or in slow-moving traffic.
- → Unlock the vehicle for as short a time as possible when stopped to rest, eat or make a delivery.
- → Stop only in designated rest areas where other vehicles are parked.
- → Do not stop to help motorists in trouble, but call for assistance.
- → Be aware of surroundings. Watch for suspicious vehicles at the pickup point, cars or vans that follow the vehicle on the highway or anything that seems out of line.
- → Never pick up hitchhikers.
- → When making a delivery, do not leave cargo unattended.
- → Keep the vehicle license plate number and vehicle identification number (VIN) with you at all times for the vehicle you are operating. They will be critical for law enforcement if the vehicle is stolen or hijacked.

**TARGETS
THREATS**

SUSPICIOUS PACKAGES

Characteristics of suspicious packages:

→ **Inappropriate or unusual labeling:** excessive postage; handwritten or poorly typed addresses; misspellings of common words; missing or strange return address; incorrect title or title without a name; not addressed to a specific person; marked with restrictions (personal, confidential, do not X-ray, etc.); marked with threatening language; postmarked from a city or state that does not match the return address

→ **Appearance:** powdery substance felt through or appearing on the package or envelope; oily stains, discolorations or odor; lopsided or uneven envelope; excessive packaging material such as masking tape, string, etc.

→ **Other suspicious signs:** excessive weight, ticking sound, protruding wires or aluminum foil

Handling of suspicious packages or envelopes:

→ Handle with care. Don't shake, bump or empty the contents of any suspicious package or envelope.

→ Isolate it and look for indicators. Don't open it or smell or taste the contents. Don't carry it, show it to others or allow others to examine it.

→ Alert others in the area about the suspicious package or envelope. Leave the area, close any doors and take actions to prevent others from entering the area. If possible, shut off the ventilation system.

→ Wash hands with soap and warm water to prevent spreading potentially infectious material to face or skin. Seek additional instructions for exposed or potentially exposed people.

→ Notify authorities of the need to investigate; provide as many observational details as possible to help them prepare their response.

PACKAGES

12

TACTICS

International and domestic terrorist groups, as well as unaffiliated individuals, have used vehicle-borne improvised explosive devices (VBIEDs) and improvised explosive devices (IEDs) in their attacks.

The 1993 World Trade Center attack, the 1995 Oklahoma City attack and the 2010 Times Square attempted attack have demonstrated that this tactic is very effective and warrants special consideration when implementing mitigation strategies.

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

VBIEDs (CONT'D)

→ 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

→ 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

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.

→ 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.

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

BOMB THREAT DISTANCES

16

17

TACTICS

Mandatory Evacuation Distance
Inside and outside of buildings. Proceed to **Preferred Evacuation Distance.**

Shelter-in-Place Zone
Move to **Preferred Evacuation Distance.** If unable, seek shelter inside of building, away from windows and exterior walls.

Preferred Evacuation Distance
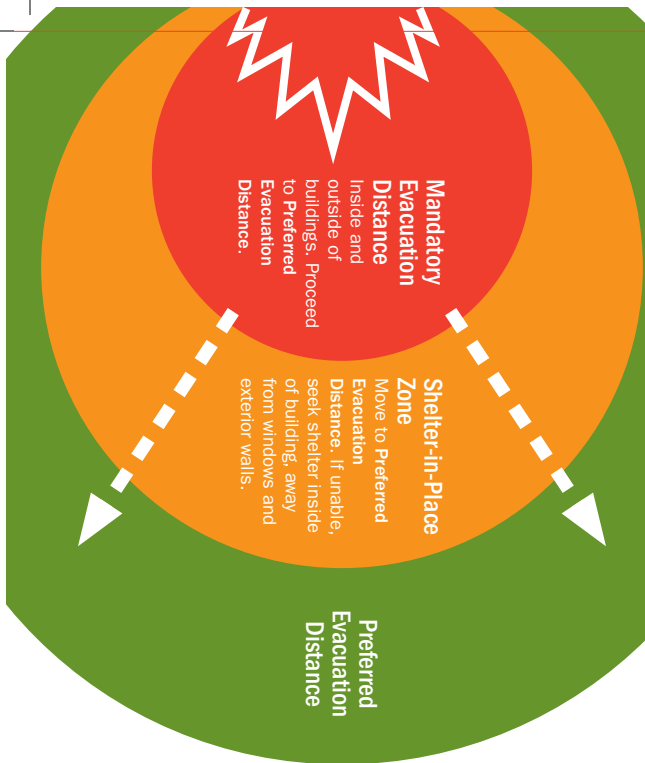
CAUTION!

- 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

ACTIVE SHOOTER

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.

ACTIVE SHOOTER EVENTS

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.

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.

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

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

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

20

SECURITY PLANNING: HIGHWAY INFRASTRUCTURE

The TSA Highway & Motor Carrier Section is recommending that highway infrastructure owners and operators consider implementing the following security action items into their emergency management/security plans where appropriate. Owners and operators should also consider incorporating additional security actions in conjunction with the level of threat as determined by DHS.

When developing security plans, past terrorist activity should always be considered but should not be the only factor in developing your plans. Be on guard for the unprecedented.

General Security

→ Conduct risk assessments on critical assets.

> **Threat + Vulnerability + Consequence = Risk**

→ Incorporate TSA security action items into existing emergency management/security plans.
→ Be aware of industry security practices and, where appropriate, incorporate them into emergency management/security plans.
→ Designate primary and secondary security points of contact (SPOCs) and clearly identify their roles and responsibilities.
→ Establish internal security procedures such as the following:
  - Implement an inventory control process (for vehicles, keys, etc.).
  - Develop an organization-wide information control policy (e.g., security sensitive information policy).
→ Coordinate with local law enforcement to:
  - Ensure proper communication between transportation/traffic management centers and law enforcement.

(Continued from previous page)

- Prepare for the dissemination of security information on dynamic/variable and portable message boards.
- Establish and maintain secure perimeter zones around structures or around critical components (piers/towers).
- Monitor sight lines to critical areas on structures (pay special attention to out-of-place people, objects and vehicles at critical locations).
- Establish a process for removal of abandoned or disabled vehicles parked in secure areas.
- During heightened alerts, consider screening commercial vehicles before they access structures and prohibiting them from transporting hazardous materials.

Personnel Security

→ Ensure employees required to operate commercial vehicles have the appropriate commercial driver's license (CDL) and appropriate endorsements.

→ Develop an organization-wide employee vetting policy that includes background checks on all employees (new hires, temp/permanent employees and contractors) based on duties assigned.

→ Develop an organization-wide policy on issuance and usage of employee identification cards that include (at a minimum) a photo of the individual. Other biometrics (fingerprints, etc.) should be added as appropriate.

→ Ensure all employees visually display identification cards.

Physical Security

→ Develop an organization-wide policy to establish secure physical areas. Establish a tiered-access privilege program that defines the level of access (physical access control) to the secured physical areas.

SECURITY PLANNING

22

→ Deploy physical security countermeasures on identified critical assets (already established through risk assessment), such as cameras, intrusion detection systems, fencing, gates, keypads/PINs, Jersey walls, bollards, etc. These measures should provide stand-off to critical structural components.

En Route Security

→ Establish an emergency communications plan.
→ Establish an appropriate vehicle security program.
→ Implement security actions that correspond to threat levels.
→ Establish security inspection procedures for the organization's vehicles.
→ Establish reporting procedures for security-related incidents.
→ Entity should have standard remote locking system on vehicles.

Unauthorized Access

→ Implement access control systems for vehicles, critical infrastructure and locations storing security-critical information.
→ Make sure doors/access openings to critical areas are locked. Increase monitoring with surveillance cameras and/or detection devices at critical sites.
→ Establish a process with local law enforcement to intercept intruders identified via cameras and/or intrusion detection systems (alarms).

Information Technology Security

→ Develop an organization-wide policy to identify and designate secured virtual areas and establish a tiered-access privilege program that defines the level of access (virtual access control).

Information Technology Security (Cont'd)

→ Establish an Information Sharing Continuity of Operations (IS-COOP) plan (i.e., what to do when the system goes down) as part of the emergency management/security plan. This plan should cover system backup and relocation in the event of an incident, so that all essential capabilities can be continued with little disruption.

→ Establish password standards that include minimum lengths and expiration periods for all employee accesses. Access to critical files and hardware should be limited through additional passwords and firewall support. All passwords should be changed several times a year.

→ Designate an information security officer.

SECURITY INSPECTION CHECKLIST

Bridges

☐ Are there patrols or dedicated law enforcement?

☐ Are critical areas on and beneath the bridge well-lit, and are sight lines to them free of vegetation?

☐ Are there barriers, such as a pier protection system, to prevent vehicle/vessel collision and to provide stand-off to critical bridge members?

☐ Is there a secure perimeter zone around the bridge or critical bridge components (piers/towers)?

☐ Are there unprotected places in the structure where weaknesses can be exploited (e.g., enough space around bearings to place a 6 x 6 x 6-inch object)?

☐ Are areas beneath the bridge fenced to prevent access?

☐ Is public parking allowed under the bridge?

☐ Is there a shoulder, sidewalk or pedestrian access on the bridge?

☐ Is there easy access to critical members (cables, bearings, pile caps, abutments and/or wingwalls)?

- ☐ Are surveillance cameras, emergency telephones or panic buttons present?
- ☐ Does the roadway drain to beneath the bridge (e.g., potential gasoline fire under the bridge from a vehicle accident)?
- ☐ Institute a process to remove abandoned or disabled vehicles.
- ☐ Is the bridge near or on a route to a critical site (e.g., chemical/industrial)?
- ☐ Consider restricting the passage of hazardous or flammable cargo, especially when at high levels of alert.

Tunnels

- ☐ Are there patrols or dedicated law enforcement?
- ☐ Increase stand-off to critical buildings and equipment.
- ☐ Control access to critical systems and buildings (e.g., administration and control buildings, ventilation shafts and machinery, power supplies and emergency generation equipment, pump stations, fire detection and suppression systems, and traffic control).
- ☐ Provide efficient and redundant ventilation systems.
- ☐ Provide efficient and redundant fire suppression systems.
- ☐ Implement automated "one button" first response emergency systems.
- ☐ Implement video surveillance and automated sensor systems (e.g., automated incident-detection systems and intelligent video).
- ☐ Consider restricting the passage of hazardous or flammable cargo, especially when at high levels of alert.
- ☐ Be aware of the utilities supported by the tunnel.
- ☐ Institute a process to remove abandoned or disabled vehicles parked in secure areas.
- ☐ Is the tunnel near or on a route to a critical site (e.g., chemical/industrial)?

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.

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

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.

SECURITY EXERCISES

26

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.

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.

I-STEP / CYBERSECURITY

28

CYBERSECURITY

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: **highwaysecurity@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®
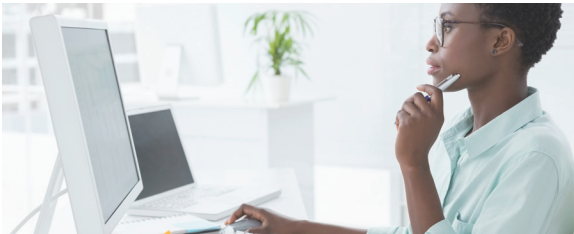
PREVEN-TION

EVACUATION

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

Evacuation plans should include the following:

→ Sheltering-in-place

→ Primary and secondary muster points

→ Telework capabilities

→ System requirements

→ Care and needs of employees' families

→ Operational relationships with support organizations in the same situation locally, regionally or nationally

PERSONAL PROTECTIVE EQUIPMENT

Personal protective equipment (PPE) is designed to protect employees from serious workplace injuries or illnesses. In accordance with applicable Occupational Safety & Health Administration (OSHA) standards, companies must assess their workplaces to determine if hazards are present that require the use of PPE.

Consistent with OSHA requirements, employees should be trained on the following:

→ The proper use of PPE

→ When PPE is necessary

→ What kind of PPE is necessary

→ The limitations of PPE

→ How to don, adjust, wear and doff PPE

→ How to maintain PPE

Regulations are available in the OSHA Standards – 29 CFR Part 1910, Subpart I.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL & NUCLEAR INCIDENTS

INDICATORS OF A POSSIBLE CHEMICAL INCIDENT

→ **Many dead animals/birds/fish** in the same area

→ **Lack of insect life:** Normal insect activity missing, dead insects evident on the ground/water surface/shoreline

→ **Physical symptoms:** Numerous people with unexplained water-like blisters, pinpointed pupils, choking, respiratory ailments and/or rashes

→ **Mass casualties:** Numerous people with unexplained similar serious health problems, ranging from nausea to disorientation to difficulty breathing to convulsions and death

→ **Definite pattern of casualties:** A pattern of casualties associated with possible agent dissemination methods

→ **Illness in specific areas:** Lower incidence of symptoms for people working indoors than out, or the reverse

→ **Unusual liquid droplets:** Numerous surfaces exhibiting oily droplets/film

→ **Areas that look different in appearance:** Not just a patch of dead weeds, but trees, shrubs, bushes, food crops and/or lawns that are dead, discolored or withered

→ **Unexplained odors:** Smells ranging from fruit/flower to sharp/pungent to garlic/horseradish-like to bitter almonds/peach kernels to newly mown hay; the odor is completely out of character with its surroundings

→ **Low-lying clouds:** Low-lying cloud/fog-like condition that is not explained by its surroundings

→ **Unusual metal debris:** Unexplained bomb/munitions-like material, especially if it contains a liquid

INDICATORS OF A POSSIBLE BIOLOGICAL INCIDENT

The three basic groups of biological agents that would likely be used as weapons are bacteria, viruses and toxins. Biological agents can be dispersed by spraying them into the air, by infecting animals that carry the disease to humans and by contaminating food and water. Indicators include the following:

→ Unusual numbers of sick or dying people or animals
- Any number of symptoms may occur, including unexplained gastrointestinal illnesses and upper respiratory problems similar to flu or colds. The time before symptoms are observed depends on the agent used and the dose received. Casualties may occur hours to days or weeks after the incident.

→ Unscheduled and unusual spray being disseminated, especially outdoors during periods of darkness

→ Abandoned spray devices with no distinct odors

→ Placards associated with biological incidents indicating the presence of infectious substances

Delivery Methods

→ **Aerosols:** Biological agents are dispersed into the air, forming a fine mist that may drift for miles. Inhaling the agent may cause disease in people or animals.

→ **Animals:** Some diseases are spread by insects and animals (e.g., fleas, flies, mosquitoes, mice, livestock).

→ **Food and water contamination:** Some pathogenic organisms and toxins may persist in food and water supplies. While some agents can be killed, and toxins deactivated, by cooking food and boiling water, there are agents that are heat resistant and highly toxic that will survive the cooking process.

→ **Person-to-person:** The spread of a few infectious agents is also possible. Humans have been the source of infection for smallpox, plague and the Lassa virus.

BIOLOGICAL INCIDENT

32

INDICATORS OF A POSSIBLE RADIOLOGICAL INCIDENT

→ **Unusual numbers of sick or dying people or animals:** Casualties hours to days or weeks after an incident has occurred

- The time required before symptoms are observed depends on the radioactive material used and the dose received. Additional symptoms include skin reddening and, in severe cases, vomiting.

→ **Unusual metal debris:** Unexplained bomb/munitions-like material

→ **Radiation symbols:** Containers that display a radiation symbol

→ **Heat-emitting material:** Material that seems to emit heat without any sign of external heating source

→ **Glowing material/particles:** Strongly radioactive material that appears to glow

Health and Safety Risk

It is important to understand that a person who has been exposed to radiation is unlikely to pose a radiological health risk to any other person. However, if a relatively high activity gamma source (external exposure) is present at the emergency site, it is possible for an individual to receive a radiation dose that could pose a health risk. It is anticipated that hazmat personnel will have made an initial radiological assessment, and specific safety precautions will be given.

Radiological Assessment

First responders, firefighters or hazmat personnel may have performed an initial assessment or screening for the involvement of radioactive materials. Ask the incident commander (IC) or fire/hazmat chief if radioactive materials have been identified or are suspected.

RADIOLOGICAL INCIDENT

CBRN

IDENTIFICATION & CREDENTIALING

TSA requires that a security threat assessment (STA) be conducted on certain people in the highway and motor carrier community before they can engage in certain duties.

Three TSA highway programs require an STA (and all of them require the payment of a user fee):

1. The Hazardous Materials Endorsement (HME) Threat Assessment Program (HTAP) conducts an STA on any individual who wishes to have the HME included on his or her state-issued commercial driver's license (CDL). The STA for this program is comprised of an immigration, criminal history and terrorism check.

2. The Transportation Worker Identification Credential (TWIC®) Program conducts an STA on any individual requiring unescorted access to secure areas of regulated maritime facilities and vessels. The STA for this program is the same as the HME check and includes an immigration, criminal history and terrorism check.

TSA's HME and TWIC® Programs provide the most complete government security background check available to people employed in the transportation business, using some databases that are not available to commercial background firms.

If a transportation company (truck, bus, rail, pipeline) does business in secure areas of maritime-related worksites or hauls placarded hazardous materials, they may require employees or candidates for employment to obtain a TWIC® or HME respectively. Employers without such a business association may not lawfully require employees to obtain a TWIC® or HME.

SECURITY THREAT ASSESSMENTS

34

SECURITY THREAT ASSESSMENTS

Individuals who work for or intend to seek employment with a transportation business associated with a TWIC®-controlled secure area or placarded hazardous materials may, at their discretion, apply for a TWIC® and HME respectively to enhance their opportunity for employment.

For both the HME and TWIC® Programs, the background investigation reviews criminal history including convictions and incarcerations, citizenship or alien status, and terrorist watch lists. Some criminal offenses may lead to disqualification; appeals or waivers from such disqualification are available on a case-by-case basis.

TWIC® application information must be maintained purely between the applicant and TSA. The governing statute does not permit TSA to share detailed information about disqualifications with employers or potential employers. The result of the application is simply the award of a TWIC® or the lack of that credential.

HME and TWIC® background checks must be renewed every five years. The cost of a TWIC® as of April 2016 is $128, and the HME varies by state.

To enroll in TWIC®, go to:
https://universalenroll.dhs.gov/programs/twic

ID &
CREDEN-
TIALING

TWIC® Card Physical Security Features

First production version imprint:
TWIC® v1.0 08.07

Recent version:
TWIC® Rev 1.1 December 2014

Other versions:
v1.0 09.07, v1.0 10.07, v1.0 01.08, v1.0 04.08, v1.0 09.09, v2.0 06.11, v2.0 10.11

All versions:

→ Holographic overlay on front of all TWIC® cards

→ Clear ¾ patch overlay on rear

→ No manufacturer's brand imprint on ICC chip

Example of TWIC® Card, Rev 1.1 December 2014

Front   **Back**

3. The Indirect Air Carrier (IAC) Program is required for transporters of certain classes of air cargo destined to be loaded on passenger aircraft. IAC threat assessments do not require submission of fingerprints and are not dependent on criminal history checks.

SECURITY THREAT ASSESSMENTS

36

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**

TSA's Highway and Motor Carrier (HMC): The vision of the highway mode is to lead the national effort to maintain the capability to move freely and facilitate commerce in all conditions, and to continuously set the standard for excellence in highway transportation security through our people, processes and technology.

www.tsa.gov/for-industry/surface-transportation

Email: **highwaysecurity@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. 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.
- → 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

FEDERAL POCs

38

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	

HIGHWAY TRANSPORTATION INFRASTRUCTURE
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 or to request additional complimentary guides, contact TSA at **highwaysecurity@dhs.gov** or visit the website at: **www.tsa.gov/for-industry/surface-transportation**