

**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**

# **PIPELINE**

## **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 their government is powerless to prevent terrorism and to get immediate publicity for their causes.

Many terrorist incidents involve small, compartmentalized extremist groups consisting of one or more radicalized individuals. Terrorist cells can blend into a community and remain dormant for extended periods of time. Local, state and federal law enforcement officials 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 terrorist’s 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's important to understand the presence of one or two indicators does not presume terrorist activity, but the presence of several indicators should be reported immediately.

3  
TERRORISM  
INDICATORS

### 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:

- Strengths and vulnerabilities
- Protection/security measures
- Emergency/law enforcement response patterns and times

Suspicious surveillance activity may include the following:

- Recording or monitoring activities
- Drawing diagrams, taking notes, 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

**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 and contraband
- Funneling money from charitable organizations and legitimate businesses

Signs to watch out for:

- 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 or large quantities of fertilizers

# 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  
INDICA-  
TORS

Reportable suspicious “acquiring supplies” activities include but are not limited to:

- Suspicious vehicles in strange or restricted areas or vehicles parked in locations for days without attendance/use
- Storage of large quantities of fertilizer, odd machinery or supplies capable of being weaponized
- 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

**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 hard and soft targets.

These targets could include, but are not limited to:

- Key assets, such as nuclear power plants, dams, government facilities, financial institutions, national monuments, commercial facilities, etc.
- Energy sector specific assets, such as remote pipeline assets, power-generating facilities, substations, fuel farms, gas stations, etc.
- Places hosting large crowds, such as shopping malls, sporting events, convention centers, large hotels, etc.

Contact your state DHS Protective Security Advisor (PSA) for questions concerning potential targets.

Terrorists are opportunistic. They exploit vulnerabilities and choose the time, place and method of attack according to observed or perceived vulnerabilities. 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.

7

TARGETS  
THREATS

## THREATS

Al-Qa'ida, the Islamic State of Iraq and the Levant (ISIL), Daesh (Arabic acronym derived from the phrase "al Dawlah al-Islameyah fi Iraq wal-Sham" or literally, "Islamic State in Iraq and al-Sham") and homegrown violent extremists (HVEs) will use any or all means of surface transportation modes to facilitate attacks.

Past and present examples include:

- The 1993 World Trade Center attack, where a rented truck was used to deliver a VBIED, killing six people and injuring more than 1,000 others.
- The 1995 Oklahoma City bombing of the Alfred P. Murrah Federal Building, which featured the use of a rented truck. This attack killed 168 people and injured 680 others. This attack also damaged or destroyed 324 buildings.
- The September 11, 2001, World Trade Center attack.
- The December 25, 2009, attempt to detonate an explosive device aboard Northwest Airlines Flight 253 above the city of Detroit. This incident resulted in current Advanced Imaging Technology (AIT) security initiatives at domestic airports.
- The September 2015 attempt to bomb a Kansas City, Missouri, World Trade Center (9/11) memorial event. The perpetrator attempted to persuade a confidential FBI informant to coat the shrapnel of the bomb with rat poison in order to maximize casualties.



**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 behaviors associated with insider threat. Early reporting of suspicious behavior or activity often allows for proactive intervention and prevention measures; however, not all behaviors are actionable. It should be noted, suspicious behavior/activity left unchecked could pose threats to individuals or the workplace, or to local, state or 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)
- A newly hired employee exhibiting interest in maps, data sources or secure drives not related to the job, or a newly hired employee with no discernable skill sets related to the job (this may indicate the person was not the one interviewed via phone for the position)
- Mishandling of classified 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 page 27 for more information on this.)

# 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

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



## 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.

### Handling of suspicious packages or envelopes:

- Immediately report the suspicious package or envelope following your established reporting protocol (chain of command, security team). **DO NOT** handle, shake, bump or empty the contents of any suspicious package or envelope.
- Do not carry the package or envelope, 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.

Keep a roll of yellow caution tape handy for use in cordoning off an area.



# 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.

11

VBIEDS

TACTICS

## 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 demonstrated 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 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 operating a vehicle in an overly cautious manner who attempts to abandon the vehicle or acts nervously
- Vehicle drivers displaying suspicious behavior, such as nervousness or sweating, combined with an action 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)

**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 (CONT'D)

- Smoke or strong chemical or fuel odors emanating from a vehicle
- Recent theft of explosives in geographical 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.

## 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.

13

IEDS

TACTICS

Some points to consider include:

- Familiarize yourself with descriptions or pictures of IEDs. Report similar looking items or people carrying similar looking items to your security or law enforcement team. IED component parts include but are not limited to:
  - Power source (battery or similar device)
  - Initiator (blasting cap, switches)
- Keep a safe observation distance if you suspect an IED. If in doubt, leave the area immediately and report the issue.
- Beware of items/containers with electronic components (e.g., circuit boards, cell phones, antennas) that are not in their normal configuration and are connected to containers that could hold explosives or other hazmat.
- 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.
- Do not approach or touch any suspicious device.
- Do not activate a radio or cell phone within 300 feet/91 meters of 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.

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 STAND-OFF CARD



## BOMB THREAT DISTANCES

14

**COPYRIGHTED MATERIAL**

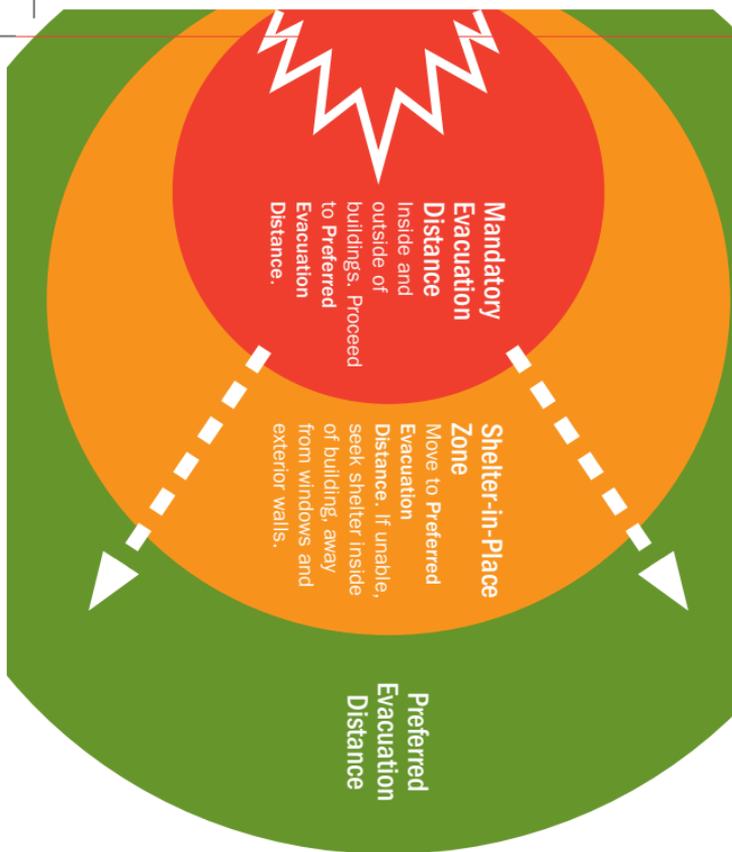
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

# 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.

## 15 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.

## ACTIVE SHOOTER

An active shooter is an individual 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.

# 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.

17

ACTIVE SHOOTER

ACTIVE  
SHOOTER



## 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.



**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 (CONT'D)

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.

### 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

Source: DHS Active Shooter Event Quick Reference Guide



Free online training is available through the Federal Emergency Management Agency (FEMA) Emergency Management Institute, at:

[www.training.fema.gov/is/courseoverview.aspx?code=IS-907](http://www.training.fema.gov/is/courseoverview.aspx?code=IS-907)

# 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

19

### 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](http://www.dhs.gov/national-terrorism-advisory-system)

NTAS

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.

## PIPELINE MODE: GENERAL SECURITY CONSIDERATIONS

When developing security programs, plans and measurable risk-based activities, DHS and TSA recommend analyzing and preparing action plans from both a terrorism and an “all hazards” perspective.

The 2013 DHS National Infrastructure Protection Plan (NIPP) provides solid insight and guidance for developing plans based on both considerations.



The NIPP can be found at:

[www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf](http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf)

The latest edition of TSA's Pipeline Security Guidelines, developed in collaboration with the pipeline industry, provides specific recommendations for industry security practices.

These guidelines can be found at: [www.tsa.gov/for-industry/surface-transportation](http://www.tsa.gov/for-industry/surface-transportation)



Pipeline Security Guidelines  
April 2011



Transportation  
Security  
Administration

## 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.

Industry security professionals may wish to consider implementing the following general recommendations, pulled from the TSA Pipeline Security Guidelines, to establish and maintain a robust security posture within their organizations. This is not a comprehensive list of recommendations. Refer to the Guidelines for detailed information pertaining to the general recommendations noted below:

- Develop a risk-based security program/approach to security applications throughout your company (Pipeline Security Guidelines, Section 4).
- Develop a corporate security plan (Pipeline Security Guidelines, Section 3).
- Consider incorporating the following elements into your security plan:
  - System description
  - Security administration and management structure
  - Risk analysis and assessment methodology
  - Physical security and access control measures
  - Equipment maintenance and testing
  - Personnel screening
  - Communications
  - Personnel training
  - Drills and exercises
  - Security incident procedures
  - National Threat Advisory System (NTAS) response procedures (flip to page 19 in this guide)
  - Security plan review periods
  - Record keeping
  - Cyber/Supervisory Control and Data Acquisition (SCADA) system security measures
  - Critical contact lists
  - Security testing and audits

## 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.

### PIPELINE MODE: GENERAL SECURITY CONSIDERATIONS (CONT'D)

- Assess the relative criticality of all company facilities (Pipeline Security Guidelines, Section 5).
- Develop facility security measures (Pipeline Security Guidelines, Section 6).
- Adopt the National Institute of Standards and Technology (NIST) cybersecurity framework within your organization (flip to page 32 in this guide).

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

- Notify TSA of all security incidents by phone or email as soon as possible (Pipeline Security Guidelines, Appendix B).
- Develop and/or implement a zero-tolerance workplace violence policy and post the policy via prominent signage throughout strategic headquarters and facility locations (common areas, entrances, lunch/break rooms, etc.).

If needed, contact a TSA Pipeline Security Specialist at [pipelinesecurity@tsa.dhs.gov](mailto:pipelinesecurity@tsa.dhs.gov) for security plan or program development assistance.

TSA recognizes many pipeline industry stakeholders own, operate or use significant motor vehicle and freight rail transportation assets and resources in the conduct of business operations. In addition to the general motor carrier guidance noted below, TSA encourages review of both the QuickSeries® *Trucking* and *Freight Rail Counterterrorism Guides*. All TSA Counterterrorism Guides are available in hard copy and electronic/smartphone formats at no cost.

## 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.

### ENERGY PRODUCT TRANSPORTATION CARRIER/ VEHICLE SECURITY CONSIDERATIONS

- Establish a robust communications plan with carrier drivers/operators.
- Establish an appropriate vehicle and cargo security program.
- Implement a seal/lock control program.
- Establish reporting procedures for security-related incidents.
- Establish preplanning, advance notice of arrival and receipt confirmation procedures.
- Preplan primary and alternate routes to reduce risks to the driver, cargo and public.
- Whenever possible, minimize the time an energy product carrier is unattended and ensure the mobile transportation mode is secured at all times if unattended.
- Implement vehicle activation and tracking technologies as appropriate.



## 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.

### ENERGY, OIL & NATURAL GAS COMPANY VEHICLE/ EQUIPMENT HIJACKING PREVENTION

Hijackers may target energy product transport trucks or other commercial vehicles for both their cargo as well as to use the vehicle for other illegal purposes.

Hijacking prevention smart practices for drivers include but are not limited to the following:

- Adopting a “no stop” policy when possible, especially within two to three hours of the trip origin
- Implementing en route tracking and communications protocols
- Knowing or learning the route, especially if it is a new one or has a pickup or drop-off location never visited before
  - Keep fixed driving routes and know alternatives.
  - Designate predetermined checkpoints.
- Incorporating redundant planning in the event of a Global Positioning System (GPS) failure
- Utilizing technology to prevent GPS jamming or spoofing when carrying potentially hazardous cargo
- Knowing safe areas if targeting is detected
  - Park in secure areas with ample lighting.
- Carrying a 24-hour emergency telephone number at all times
- Knowing the cargo, especially when carrying a potentially hazardous or high-value load
- Checking the load when possible to make sure what is in the vehicle is what is supposed to be there

## 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

### HIJACKING PREVENTION

PREVEN-  
TION

- Informing the dispatcher of your route and ensuring route compliance
  - If the route changes, inform appropriate personnel.
- Remembering there is safety and security in motion
  - The most dangerous time for hijacking is when a vehicle is stopped.
- Locking the vehicle every time you make a stop
  - Keep the trailer unit locked securely from the moment the vehicle is loaded.
  - Lock the cab and roll up the windows when parked or in slow-moving traffic.
- Unlocking the truck for as short a time as possible when stopped to rest, eat or make a delivery
- Stopping only in designated rest areas where other trucks are parked
- Avoiding stops at the same places every trip
- Avoiding stopping to help motorists in trouble
  - Call for assistance instead.
- Being 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 picking up hitchhikers
- Ensuring cargo is not left unattended during deliveries
- Keeping the vehicle license plate number and vehicle identification number (VIN) with you at all times for the vehicle you are operating – for both the tractor and trailer
  - These numbers will be critical for law enforcement if the vehicle is stolen or hijacked.

**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.

### CLONED VEHICLES

The use of “cloned” vehicles has become increasingly popular by criminals and terrorists to gain access to restricted or high-profile areas.

Cloned vehicles and similarly disguised vehicles and equipment operators and their drivers/operators impersonating legitimate pipeline businesses, product carriers, maintenance companies, law enforcement, 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
- Vehicle 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 having 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.

## IDENTIFICATION & CREDENTIALING (ENERGY/OIL MOTOR CARRIERS)

TSA requires security threat assessments (STAs) for certain people transporting energy products, refined/crude products and other hazmat energy products via the highway and motor carrier transportation mode before those highway professionals can engage in certain duties.

The following TSA highway programs require an STA (and both 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.

## 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.

### HME and TWIC® (Cont'd)

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>



# 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

ID & CREDENTIALING

## TWIC® Card Physical Security Features

First production version imprint:

**TWIC® v1.0 08.07**

Recent version:

**TWIC® Rev 1.1 December 2014**

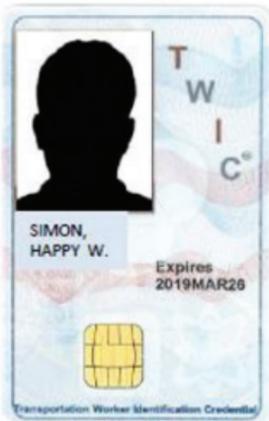
Other versions:

**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

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 EXERCISES

Security exercises should be conducted annually to identify strengths, weaknesses, disconnects and security gaps. Generally, tabletop, functional and full-scale exercises are effective exercises identifying security strengths and vulnerabilities. Exercises should include the appropriate company representatives and local, state and federal security agencies and should focus on prevention, protection, mitigation, response and recovery efforts.

Exercises should relate to the organization's security plan and 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 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

### 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.

31

I-STEP

PREVENTION

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](mailto:ISTEP@dhs.gov)**

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

**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.

### 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.

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:

[pipelinesecurity@tsa.dhs.gov](mailto:pipelinesecurity@tsa.dhs.gov)

or: [highwaysecurity@tsa.dhs.gov](mailto:highwaysecurity@tsa.dhs.gov)

The Framework may be found at:

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

## 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.

### 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](http://www.dhs.gov/stopthinkconnect)

### EVACUATION PLANS/EXERCISES

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

### PERSONAL PROTECTIVE EQUIPMENT

Personal protective equipment (PPE) is designed to protect employees from serious workplace injuries or illnesses. In accordance with applicable 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 proper use of PPE, when and what kind of PPE is necessary, the limitations of PPE, and how to don, adjust, wear, doff and maintain PPE.

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

33

EVACUATION / PPE

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.

# 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

# 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.

35

BIOLOGICAL INCIDENT

## 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.

CBRN

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.

### 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.

## 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](http://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](mailto:HSIN.Outreach@hq.dhs.gov)

**TSA's Surface Division Pipeline Section** works through the division's Industry Engagement Branch within TSA's Office of Security Policy and Industry Engagement (OSPIE). Our vision 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 pipeline security through our people, processes and technology.

[www.tsa.gov/for-industry/surface-transportation](http://www.tsa.gov/for-industry/surface-transportation)

Email: [pipelinesecurity@tsa.dhs.gov](mailto:pipelinesecurity@tsa.dhs.gov)



37

FEDERAL 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.

**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](http://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](http://www.fbi.gov/about-us/investigate/terrorism/national-joint-terrorism-task-force)

**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.

## STATE & LOCAL POCs

39

**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	

**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.

# PIPELINE

## COUNTERTERRORISM GUIDE

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

Company personnel should follow 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 [pipelinesecurity@tsa.dhs.gov](mailto:pipelinesecurity@tsa.dhs.gov) or visit the website at: [www.tsa.gov/for-industry/surface-transportation](http://www.tsa.gov/for-industry/surface-transportation)



© 2016 QuickSeries Publishing  
1-800-361-4653 | [www.quickseries.com](http://www.quickseries.com)

01-0805-051-02 | 0805-001  
ISBN 978-1-62350-312-3 | Printed in Canada

**COPYRIGHTED MATERIAL**

NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.