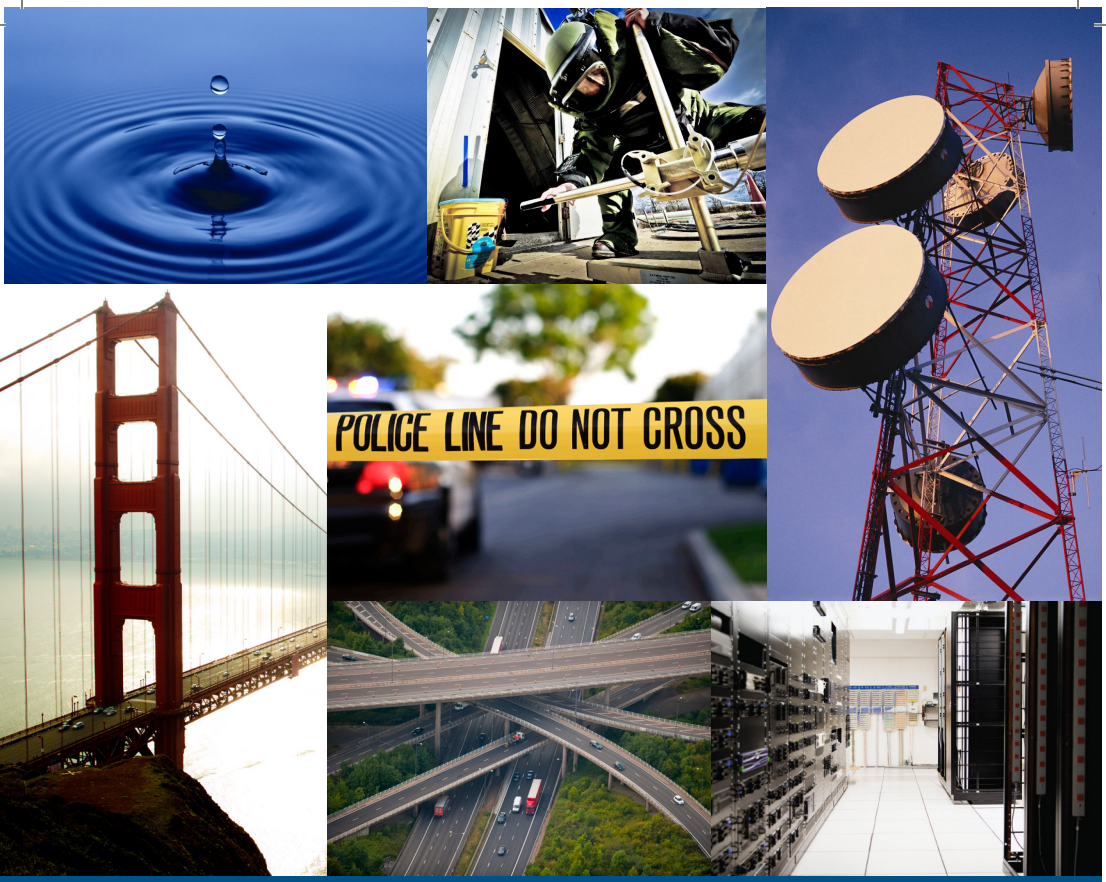

Hometown Security Reference Guide

Homeland Security

Table of Contents

Office of Infrastructure Protection

The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage the risks to their assets, systems, and networks. For more information on IP, visit www.dhs.gov/office-infrastructure-protection.

Vision and Mission

The vision of the Office of Infrastructure Protection is secure and resilient critical infrastructure across the Nation achieved through sound risk management, collaboration, information sharing, innovation, effective program management, and a highly skilled workforce.

The mission is to lead the national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

Protective Security Advisor Program

The U.S. Department of Homeland Security (DHS) proactively engages with Federal, State, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect critical infrastructure through the National Protection and Programs Directorate's Office of Infrastructure Protection (IP) administered Protective Security Advisor (PSA) program. PSAs are physical security experts with core mission areas to facilitate the protection of critical infrastructure:

- **Plan, coordinate, and conduct security surveys and assessments –** PSAs conduct voluntary, nonregulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions. Assessments include options of protective measures to consider that can be implemented to further protect facilities and venues.

- **Plan and conduct risk mitigation training –** PSAs conduct training activities with critical infrastructure owners and operators and community groups (e.g., bomb threat management and active shooter).

- **Support National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events –** PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.

- **Respond to incidents –** PSAs plan for and, when directed, deploy to Unified Area Command Groups, Joint Operations Centers, Federal Emergency Management Agency Regional Response Coordination Centers, and/or State and local Emergency Operations Centers in response to natural or man-made incidents.

For more information or to contact your local PSA, please contact *NICC@hq.dhs.gov*.

The U.S. Department of Homeland Security (DHS) engages closely with private sector and community partners to provide expert counsel and recommendations about protective measures that can be implemented to protect facilities and venues.

The Department encourages businesses to **Connect, Plan, Train,** and **Report.** Applying these four steps in advance of an incident or attack can help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities.

For more information on the Hometown Security Initiative, please visit www.dhs.gov/hometown-security.

Hometown Security: Connect

CONNECT: Reach out and develop relationships in your community, including local law enforcement. Having these relationships established before an incident occurs can help speed up the response when something happens. Contacts that might be considered include:

- Contact the local DHS Protective Security Advisor who is available to support your efforts by emailing NICC@hq.dhs.gov.
- Develop relationships with local law enforcement and businesses in your area. Invite local law enforcement to tour your business.
- Connect with community security and preparedness organizations such as the Federal Bureau of Investigation's public-private partnership program "InfraGard."
- Communicate with your customers and let them know about the security measures you are taking to ensure a positive experience and to maintain public safety.
- If your business is located at or near a Federal facility, connect with DHS's Federal Protective Service at 1-877-4FPS-411.
- Contact your local Fusion Center. For information or to locate your local fusion center, email FusionCenterSupport@hq.dhs.gov.

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. The NTAS consists of two types of advisories:

- **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.
- **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, please visit www.dhs.gov/national-terrorism-advisory-system.

PLAN: Take the time now to plan on how you will handle a security event should one occur. Learn from other events to inform your plans.

- Be aware of current threats related to your geographic region or impacting your business sector.
- Develop security, emergency response, emergency communications, and business continuity plans, while considering the protection of your employees and customers, access control, closed-circuit television, signage, suspicious activity reporting, and parking security.
- Evaluate your security requirements and design a monitoring, surveillance, and inspection program that is consistent with your business operations.
- Develop evacuation and shelter-in-place plans, and ensure that multiple evacuation routes are clearly marked with appropriate signage and that rallying points are available.
- Develop and implement a security plan for computer and information systems hardware and software.
- Engage local first responders (i.e., police, fire, medical) in all of the above efforts to ensure plans are communicated and integrated with response agencies.

Security Planning

When developing security plans, past terrorist activity should always be considered, but should not be the only factor in developing your plans. If applicable, the following planning steps should be considered.

General Security

Identify critical assets and execute the necessary level of protection to mitigate identified vulnerabilities.

- Develop and maintain (update and keep current) a written security plan.
- Designate primary and secondary security points of contact and clearly identify their roles and responsibilities.
- Establish internal security procedures such as:
  - Implement an inventory control process (for vehicles, access door keys, etc.).
  - Develop an organization-wide information control policy (e.g., security sensitive information policy).
  - 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.

Personnel Security

Develop an employee vetting policy, based on assigned duties, that includes recurring background checks.

- Develop a policy on issuance and usage of employee identification cards that include (at a minimum) a photo of the individual. Biometrics (i.e., fingerprints, etc.) should be added as appropriate.

Physical Security

Develop a policy to identify and designate critical assets. Establish a tiered-access privilege program that defines the level of access (physical access control) to the critical assets.

- Avoid use of one-key-fits-all fleet and door lock management.
- Deploy, when and where appropriate, physical security countermeasures on identified critical assets, such as cameras, intrusion detection systems, fencing, gates, keypads/PINs, Jersey walls, bollards, etc. These measures should provide stand-off to critical structural components.

Mobile/Vehicle Security

- Establish an emergency communications and response plan for vehicle security related incidents.
- Implement vehicle activation and tracking technologies.
- Establish security inspection procedures for vehicles.
- Entity should have standard remote locking system on vehicles.
- Be aware of the following and report unusual activity while en route or when stopping:
  - Report suspicious vehicles or people; try to note license plate number and description.
  - Do not allow pick up of unknown individuals (not scheduled).
  - Do not make unauthorized stops.
  - Maintain positive control of all doors.

Information Technology Security

- Develop a carrier/agency-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).
- Establish an Information Sharing Continuity of Operations plan (e.g., 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.

Hometown Security: Train

TRAIN: Provide your employees with training resources and exercise your security and emergency plans often. Plans must be exercised in order to be effective.

- Train employees on identifying and reporting suspicious activities, active shooter scenarios, and bomb threat management.
- Exercise your security, emergency, and communications plan.

Training and Exercises

- Ensure all employees receive security awareness training. Track and maintain training records.
- Develop and implement a policy on drills, exercises, and incident response requirements for all levels of employees in coordination, if appropriate, with external first response agencies.
- Security exercises (either discussion-based or operations-based) should be conducted annually to identify strengths, weaknesses, and security gaps. Exercises should include the appropriate company representatives, local agencies as appropriate, and should focus on prevention, protection, response, and recovery.
- Exercises should test the organization's security plan and the appropriate countermeasures and mitigation strategies that will be implemented during a security incident.
- DHS has the Sector-Specific Tabletop Exercise Program (SSTEP) that allows users to leverage pre-built exercise templates and tailor them to their communities' specific needs in order to assess, develop and update plans, programs, policies, and procedures within an incident management functional area. These exercises are available for download from the HSIN-CI portal. For additional information, contact IP.Exercise@hq.dhs.gov

Contact your local PSA for training and exercise opportunities at NICC@hq.dhs.gov or visit www.dhs.gov/critical-infrastructure-training for more information.

REPORT: Post details of what to watch for and how to report it. Join the "If You See Something, Say Something™" campaign.

- Post details on reporting suspicious activity and encourage employees, tenants, and visitors to report suspicious behavior to property management security or local law enforcement. Things to consider include unattended vehicles; repeat visitors or outsiders who have no apparent business in non-public area; abandoned parcels, suitcases, backpacks, and packages; and other unusual activity.
- Get involved with the Department's "If You See Something, Say Something™" campaign. Find out how by visiting www.dhs.gov/see-something-say-something.
- Report any life-threatening or imminent danger to proper authorities by calling 911.

State and Local Point of Contacts

Agency	Phone Number
Local Federal Bureau of Investigation Joint Terrorism Task Forces (FBI-JTTFs)	
State/Local HAZMAT Response Team	
State Police	
Local Police	
Local Fire	
State/Local Fusion Center	
Other	

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
- For more information and to access resources, visit *www.dhs.gov/activeshooter*

Active Shooter Events

When an active shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation. You have three options: **Run, Hide, or Fight**. Protect life by using Run-Hide-Fight, and promptly initiate law enforcement notification procedures.

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 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 shooters 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 may depend on it.

Cybersecurity Evaluation Program

The Cybersecurity Evaluation Program (CSEP) performs Cyber Resilience Reviews (CRRs), which measure adoption of maturity aspects of cybersecurity risk management using a common, capability-based framework. A CRR serves as a repeatable cyber review of an organization's ability to manage cybersecurity and ensure core process-based capabilities exist. For more information, contact the program at CSE@dhs.gov.

Cybersecurity Evaluation Tool

The Cybersecurity Evaluation Tool (CSET) provides a systematic and repeatable approach to assess the cybersecurity posture of industrial control systems (ICS) networks. CSET is a stand-alone software tool that enables users to assess their network and ICS security practices against industry and government standards and provides prioritized recommendations. To request a CSET CD, email cset@dhs.gov. For all other questions, email cssp@dhs.gov or visit https://ics-cert.us-cert.gov/.

Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. US-CERT is a trusted partner and authoritative source in cyberspace for the Federal government, SLTT governments, private industry, and international organizations. US-CERT offers secure web forms for users to report incidents and submit malware artifacts for analysis. To learn more about US-CERT, visit www.us-cert.gov/about-us.

Industrial Control Systems Cyber Emergency Response Team

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates industrial control systems-related security incidents and information sharing through Fly-Away (Incident Response) Teams with its public and private sector constituents, as well as international and private sector CERTs. ICS-CERT also operates a Malware Lab to analyze vulnerabilities and malware threats to ICS equipment. For additional information, visit www.us-cert.gov/control_systems/ics-cert/. To report suspicious cyber activity affecting ICS, call the ICS-CERT Watch Floor at (877) 776-7585 or email ics-cert@dhs.gov.

Pre-Incident Indicators

Pre-incident indicators can alert officials to a potential terrorist plot if properly reported. It is important to understand that the presence of one or two indicators does not presume terrorist activity; nonetheless, the presence of any indicator should be reported immediately to law enforcement.

Eight Signs of Terrorism

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

1. Surveillance

Action to determine:

- Security strengths and weaknesses
- What security is 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 or attempting to penetrate security and/or access points to facilities

2. Elicitation

Attempts to gain information about operations and security by:

- Mail, email, social media, phone, and/or in person
- Gaining employment to monitor day-to-day activities

3. Testing Security

Attempts to evaluate security capabilities, procedures, and response times by:

- 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
- Attempting to circumvent security to gain access to a restricted area
- Use of bomb threats or false alarms

4. Funding

Signs to watch out for:

- An unusually large transaction paid for with cash or gift cards
- Donations to unknown charities
- Very large purchases in a short time period

5. Acquiring Supplies (legally or illegally)

Suspicious supplies:

- Weapons (including edged weapons and firearms)
- Transportation (including suspicious rental activity)
- Communication systems (i.e., two-way radios and walky-talkies)
- Abnormal amounts or types of chemical precursors (i.e., acids and peroxide)

Suspicious activity:

- 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 unconventional ways

6. Impersonation

Signs to look out for:

- Individuals whose uniforms are missing a badge or company patch, are slightly the wrong color, or otherwise make them appear out of place (i.e., law enforcement, mail carriers, utility workers, or company employees)
- Suspicious actions (i.e., attempting to access prohibited areas)
- Suspicious conversations (i.e., attempting to gauge for highly sensitive information of which they are not privy to)

7. Rehearsal

Practicing the operation may include:

- Putting operatives into position
- Monitoring police or first responder radio channels
- Dry runs and simulated methods of attack
- Measuring emergency response times of area police and firefighters

8. Attack Deployment

- Arrange assets
- Pre-position in the midst of an attack

Counter-IED Training and Awareness

To reduce risk to the nation's critical infrastructure, the Office for Bombing Prevention (OBP) develops and delivers a diverse portfolio of counter improvised explosive device (C-IED) awareness solutions and training courses to build nationwide counter-IED core capabilities and enhance awareness of IED threats.

Bomb-Making Materials Awareness Program (BMAP)

BMAP is a national outreach program, sponsored by the Department of Homeland Security (DHS) in partnership with the Federal Bureau of Investigation, designed to increase public and private sector awareness of the potential illicit use of homemade explosive (HME) precursor chemicals, explosive powders, and improvised explosive device (IED) components.

Federally Sponsored Counter-IED Training Education Resource Catalog

OBP also maintains catalogs of counter-IED preparedness training and education resources that are provided directly by the Federal government or are Federally sponsored.

- Federally Sponsored C-IED Training Education Resource Catalog - SLTT Partners
- Federally Sponsored C-IED Training Education Resource Catalog - Private Sector Partners

Counter-IED Awareness Products

OBP provides a wide array of awareness products that includes cards and posters, checklists, brochures, videos, briefings, and applications designed to share counter-IED awareness information within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents.

Counter-IED and Risk Mitigation Training

OBP offers training through multiple platforms to meet partners' needs. Courses are taught around the United States through direct delivery in a traditional classroom setting or in-residence at FEMA's Center for Domestic Preparedness, online through a virtual instructor-led training (VILT) platform, and through computer-based training (CBT).

Awareness:
- AWR-333: IED Construction and Classification
- AWR-334: Introduction to the Terrorist Attack Cycle
- AWR-335: Response to Suspicious Behaviors and Items
- AWR-337: IED Explosive Effects Mitigation
- AWR-338: Homemade Explosives (HME) and Precursor Awareness
- AWR-340: Protective Measures Awareness
- AWR-341: IED Awareness and Safety Procedures CBT
- AWR-348: Bombing Prevention Awareness
- AWR-349: HME and Precursor Chemicals Awareness for Public Safety CBT

Performance:
- PER-312: Vehicle-Borne Improvised Explosive Device Detection
- PER-336: Protective Measures
- PER-339: IED Search Procedures
- PER-346: Surveillance Detection

Management:
- MGT-451: Bomb Threat Management

For more information on C-IED training, please visit www.dhs.gov/obp or email OBP@hq.dhs.gov.

TRIP*wire*, the **T**echnical **R**esource for **I**ncident **P**revention (https://tripwire.dhs.gov), is the Department of Homeland Security's 24/7 online, collaborative information-sharing network for bomb squad, first responders, military personnel, government officials, intelligence analysts, and security professionals to increase awareness of evolving terrorist improvised explosive device (IED) tactics, techniques, and procedures, as well as incident lessons learned and counter-IED preparedness information. The system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help users anticipate, identify, and prevent IED incidents.

IED Threat Information Sharing - Bombing Prevention at Your Fingertips via TRIP*wire*:

- Use the "What's New" feature for coverage and analysis of the latest domestic and international IED-specific events and incidents
- Leverage the wealth of explosives-related information and analysis to identify explosive hazards, including IED components, and potential terrorist tactics in high-risk operations
- Access critical counter-IED information, such as common site vulnerabilities, potential threat indicators, protective measures, bombing prevention training, planning, and policy guidance to enhance domestic preparedness
- Review expert-validated profiles and cutting-edge terrorist IED videos to recognize operational tactics and prioritize and improve protective measures or training scenarios
- Use the Domestic IED Incident Map and Reports to understand risks in your community

Bomb Threat Guidance

Bomb threats or suspicious items are rare, but should always be taken seriously. DHS offers the following resources that outline in-depth procedures for either bomb threats or suspicious items and will help you prepare and react appropriately during these events.

- DHS – "What to Do In A Bomb Threat Video"
- DHS–Department of Justice (DOJ) Bomb Threat Stand-Off Card
- DHS Bomb Threat Procedures Checklist
- DHS–DOJ Bomb Threat Guidance Brochure

For more information and to access the above bomb threat guidance resources, please visit www.dhs.gov/what-to-do-bomb-threat.

PRIOR TO THREAT

- Plan and prepare
- Develop a Bomb Threat Response Plan
- Provide Bomb Threat Response Plan training to all personnel

IF THREAT IS RECEIVED

- Conduct threat assessment
- Execute appropriate actions outlined in Bomb Threat Response Plan

1. Planning and Preparation

Planning Considerations

- Coordinate with local law enforcement and first responders to ensure smooth handling of a bomb threat
- Develop clear-cut primary and alternate levels of authority (referred to in this document as "Site Decision Maker(s)")
- Select Evacuation Teams and Search Teams
- Develop training plan
- Determine search procedures
- Designate control center locations
- Plan for emergency assistance (police, fire, etc.)
- Establish primary and alternate evacuation routes and assembly areas
- Establish evacuation signal(s)
- Develop a communications plan
- Determine procedures for accessing/shutting off and reactivating utilities

Preparation Considerations

- Control building access
- Implement strict master key control
- Inspect incoming parcels
- Safeguard confidential material
- Keep exits unobstructed
- Ensure adequate internal/external emergency lighting
- Utilize electronic surveillance

2. Emergency Toolkit Contents

Items you may want to consider including in your Emergency Toolkit that will be taken to the Incident Command Post.

Building Facility

- Complete set of master keys: coded to rooms and corresponding with a printed key list
- Blueprints and floor plans or site map of building
- Video, photographs, or CD depicting building interior and exterior

Emergency Response Plans

- Copies of the Site Crisis Response Plan, Bomb Threat Plan, and Crisis Management Plan
- A list of the following phone numbers:
  - Site Decision Maker(s)
  - Police/Fire/Emergency Medical Services (EMS)
  - Federal Bureau of Investigation (FBI)
  - Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
  - Postal Inspector
  - Nearest hospital
  - Facility emergency names and phone numbers

Personnel Information

- Building emergency response team member contact information and assignments
- List of personnel trained in CPR and/or first aid
- Updated list, with pictures if possible, of all staff/personnel
- Staff/visitors sign-in/out sheets that include names and dates; Include provision for staff/visitors transported to medical facilities
- List of staff with special needs and description of need
- Contact information for neighboring/contiguous buildings

Additional Emergency Action Resources

- Reflective vests for building emergency response team members with identifying marks
- Bullhorn with charged batteries
- AM/FM portable radio
- Flashlights and batteries
- Local street and zone maps
- Clipboards
- Writing materials (legal pads, pens, pencils, markers)
- Plastic red/yellow tape for cordoning off areas

3. Receiving a Threat

Phoned Threat

- **Remain calm and DO NOT HANG UP**
- If possible, signal other staff members to listen and notify Site Decision Maker(s) and authorities
- If the phone has a display, copy the number and/or letters on the window display
- Write down the exact wording of the threat
- Keep the caller on the line for as long as possible and use the Bomb Threat Checklist to gather as much information as you can
- Record, if possible
- Fill out the Bomb Threat Checklist immediately
- Be available for interviews with the building's emergency response team and law enforcement

Verbal Threat

- If the perpetrator leaves, note which direction they went
- Notify the Site Decision Maker(s) and authorities
- Write down the threat exactly as it was communicated
- Note the description of the person who made the threat:

• Name (if known)	• Race
• Gender	• Type/color of clothing
• Body size (height/weight)	• Hair and eye color
• Distinguishing features	• Voice (loud, deep, accent, etc.)

Written Threat

- Handle the document as little as possible
- Notify the Site Decision Maker(s) and authorities
- Rewrite the threat exactly as is on another sheet of paper and note the following:
  - Date/time/location document was found
  - Any situations or conditions surrounding the discovery/delivery
  - Full names of any personnel who saw the threat
  - Secure the original threat; **DO NOT** alter the item in any way
  - If small/removable, place in a bag or envelope
  - If large/stationary, secure the location

Emailed Threat

- Leave the message open on the computer
- Notify the Site Decision Maker(s) and authorities
- Print, photograph, or copy the message and subject line; note the date and time

4. Threat Assessment

All threats should be carefully evaluated. One must consider the facts and the context, and then conclude whether there is a possible threat.

Low Risk

Lacks Realism: A threat that poses a minimum risk to the victim and public safety. Probable motive is to cause disruption.

- Threat is vague and indirect
- Information contained within the threat is inconsistent, implausible, or lacks detail
- Caller is definitely known and has called numerous times
- The threat was discovered instead of delivered (e.g., a threat written on a wall)

Medium Risk

Increased Level of Realism: Threat that could be carried out, although it may not appear entirely realistic.

- Threat is direct and feasible
- Wording in the threat suggests the perpetrator has given some thought on how the act will be carried out
- May include indications of a possible place and time
- No strong indication the perpetrator has taken preparatory steps, although there may be some indirect reference pointing to that possibility
- Indication the perpetrator has details regarding the availability of components needed to construct a bomb
- Increased specificity to the threat (e.g., "**I'm serious!**" or "**I really mean this!**")

High Risk

Specific and Realistic: Threat appears to pose an immediate and serious danger to the safety of others.

- Threat is direct, specific, and realistic; may include names of possible victims, specific time, and location of device
- Perpetrator provides his/her identity
- Threat suggests concrete steps have been taken toward carrying out the threat
- Perpetrator indicates they have practiced with a weapon or have had the intended victim(s) under surveillance

5. Staff Response

Considerations for Site Decision Maker(s)

- Immediately contact local law enforcement if not done
- Limit access to building
- Review Bomb Threat Response Plan
- Conduct Threat Assessment
- **Determine if search is warranted based on Threat Assessment**

If Search Is Initiated

- Enact Search Plan
- Communicate situation to staff/personnel and request that they make a quick and complete visual scan of their personal workspace for anything unusual
- Account for all personnel
- Assemble Search and Evacuation Team(s) and update about bomb threat condition

General Search Team guidelines:

- Search Teams make a quick and complete visual scan of the search area
- Divide individual rooms/areas into search levels
- Take special note of any object(s) that seem out of place
- Check ledges, balconies, waste baskets, and false ceilings and floors
- Check for unusual odors and listen for any unusual background noises
- If anything unusual is noticed, move people away from the potential hazard and immediately report the location of the object(s) to the Site Decision Maker(s)

NOTE: Use of radio communications is NOT recommended unless the area has been searched and cleared.

For additional information and products on bomb threats and improvised explosive device (IED) search procedures, please visit the DHS Office for Bombing Prevention website at ***https://www.dhs.gov/what-to-do-bomb-threat***

6. Suspicious Item

A **suspicious item** is anything (e.g., package, vehicle) that is reasonably believed to contain explosives, an IED, or other hazardous material that requires a bomb technician to further evaluate it. Potential indicators are threats, placement, and proximity of the item to people and valuable assets. Examples include unexplainable wires or electronics, other visible bomb-like components, unusual sounds, vapors, mists, or odors. Generally anything that is **H**idden, **O**bviously suspicious, and not **T**ypical (**HOT**) should be deemed suspicious.

If Suspicious Item Is Found

- **DO NOT** touch, tamper with, or move the item
- Immediately report item to Site Decision Maker(s) and local law enforcement/first responders
- Site Decision Maker(s) must:
  - Ensure area is secured and cleared of personnel
  - Notify Search Teams
  - Ensure emergency responders are briefed
  - Evacuation and Search Teams should remain available to assist and inform evacuees, media, staff, and others

Considerations for Site Decision Maker(s)

- Not all items are suspicious
- An **unattended item** is anything (e.g., bag, package, vehicle) not in someone's possession and where there are no obvious signs of being suspicious (see above), especially if no threat was received

NOTE: The discovery of one suspicious item should not automatically mean the conclusion of a search. More suspicious items may be present.

The Site Decision Maker(s) must take the discovery of multiple suspicious items into consideration during the planning and execution stages of the facility's Bomb Threat Response Plan.

7. Lockdown/Evacuation

Considerations for Site Decision Maker(s)

- Repeat Threat Assessment:
  - Is the threat still credible?
  - Were any suspicious items located (if search was initiated)?
- Based on Threat Assessment, search (if initiated), and totality of circumstances, determine if addition measures are warranted:
  - Partial or full lockdown?
  - Partial or full evacuation?
  - No further action?

If Evacuation Is Initiated

- Select evacuation routes and assembly areas that are not in the vicinity of the suspicious item; ensure these routes have been searched and cleared
- Notify police/fire/EMS of evacuation and request assistance
- Account for all personnel
- Evacuation Team confirms the building is empty
- Bring emergency kit and building trauma kits, if available
- Advise all evacuees to remove all personal items (e.g., purses, backpacks)

Continuing Actions After Evacuation

- Debrief emergency services and assist in coordinating further actions
- Take accountability and report
- Open media, medical, and family areas — brief regularly
- As appropriate, determine reoccupy or dismiss action
  - Reoccupy when cleared and deemed appropriate
  - Dismiss in consultation with site administration
  - Notify all personnel of decision and ensure accountability
- Site Decision Maker(s) should remain on-scene until situation is resolved or until relieved by another administrator

A Final Note

Every bomb threat requires professional judgment and should be handled in accordance with the facility's needs. Site Decision Maker(s) and administrators should periodically review Federal guidance and work with local first responders to establish a Bomb Threat Response Plan that addresses each risk level appropriately and is optimal for their building(s) and personnel.

Chemical Incident

Indicators of a possible chemical incident include:

- Many dead animals (e.g., fish, birds) in the same area
- Lack of insect life: Normal insect life activity missing, dead insects evident on the ground, water surface, or 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 health problems, ranging from nausea and disorientation, to difficulty breathing, 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

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 of a possible biological incident include:

- Unusual numbers of sick or dying people or animals in a concentrated area
- Any number of symptoms mays occur, including unexplained gastrointestinal illnesses and upper respiratory problems similar to colds or flu.
- 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 signaling 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.
- **Animals:** Some diseases are spread by insects and animals (e.g., fleas, flies)
- **Food and water contamination:** Some pathogenic organisms and toxins may persist in food and water supplies. Not all agents can be neutralized by boiling or cooking. Some are heat resistant and highly potent.
- **Person–to–person:** The spread of a few infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and Lassa virus.

Radiological Incident

Indicators of a possible radiological incident include:

- Unusual numbers of sick or dying people or animals.
- 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.
- Unusual metal debris or unexplained bomb/munition like material.
- Containers that display a radiation symbol.
- Material that seems to emit heat without any sign of external heating source.
- Material or particles that appear 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.

Active Shooter

- DHS Active Shooter Preparedness program offers free courses, materials, and workshops to better prepare you to deal with an active shooter situation and to raise awareness of behaviors that represent pre-incident indicators and characteristics of active shooters.
- For more information and to access active shooter resources, visit www.dhs.gov/activeshooter.

Protective Security Advisors

- Protective Security Advisors proactively engage with government partners and the private sector to protect critical infrastructure.
- For more information or to contact your local PSA, please email NICC@hq.dhs.gov.

Additional Resources

- The Ready Campaign provides help with planning for businesses. For more information, visit www.dhs.gov/ready.
- "If You See Something, Say Something™" is more than just a slogan. Call local law enforcement. Visit www.dhs.gov/see-something-say-something for information.
- Counter-improvised explosive device information and resources are available at www.dhs.gov/bombing-prevention-training.
- Review the "What You Can Do When There Is a Bomb Threat" checklist and watch the video available at www.dhs.gov/what-to-do-bomb-threat.
- Learn about DHS cybersecurity programs and the Cybersecurity Awareness Campaign. Visit www.dhs.gov/topic/cybersecurity for information and resources.
- Get the latest cyber tips from the U.S. Computer Emergency Response Team.
- InfraGard is a public-private partnership between the FBI and the private sector that represents individuals from businesses, academic institutions, State and local law enforcement, fire and emergency management agencies, as well as other participants dedicated to sharing information, education, and intelligence. Visit www.infragard.org/ for more information.