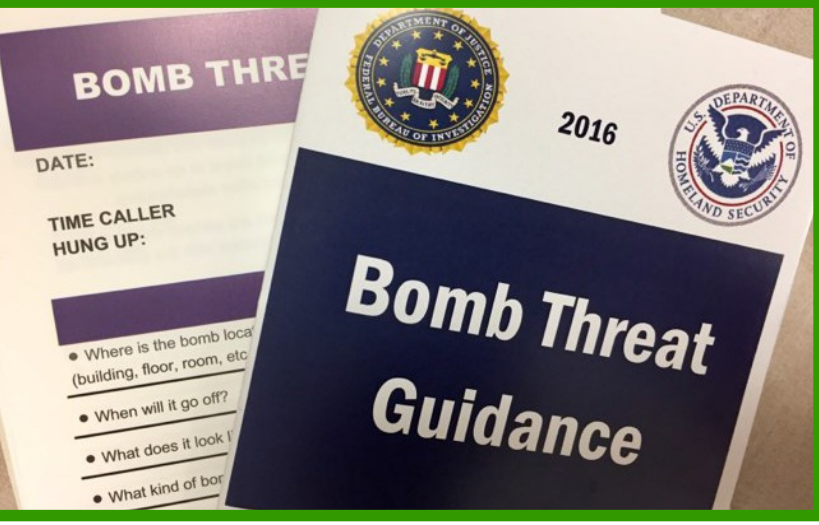
CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.



Security and Resiliency Guide

Counter-Improvised Explosive Device (C-IED) Annex for Healthcare and Public Health Facility Stakeholders

Table of Contents

Introduction 1

Purpose 1

Background 1

Definitions 2

Sector Definition 2

Risks Posed by IED Incidents 4

C-IED Goals and Tasks 6

Introduction 6

Goal 1 – Use and share risk information to guide IED-related physical security, law enforcement, and emergency response activities 7

Goal 2 – Identify and report IED-related suspicious activity 10

Goal 4 – Implement site-specific protective measures to prevent and minimize the impact of IED incidents 12

Goal 5 – Utilize IED screening and detection methods in high-risk environments 14

Goal 6 – Take immediate safety precautions for bomb threats, suspicious items, and IEDs 15

Goal 7 – Safely coordinate response activities at IED incident sites 17

Conclusion 21

Appendix 1: Healthcare Facility C-IED Tasks 22

Appendix 2: Aligning Role-Based Responsibilities 23

Appendix 3: Goals and Tasks Checklist 25

Appendix 4: Healthcare and Public Health Sector C-IED Resources 29

Appendix 5: C-IED Planning Process 31

Appendix 6: Healthcare and Public Health Sector C-IED References 32

The information you have accessed or received is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. DHS does not endorse any entity, product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

Introduction

Purpose

Bombings using improvised explosive devices (IEDs) are a common security concern related to terrorism and violence in the United States (U.S.). Multiple high-profile, domestic incidents have occurred over the last several decades, and international attacks are frequently in the news. Healthcare facilities are not immune from IED incidents, including bomb threats, suspicious items or behavior, and attacks using IEDs. Between May 2016 and May 2019, media reports indicated that there were 243 healthcare-related IED incidents in the U.S.[1] According to the World Health Organization (WHO), from 2016 to 2018, there was an annual average of 337 attacks on healthcare targets across 19 overseas countries that reported data. During that time span, those attacks resulted in an average of 325 deaths and 415 injuries per year. On average, 60% of attacks were bombings.[2]

This guide defines actions that management and staff at healthcare facilities can take to understand and improve their ability to perform counter-IED (C-IED) activities and make security decisions. This guide is designed to provide personnel at healthcare facilities with:

1) A practical framework to examine their ability to perform C-IED activities, and

2) Supporting guidance and materials to strengthen their C-IED preparedness.

As each healthcare facility is unique in its size, mission, complexity, and location, no specific guidance can apply to all. For this reason, the information provided in this guide is meant to provide suggestions and examples of what other leading facilities are doing as options for management teams to consider to enhance their facility's C-IED preparedness.

Benefits of the Guide to Healthcare and Public Health (HPH) Sector Stakeholders

This guide provides useful information to management and staff as they seek to improve security at their facilities. Through this guide, management and staff can:

- Gain a better understanding of their existing C-IED practices and needs;
- Obtain information to support C-IED preparedness efforts, such as risk assessments, planning, equipment purchases, and staff training; and
- Collaborate and communicate more effectively with their healthcare counterparts, community first responders, and government agencies.

Background

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) plays a key role in coordinating efforts with both public and private sectors, including healthcare facilities, to build capabilities to prevent, protect against, respond to, and mitigate bombing incidents. To assist stakeholders with enhancing preparedness for IED incidents, CISA's Office for Bombing Prevention (OBP) and other U.S. Government stakeholders developed the Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance (SRG C-IED). The SRG C-IED is a consolidated reference guide of C-

[1] Data is open-source intelligence gathered by DHS's TRIP*wire* through open source reporting by news outlets, social media, and other multimedia channels related to explosive activity.
[2] World Health Organization. *Attacks on Healthcare Dashboard*. 2016, 2017, 2018. https://www.who.int/emergencies/attacks-on-health-care/archive/en/

IED preparedness information for homeland security stakeholders. It provides an overview of IED threats, a set of common C-IED goals, associated tasks, as well as links to federal government C-IED resources.

This Guide is an annex to the SRG C-IED, developed to support the specific needs of healthcare facility stakeholders. Healthcare facility representatives, including security managers, participated in its development to ensure the annex reflects common operating procedures and the most significant security concerns. Major associations and working groups also participated, including the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC), HPH Sector Government Coordinating Council (GCC), American Hospital Association (AHA), and the International Association for Healthcare Security & Safety (IAHSS). OBP conducted facility site visits, as well as a workshop with health sector representatives, to gain insight into security best practices, gaps, and potential resources that would support C-IED preparedness for the HPH Sector.

Definitions

The following definitions may be useful for security managers and staff as they read this guide and examine their ability to perform C-IED activities and make decisions to prevent, protect against, mitigate, and respond to IED-related threats.

- **IED**: A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.
- **IED Incident**: Any event that involves a real or suspected IED threat, including IED detonations, bomb threats, the use of hoax devices, discovery of bomb-making components, or the theft of explosives or precursor materials.
- **Countering IEDs**: The interdisciplinary process for developing, implementing, evaluating, and adjusting measures to prevent, discover, protect against, mitigate, respond to, and recover from IED incidents and their consequences.

Sector Definition

The HPH Sector works to sustain the essential functions of the Nation's healthcare and public health delivery system and to support effective emergency preparedness and response to significant hazards. The HPH Sector's critical infrastructure is classified according to service types and functional categories, or subsectors, resulting in six private and two government subsectors that include: Direct Patient Care; Health Information and Technology; Health Plans and Payers; Laboratories, Blood, and Pharmaceuticals; Mass Fatality Management Services; Medical Materials; Public Health; and Federal Response and Program Offices.[3]

Figure 1: Healthcare facility stakeholders
Property of DHS

[3] (Healthcare and Public Health Sector-Specific Plan - An Annex To The NIPP 2013 2016)

Healthcare Facility Stakeholders

For the purposes of this guide, healthcare facility stakeholders include the following:

- **Security**: Protect staff, patients, and visitors and ensure that all areas of the healthcare facility property are secure; includes conducting perimeter patrols, monitoring internal/external activity, and enforcing rules and regulations.
- **Administration/Operations**: Oversee day-to-day operation of the healthcare facility, including resource allocation, as well as the development and implementation of processes and procedures. Also includes management roles, such as the Board of Directors and Chief Executive Officer (CEO).
- **Non-Clinical Staff**: Perform non-clinical support functions for healthcare facilities, such as telecommunications, food services, information technology, and health records. Two specific examples are:
    - **Reception Desk Staff**: Provide clerical support to departments by managing desk phones, scheduling appointments, admitting and discharging patients, and facilitating patient flow.
    - **Facilities Staff**: Perform facility maintenance and oversight, including facility equipment and deliveries.
- **Clinical Staff**: Deliver direct patient care, including the physicians, nurses, and other clinical personnel. Also includes diagnostic, therapy, and pharmacy staff, as well as students.
- **Patients and Visitors**: Seek medical care in the facility, or friends and family who accompany someone seeking care.

Risks Posed by IED Incidents

Between May 2016 and May 2019, 243 domestic HPH sector-related IED incidents were reported. These incidents were most frequently bomb threats or suspicious packages, accounting for 66% and 26% of events respectively.[4] Knowing and understanding the specific risks IEDs pose to healthcare facilities is a necessary first step to selecting and prioritizing the C-IED goals and tasks presented in this annex.

Risk is generally defined as the potential for an unwanted outcome from an incident as determined by its likelihood and consequences. A C-IED risk analysis should address three core questions:

- How likely is it that different types of IED incidents will occur (i.e., bomb threats, suspicious items, attack with an IED)?
- If one or more type of IED incident occurred, what would be the consequences?
- How vulnerable is the facility to an attack?

As an example, a large downtown healthcare facility in a major metropolitan area may be an attractive target for an IED incident because of the large number of people present at any given time and the relative ease of access. Alternatively, a suburban or rural healthcare facility, which may have fewer security resources, could be a desirable target for a series of bomb threats or suspicious packages. As a result of these different risk factors, the large downtown healthcare facility will have different priorities than the suburban or rural healthcare facility. These priorities will affect the decisions that the managers for each of these facilities make to strengthen their C-IED preparedness through the goals and tasks outlined in this Annex.

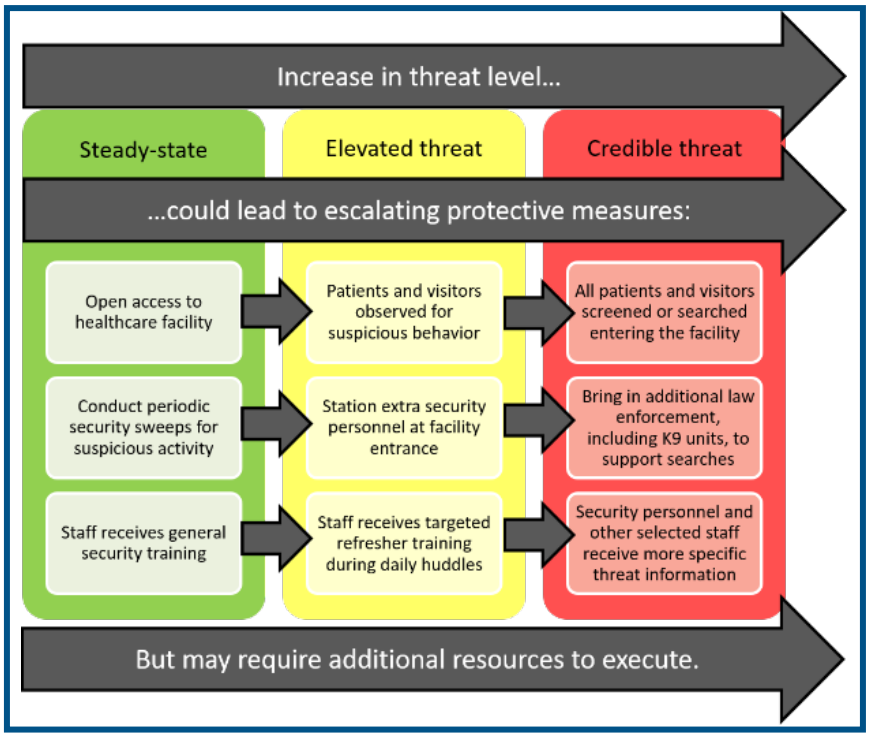


Figure 2: Example actions in response to a changing threat environment
Property of DHS

Furthermore, any change in the likelihood of an IED incident (e.g., a credible threat to healthcare facilities in a particular city) could affect the actions those facilities take to implement C-IED tasks (see Figure 2). For example, day-to-day operations during the steady-state IED threat environment likely means keeping an eye out for suspicious activity, while conducting business as usual.

During an elevated threat environment, however, the healthcare facility may decide to add additional security to monitor the lobby or waiting rooms to look for suspicious behavior. Finally, following a

[4] Data is open-source intelligence gathered by DHS's TRIP*wire* through open source reporting by news outlets, social media, and other multimedia channels related to explosive activity.

nearby bomb detonation, the facility may decide the risk is significant enough to physically search everyone that enters the facility.

Given the varied types and degrees of risks each healthcare facility faces, and their evolution over time, management needs to determine the most relevant areas to enhance the preparedness of their facility. The next section outlines C-IED goals to prevent, protect against, mitigate, and respond to bomb threats and incidents, and example tasks to implement these goals. Each facility may focus on or omit specific goals or tasks based on their own risk assessment and planning requirements. Descriptions of each C-IED task include examples from industry documents and discussions with stakeholders that summarize a spectrum of approaches for management to consider, based on their respective risks, as they build and/or improve C-IED preparedness over time.

Following the next section on goals and tasks are five appendices to support further learning and action:

- **Appendix 1** shows a visual representation of the tasks healthcare facility stakeholders may take throughout the facility.
- **Appendix 2** provides a broad list of C-IED tasks, to include the example tasks, and aligns them to the most applicable stakeholder within the healthcare facility.
- **Appendix 3** provides a list of C-IED goals and tasks in an operational checklist format for healthcare facilities to use when self-assessing their preparedness.
- **Appendix 4** lists resources available to healthcare facilities to build and improve their C-IED preparedness.
- **Appendix 5** outlines key steps in the C-IED planning process, as defined in the SRG C-IED.
- **Appendix 6** lists the references used to develop this guide.

C-IED Goals and Tasks

Introduction

Counter-IED Goals

There are 10 common C-IED goals outlined in the SRG C-IED. These goals serve as benchmarks that stakeholders can review and consider for implementation in support of reducing the overall risk posed by IED threats. Considering the overall internal needs of healthcare facilities, this annex focuses on six (bolded) of the ten C-IED goals that are most likely to be relevant. To learn more about the details, example tasks, and resources for the goals not addressed here, reference the SRG C-IED.

Goal
1. Use and share risk information to guide IED-related physical security, law enforcement, and emergency response activities. *Application to HPH: The C-IED tasks in this category include the activities by which healthcare personnel use and share information to improve coordination between stakeholders.*
2. Identify and report IED-related suspicious activity. *Application to HPH: The C-IED tasks that align to this goal include the activities to help increase awareness and preparedness for identifying and communicating IED-related suspicious activity.*
3. Prevent the acquisition of explosives and explosive precursor chemicals used in IEDs. *Omitted: Healthcare facilities are not considered a primary acquisition source for explosives or precursor chemicals.*
4. Implement site-specific protective measures to prevent and minimize the impact of IED incidents. *Application to HPH: These C-IED tasks include the activities by which healthcare personnel strive to deter IED threats and protect against an IED attack at their facilities.*
5. Utilize IED screening and detection methods in high-risk environments. *Application to HPH: These C-IED tasks discuss various screening and detection methods that healthcare personnel can utilize to identify and prevent IEDs and IED components from entering healthcare facilities.*
6. Take immediate safety precautions for bomb threats, suspicious items, and IEDs. *Application to HPH: These C-IED tasks include the activities by which healthcare personnel can effectively address IED threats to their facilities in support of increasing safety, minimizing potential disruptions, and assisting law enforcement and first responders.*
7. Safely coordinate response activities at IED incident sites. *Application to HPH: These C-IED tasks include activities by which healthcare personnel can effectively and safely respond at the IED incident site.*
8. Request Public Safety Bomb Squad assets to diagnose suspicious items and render-safe IEDs. *Omitted: Healthcare facilities are not responsible for render-safe procedures.*

Goal
9. Provide IED-specific emergency medical response. *Omitted: This Annex focuses on securing healthcare facilities against IED incidents, for resources on providing explosive-related medical care, reference the SRG C-IED.*
10. Reduce the psychological and economic impacts of IED incidents. *Omitted: This Annex focuses on securing healthcare facilities against IED incidents, for resources on explosive-related mental health management, reference the SRG C-IED.*

Goal 1 – Use and share risk information to guide IED-related physical security, law enforcement, and emergency response activities.

The following C-IED tasks include the activities security managers and staff can incorporate to effectively use and share information with all stakeholders involved.

Establish relationships with local law enforcement, fire, emergency medical services (EMS), and fusion centers.

Proactively establishing relationships with key incident first responders such as local law enforcement agencies, fire, and EMS creates the framework through which pertinent information can be shared prior to, and in the event of, an incident. Each of these entities plays a vital role in helping healthcare facilities prepare for, or respond to, a bombing incident. Consider utilizing mechanisms such as memorandums of understanding to establish the foundation for effective incident communication, response plans and procedures, facility needs, evacuation plans, and more.

Additionally, consider establishing a relationship with the local fusion center. Fusion centers serve as the primary focal points within the local area for gathering, analyzing, and sharing threat-related information. They provide interdisciplinary expertise and situational awareness to help inform the decisions of healthcare community leaders to prepare their facilities. Similarly, resources such as CISA's TRIP*wire*, an online information and resource-sharing portal, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) can provide valuable awareness information for healthcare facilities.

These ongoing relationships can help a healthcare facility:

1) **Assess the risk of an IED incident**. Leveraging relationships can be used to help healthcare facilities assess the likelihood and consequences of an IED incident that directly impacts the healthcare facility and/or adjacent facilities.

2) **Monitor IED-related security information.** It is valuable to understand the context of past and potential future IED use in relation to a specific healthcare facility to determine what type of events are most likely. This is valuable information to assist a facility in preparing accordingly. Be aware of new circumstances or information that may increase or decrease the threat of an IED. For example, a special event nearby, such as a marathon or demonstration, could increase the threat.

Establish relationships with government and industry stakeholders to maintain the routine exchange of IED-related security information—including alerts, attack indicators and warnings, and advisories. Some examples of partnerships include the following:

- Private sector liaisons from law enforcement agencies
- Local bomb technicians, who are part of local fire or law enforcement agencies
- DHS Protective Security Advisors (PSAs)
- Local emergency managers, as part of their ongoing Threat and Hazard Identification and Risk Assessment process
- Local, regional, or state fusion centers
- Healthcare or public health associations
- Regional health care coalitions (HCCs)
- Local business associations

Alert Levels

Incorporate "alert levels" into facility emergency plans. These levels can be tied to local or federal advisory systems, such as the National Terrorism Advisory System, or to criteria defined by the facility. The plan can also outline specific protective actions for each level (e.g., increased screening of visitors during an elevated alert).

Maintain open lines of communication within HCCs or regional organizations and with local utility companies.

Many healthcare facilities belong to an HCC or regional organization as a means of broadening their network and knowledge base. During an incident, regional and coalition coordination may be needed, and it is best to establish robust information-sharing relationships prior to times of crisis. Regional organizations are helpful for information sharing, either to confirm intelligence reports or gather additional context about an incident. They are also particularly useful for coordinating response activities with local first responders and surrounding healthcare facilities, establishing common training plans, helping to manage resources, and better understanding incident response plans of other key stakeholders.

Regular Information Sharing

Establish a periodic meeting of healthcare facility security managers within a given area to share security-related information. Invite local and regional stakeholders to participate and share information (e.g., fusion centers, PSA, and local law enforcement). By establishing these relationships when there is no explicit IED threat, healthcare facility security managers will know whom to contact for information when there is a specific, credible IED threat to their community.

Similar to establishing information-sharing relationships with HCCs and regional organizations, it is useful to establish relationships with local utility companies prior to an incident (e.g., local electric, water and waste water, telephone, medical gas suppliers, and emergency generator service contractors). They will help coordinate response activities that may be necessary to the healthcare facility's ongoing operations during an incident.

Develop a communications plan.

Develop a communications plan for both internal and external stakeholders. Having a communications plan

will ensure that the right messaging reaches the right people at the right time during periods of uncertainty. Plans should provide clear and concise instructions to healthcare facility visitors, patients, and staff, as well as pass along important details to law enforcement, fire, EMS, and media members. If the threat level is elevated, provide additional information about the potential threat during daily staff and volunteer meetings. Additionally, visitors tend to be more accepting of security measures when they know that there is an elevated threat. Therefore, during circumstances when the threat is elevated, consider providing updated information and guidance to visitors more often and more visibly, using posters, public service announcements, and television monitors.

Internal

Coordination across staff and security personnel is important in times of uncertainty following an IED incident. Having a previously established communication plan will ensure that key information is relayed in a clear and concise manner. These communications should be targeted, role-based, and action-oriented as much as possible. Consider how best to relay information about IED incidents—such as mass text messages to staff, PA system announcements using a code or plain language system, or notification apps—and include this information with educational and training materials for awareness.

Information to healthcare facility staff. Provide staff (doctors, nurses, administration, etc.) information about a potential IED threat, especially given that some information about the IED threat may be posted on social media. Consider also providing guidance to increase security in and around the healthcare facility and to maintain awareness for suspicious activity and/or behavior nearby.

Information to patients and visitors. Internal communications should also consider messaging to facility patients and visitors. There is a need to balance providing sufficient information for the safety of the patients and visitors, while not causing panic. Provide up-to-date information about a potential IED threat, especially if some information about the IED threat may be posted on social media. Coordinate with the healthcare facility communications department to prepare messages for patients and visitors.

Pre-Written Messaging

Develop standard messages for visitors in advance, which can be displayed around the facility and on video monitors during elevated threat environments. Also consider preparing specific messages for release on the facility's intercom system and, if applicable, ready to send via text to staff members' phones.

For more information on sharing IED-related information, see Appendix 4.

External

Having an established external communications plan to include other regional healthcare facilities, EMS dispatch, utilities, social media content, and media interaction allows pre-determined messaging to be released in a controlled and clear manner. Consider creating stock language to make crafting and distributing these communications in an emergency much easier, save time for those involved, and ensure the right messaging is getting to the right people.

Management should coordinate with public relations staff to develop a media relations strategy that addresses an IED incident within or around the facility. This strategy should encompass communications with the media and surrounding businesses or residential communities in the area. Consider using news broadcasts, social media, and other communication mediums to share important information, such as stand-off areas or evacuation plans, to law enforcement, emergency responders, and facility visitors.

Goal 2 – Identify and report IED-related suspicious activity.

The following C-IED tasks are intended to help increase awareness and preparedness for identifying and communicating IED-related suspicious activity.

Educate all staff to understand potential IED threats.

Train all staff to recognize and report suspicious behavior and items that could be associated with IEDs. For example, training for reception desk staff could address not just recognizing unattended items, but also identifying suspicious behavior, such as unusual questions or attempting to gain access to restricted areas.

Job Aids

Consider using checklists, information cards, lanyards, pamphlets, and/or smart-phone applications as job aids to help staff and visitors remember C-IED tasks.

Training can consist of instructor-led sessions or computer-based training courses. In addition, educational materials (e.g., posters, signs, and checklists) can help staff recognize and report suspicious activities and items that could be associated with IEDs. Healthcare facility managers can run drills on a regular basis to reinforce training. If the threat level is elevated, consider issuing security reminders to staff or conducting ad-hoc refresher training, such as during staff huddles.

OBP has developed a wide variety of materials, such as training videos, posters, and checklists, that healthcare facilities can use to support their IED training efforts. See Appendix 4 for a list of available resources. Fundamental training concepts to understand how to identify potential IED threats include H.O.T. and R.A.I.N. explained below.

Educate staff to apply the **H.O.T.** principles to determine whether an item is suspicious and a potential IED; not all unattended items are suspicious. Indicators can relate to: what the item looks like; where it is; when it was found/placed; who placed or reported it; and why it came to the individual's attention (5Ws). Consider suspicious any items that are **H.O.T.**: **H**idden, **O**bviously suspicious, or not **T**ypical for the environment.

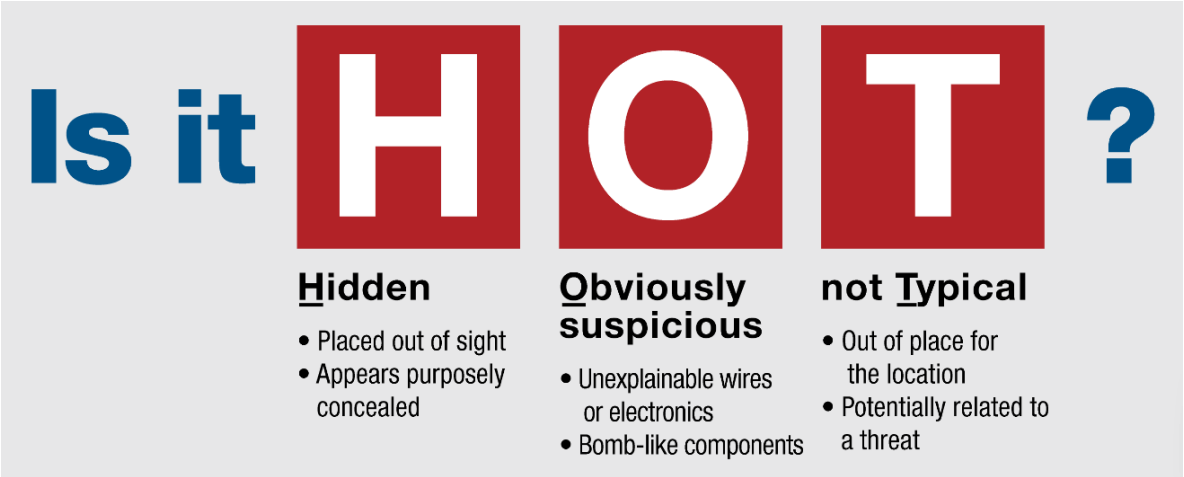


Figure 3: H.O.T. Principles
Property of DHS

Educate staff to follow the **R.A.I.N.** approach to take immediate safety actions upon identifying a suspicious item or potential IED. Once an individual identifies an item as suspicious, react as if it is an IED until determined otherwise by a public safety bomb squad (PSBS). Remember:

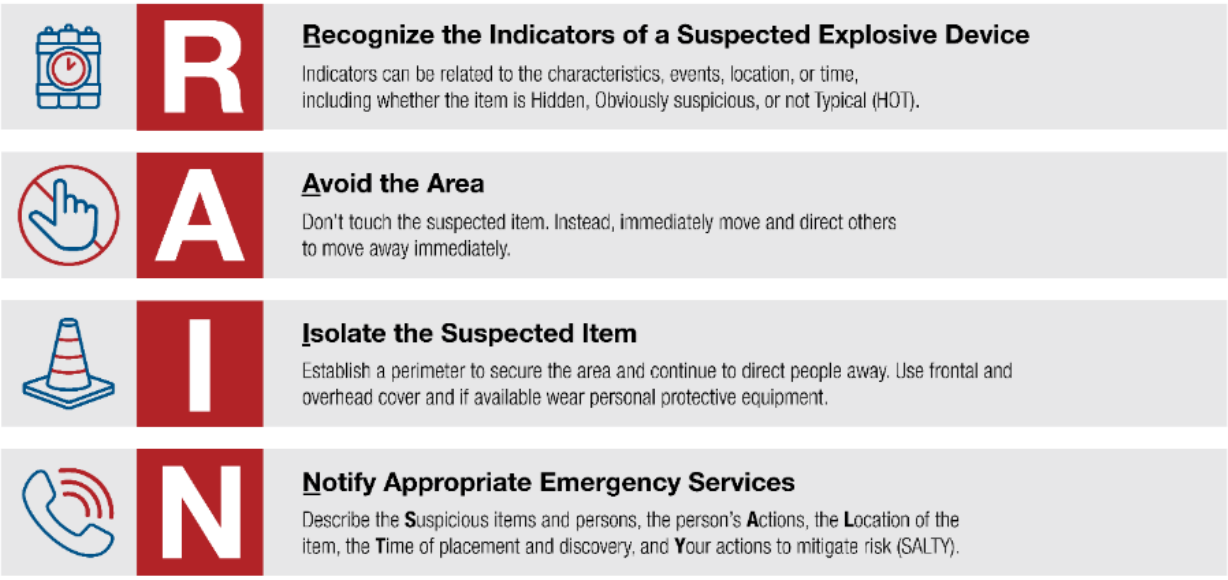


Figure 4: R.A.I.N. Approach
Property of DHS

Recognize out-of-place and suspicious behavior.

Be mindful of out-of-place and suspicious behaviors that may indicate planning or execution of an IED attack. Some examples of suspicious behaviors include the following:

- Wearing unusually bulky clothing that might conceal explosives;
- Attempting to access restricted areas; and
- Conducting surveillance of healthcare facilities.

Use Staff Awareness

Individuals who work in specific departments may have the best visibility into what is "normal" in that area. Use the expertise of staff across the facility to identify out-of-place or suspicious behavior.

Patients may also exhibit suspicious behavior through their injuries. Staff should be aware of the indicators of bomb-making injuries, such as skin discoloration or redness around the eyes from working with harsh chemicals, damage to ears from overpressure, or blunt trauma from an explosion. These indicators are not necessarily evidence of nefarious conduct and should be considered in the context of the circumstances in which they are observed or reported.

Healthcare facility staff are in the best position to observe suspicious behavior during daily activities. Security staff can provide additional support by actively monitoring closed-circuit television (CCTV) surveillance systems and conducting roving security patrols to recognize and respond to out-of-place behavior.

If the threat is elevated, use daily staff meetings to reinforce the importance of recognizing out-of-place and suspicious behaviors. See Appendix 4 for more information on recognizing suspicious behavior.

Recognize IED components and explosive precursors.

Be aware of common IED components (e.g., wires, timers, and triggers) and be able to recognize them in more vulnerable areas (e.g., emergency department lobby, waiting rooms, and nurse stations). In addition, staff should be familiar with explosive precursors, many of which are common household items, and report when they are in unexpected places or are unexpectedly missing from storage areas. Some products commonly found in healthcare facilities that can be used as precursor chemicals or as explosives include:

- Glycerin based lubrications;
- Gas tanks (Acetylene, Oxygen, Nitrogen);
- Fuels (Propane, Natural Gas);
- Cleaning products (Sanitizers, Oxidizers);
- Hydrogen peroxide antiseptic products; and
- Isotopes.

If the threat level is elevated, use daily staff meetings to reinforce the importance of recognizing IED device components and explosive precursors. For more information on IED components and precursors, see Appendix 4.

Report any bomb threats or potential IED-related information to appropriate authorities.

Establish procedures for staff to report information to facility security personnel and management on suspicious behaviors that could be associated with IEDs, such as an individual performing targeted surveillance of a healthcare facility, suspicious vehicles, or unattended bags with no identified owner. If the threat is elevated, reinforce these reporting procedures during daily staff meetings.

Contact local law enforcement with IED-related information ranging from suspicious activity that may be of interest to a credible IED threat. Law enforcement agencies may request that facilities provide evidence (e.g., CCTV footage) supporting the IED-related information and may request to speak directly to staff or individuals who reported the threat, so those individuals should remain available to assist law enforcement. For more information on reporting suspicious behavior to law enforcement, see Appendix 4.

Goal 4 – Implement site-specific protective measures to prevent and minimize the impact of IED incidents.

The following C-IED tasks include the activities that management can use to deter IED threats and protect against an IED attack at their facilities.

Implement facility-related security measures.

Identify and implement protective security features, such as perimeter lighting and fences, based on identified vulnerabilities. In addition, consider installing vehicle bollards or other physical barriers that provide effective standoff distance from potential IED attacks, which can include visually welcoming options such as security

Clear Trash Bins

Install clear trash receptacles so staff can better monitor items that go into bins, particularly in areas with open access.

planters. Similarly, consider implementing measures to mitigate the consequences of an IED detonation (e.g., installing blast-resistant windows and trash receptacles in the most vulnerable areas of the facility).

As part of these protective security features, consider installing physical distress buttons throughout the facility for staff, patients, or visitors to notify security of an issue. This could include hidden call buttons under reception desks or standalone emergency phones across larger campuses.

Conduct continuous roving security patrols.

During the steady-state threat environment, healthcare facility security typically conducts roving security patrols throughout the interior of buildings and around the campus (e.g., parking lots and walking paths between buildings), depending on the size of the facility. Security personnel should be on the lookout for suspicious behavior and items, as well as be familiar enough with the facility to recognize anything unusual or out of place. Regular patrols should also include an inspection of security barriers, such as locks, gates, and doors, for signs of intrusion, especially for high-risk areas that require extra security controls (e.g., power or utility stations, trauma centers, ambulance bays).

If the threat is elevated, consider expanding the scope of security patrols to include more thorough coverage of the facility or an increased frequency, depending on available resources. For example, if standard patrols do not include outdoor areas, expand the patrols to cover parking lots, particularly those closest to entrances. Additionally, healthcare facilities may partner with local law enforcement to conduct K9 patrols during times of an elevated threat. Increased patrols can serve both to identify suspicious activity and as a deterrent to nefarious actors.

Verify identity of full-time and temporary staff.

Healthcare facilities typically conduct criminal and financial background checks on potential staff as part of the hiring process (unless local or state laws or union regulations prevent them from doing so). Imposing similar requirements on contractors and volunteers can be more challenging. Consider requiring contractors, as a part of their agreement with the facility, to maintain a consistent standard of background checks for everyone who will be performing work for the facility. In the case of volunteers, emerging technologies that run rapid background checks could help identify potential security concerns. Consider setting a regular interval to revisit these background checks on staff and volunteers to help make sure credentials stay up to date.

Background Checks

Periodically validate the background checks that contractors perform on their staff to verify compliance.

Full-time staff are typically required to wear identification badges, which should be revised regularly. In most cases, these identification badges also serve as access cards for secure areas. It can be a challenge to maintain up-to-date identification badges for contractors, volunteers, visitors, or patients who may be in the facility temporarily or for short periods of time. Technologies to make single-use identification badges cheaply and quickly can address this security gap.

For all identification badges, consider implementing strategies to protect against the use of old identification badges to gain access to secure areas. If the threat is elevated, consider conducting an audit of identification badges and credentials to verify information is current and accurate.

Color Badges

Change the color of temporary visitor and contractor identification badges frequently to make it difficult to create fake badges or use old credentials to gain access into the facility.

Control access to secure areas.

Healthcare facilities tend to have many access points, which may limit management's ability to control the flow of people coming in and out of the building or broader campus. In particular, it may be difficult to control an unauthorized person's access to restricted entrances that need to remain open and available for immediate use (e.g., ambulance bay, loading dock). However, if the threat is elevated, consider placing additional security staff at sensitive entrance points, such as ambulance bays, to validate credentials and minimize unauthorized access. At night, consider placing security staff or other mechanisms to control or monitor access (e.g., card entry or CCTV), at the main entrances that remain open, such as the Emergency Department.

During the steady-state environment, healthcare facilities typically require authorized personnel to "swipe" their identification badge to gain access to restricted areas (e.g., specific medical departments, administrative offices, and security offices). Visual indicators on identification badges can also be used to help identify out-of-place individuals by indicating in what department personnel belong. If the threat is elevated, consider increasing the limitations on "swipe" access to further restrict personnel's access. Similarly, the facility may place additional security staff at the access points to restricted areas to validate credentials and minimize unauthorized access.

For individuals who need temporary access to an otherwise secure area (e.g., emergency department rooms), healthcare facility staff should escort or grant them access past a restricted access point. Additionally, in selecting a system to validate a visitor's identity for a temporary identification badge, consider systems that have the capability to integrate with alerts from local law enforcement (Be on the Lookout alerts (BOLO), amber alerts, etc.) that would alert healthcare facility staff to a suspicious individual and deny access, as needed. Similarly, consider if there are any outside credentials (e.g., local law enforcement, neighboring healthcare facility) that could be considered reciprocal and automatically recognized by such a system.

Incorporate blast-resistant features and materials into new and existing sites.

When a new healthcare facility is built or an older one is renovated, there is an opportunity to incorporate thoughtful security by design. In situations where sufficient standoff distance or layered defense is not achievable, structural hardening and use of blast-resistant features and materials is particularly important. Appendix 4 provides resources for selecting and incorporating blast-resistant features. Additionally, consider measures that will make staff and other individuals more aware of security, without limiting anyone's access to the healthcare facility (e.g., gated entrances into a parking lot and limited open access points). Similarly, with a new or renovated facility opening, take the opportunity to (re)educate staff on best practices and security design features.

Goal 5 – Utilize IED screening and detection methods in high-risk environments.

The following C-IED tasks include various screening and detection methods that facility personnel can use to identify and prevent IEDs and IED components from entering facilities.

Screen incoming persons and objects.

Screen patients, volunteers, and visitors and inspect bags upon entry.

During the steady-state threat environment, screening of patients, volunteers, and visitors as well as their bags is typically limited to visual efforts to recognize suspicious items and behavior. However, if the threat is elevated, consider implementing approaches to increase the security presence and enhance screening and inspection practices, such as adding additional security staff to monitor healthcare facility entrances, using hand-held metal detectors, or instituting random screening and bag checks. The additional screening of visitors is used to verify their purpose at the healthcare facility and verify patients' identification for access within the facility.

Screening and inspection practices also need to balance security with providing rapid access to healthcare services, especially for emergency room services. For more information on bag screening, see Appendix 4.

Screen vehicles.

During the steady-state threat environment, screening of vehicles is typically limited to visual efforts to recognize suspicious items and behavior, especially in city areas where efforts to screen vehicles would likely block traffic. This visual monitoring can also be supplemented by registering vehicles associated with visitors and using stickers on staff cars to help track traffic on the facility and identify unattended vehicles. However, if the threat is elevated, the need to screen vehicles may outweigh collateral inconveniences. Consider adding extra security staff for enhanced vehicle screening to monitor the loading and unloading areas immediately outside the entrance. For more information, see Appendix 4.

Figure 5: Inspecting a Delivery Truck
Source: OBP

Screen incoming mail and deliveries.

Healthcare facilities typically monitor mail and other deliveries during the steady-state threat environment to properly handle sensitive medical supplies and healthcare paperwork. This monitoring consists of general screening to recognize anything suspicious that could be associated with IEDs (e.g., strange odors, ticking sounds, and protruding wires). However, if the threat is elevated, reinforce the importance of screening all mail and deliveries and reporting anything suspicious during daily staff meetings. Special attention should also be paid to packages resulting from online orders or personal shopping, which may increase the volume of mail the healthcare facility receives and appear to deviate from what would be considered a "typical" package for the facility. For more information on screening deliveries, see Appendix 4.

Goal 6 – Take immediate safety precautions for bomb threats, suspicious items, and IEDs.

The following C-IED tasks include the activities by which healthcare personnel can take immediate safety precautions for bomb threats, suspicious items, and IEDs.

Search for potential IEDs.

Standard practice upon receiving a bomb threat is to initiate a strategic search of the entire facility to locate the potential bomb, to include the interior (e.g., restrooms and garbage cans) and exterior (e.g., along exterior perimeter walls and parking lots). The search should also prioritize evidence preservation to assist with a possible law enforcement investigation. Assign responsibilities to support an IED search to staff who are familiar with specific areas, as they will be most able to spot anything out of place.

Go Bags

Prepare go bags for search teams/law enforcement with blue prints, assignments, all access badges, etc.

If available, CCTV footage can aid in the search to determine, for example, if a suspicious package is merely an unattended bag or if it was left behind deliberately. Emerging technology, such as geo-specific social media monitoring tools that allow users to monitor information being posted to social media sites from a specified location, can provide additional information to security managers and staff to support the search for potential IEDs.

If a potential IED is located through the search process, notify law enforcement, monitor the device, and do not touch it until law enforcement arrives on scene and provides further instructions. Importantly, limit the use of communication devices when searching for an IED, as the use of two-way radios and cell phones could trigger detonation of an IED.

Implement emergency operations plan and/or business continuity plan.

Implement the facility's emergency operations plan and/or business continuity plan to guide the response to a credible IED threat or successful detonation. Incorporating Hospital Incident Command System (HICS) protocols into the facility's plan is highly encouraged.

Off-Site Command Center

Employ an off-site command center, as the necessary face-to-face coordination between facility management and law enforcement may not be feasible in the building should an IED detonation occur.

At a minimum, the plan should outline procedures for the following:

- Reporting credible IED threats to local law enforcement;
- Searching for potential IEDs and what to do if one is located, also considering a pre-evacuation protocol that includes conducting a secondary sweep for additional suspicious items along the evacuation routes and reception areas;
- Coordinating with first responders to ensure unity of effort and maintaining ongoing communications;
- Activating the healthcare facility command center;
- Implementing the communications plan for providing information to first responders, staff, patients, visitors, and the media (consider using a joint information center [JIC]); and
- Evacuating the facility partially or completely based on an identified IED.

When responding to an IED threat, management should notify and provide information to local law enforcement and fire rescue agencies.

Information to law enforcement and fire rescue agencies. The types of information that healthcare facility managers should expect to provide arriving law enforcement and fire rescue responders include, but are not limited to:

Figure 6: Security team monitors CCTV
Source: Shutterstock

- Information collected on a bomb threat checklist, such as who received the bomb threat, the phone number of the caller, and what the caller said;
- Any suspicious activity or deliveries at the time the threat was made;
- Whether a search for the suspected IED has been conducted, and if so, the results of that search;
- Size of any suspected IEDs located, as this will determine the area that will need to be cordoned off;
- Healthcare facility floor plan, CCTV, and other surveillance information that could be informative; and
- Potential hazardous materials or chemicals present that could affect responders or reduce the effectiveness of a K9 unit.

In addition, law enforcement officers often will want to speak directly with the person who received initial information about an IED threat, the Security Director, and Operations Officer.

Goal 7 – Safely coordinate response activities at IED incident sites.

The following C-IED tasks include the activities by which healthcare personnel can effectively coordinate and facilitate the rapid response to an IED incident.

Coordinate with first responders and provide support for response operations following an IED detonation.

Immediately following an IED detonation, management should activate the emergency operations plan, which includes extensive coordination. The following table outlines key command roles and responsibilities suggested by HICS. While these specific roles might not exist during the steady-state, they would be activated and carried out by staff as needed during an incident.[5]

[5] California Emergency Medical Services Authority. *Hospital Incident Command System Guidebook*. 2014.

Role	Responsibilities
Incident Commander	• Confirm the accuracy and validity of the incident. • Approve and activate partial or complete healthcare facility lockdown or evacuation to ensure safety of patients, staff, and visitors. • Establish a liaison role with law enforcement or public safety response agencies who arrive to assist healthcare facility response. • Notify healthcare facility CEO, Board of Directors, and other appropriate stakeholders of incident status. • Establish operational periods, objectives, and regular briefing schedule
Public Information Officer	• Maintain communication with patients, staff, and visitors regarding the current situation and what is being done to address it. • Develop information release for media; work with law enforcement or public safety officials on details to be released; ensure families of impacted patients and staff are aware prior to release of information. • Monitor media outlets for updates on the incident and possible impacts on the healthcare facility. Communicate information via regular briefings to Section Chiefs and Incident Commander.
Liaison Officer	• Notify community partners in accordance with local policies and procedures (e.g., consider local Emergency Operations Center, other area healthcare facilities, local emergency medical services, and health care coalition coordinator), to determine incident details, community status, estimates of casualties, and establish contacts for requesting supplies, equipment, or personnel not available in the facility. • Liaise with law enforcement as applicable.
Safety Officer	• Oversee the safe movement of patients, staff, and visitors from hazardous areas. • Provide incident specific information and intelligence if the incident involves hazardous materials or if the incident may impact combustible or explosive agents on site. • Oversee the selection of relocation sites, healthcare facility Command Center, external command posts, media center, and staging areas to ensure safe distance from the incident site.
Medical Branch Director	• Activate and oversee the evacuation of patient care areas when ordered by Incident Commander. • Identify evacuation priorities and transfer requirements. • Identify procedures and appointments that will be impacted if partial or complete healthcare facility evacuation is ordered. • Coordinate with the Liaison Officer and Public Information Officer to ensure notification of all impacted patients and visitors.

In addition to coordinating roles within the targeted healthcare facility, it may be necessary to coordinate support across nearby facilities. First responders may request support from unaffected buildings or medical facilities located within the vicinity of an IED detonation. First responders may want to utilize these other facilities for the following:

- Command post to direct response operations requiring conference rooms, office supplies, communications, and information technology support;
- Alternate Care Sites (ACS): facilities that enable healthcare providers to provide medical care for

Alternative Care Sites

- Establish agreements with other facilities in advance to expedite the process of rerouting patients
- Set up triage function closer to the incident site when in austere conditions (e.g., tent in the parking lot)
- Temporarily stop or relocate all elective procedures

injured or sick patients or continue care for chronic conditions;

- Family Assistance Centers (FAC): secure area used for family reunification and emergency sheltering, notifying families about loved ones, share situational updates, and provide emotional support.

Coordinate with other healthcare facilities to determine if they are willing and able to support response efforts and communicate that information to first responders.

Family Assistance Centers

- Prepare for large crowds of visitors by assigning a dedicated space and establishing a process for sharing communication
- Consider training staff on group communication, culture and faith considerations when speaking with families
- Refer to the National Incident Management System (NIMS)/HICS structure for additional guidance

Consider types of lockdowns/lockouts.

In the event of an IED incident, restricting access either into or out of a healthcare facility might be necessary to maintain control and ultimately keep patients and staff safe. Based on the severity of the situation, it will be up to healthcare facility security and administration to determine the type and extent of the lockdown/lockout.

Controlled lockdowns/lockouts are typically employed in one of three types:

- Entry Only: all perimeter doors are secured and guarded by security personnel; anyone attempting to enter should be screened
- Exit Only: all perimeter doors are secured and guarded by security personnel; anyone attempting to leave should be screened
- Entry/Exit: all perimeter doors are secured and guarded by security personnel; anyone attempting to enter or leave should be screened

Controlled lockdowns/lockouts can be applied to varying extents:

- Partial Lockdown/Lockout: all individuals should be directed to pre-designated controlled entrances or exits, with security maintaining control at these locations; anyone attempting to enter, or leave should be screened
- Departmental Lockdown/Lockout: used to control entry or exit to a specific area of the healthcare facility; security personnel should guard all doors and elevators to and from this area
- Total Lockdown/Lockout: all perimeter doors are secured, and no one is allowed to enter or exit the facility

Factors to consider when activating a lockdown/lockout:

- Additional personnel will likely be needed to maintain control of all open doors during normal business hours;
- Tensions may arise from individuals who cannot enter the facility to see their loved ones;
- Utilize alternate care sites if ambulances and walk-in patients need to be diverted;
- Modified lockdown/lockout procedures should be considered to enable the safe entry of medical care staff; and

- Internal and external signage indicating restricted entry should be posted as soon as possible.

Evacuate the healthcare facility.

If an IED threat is determined to be credible, evacuation of staff, patients, and visitors may be necessary; however, given the challenges associated with moving critical patients, evacuation should be viewed as a last resort. Depending on the location of the IED threat, first determine whether the entire facility needs to be evacuated, or if a partial evacuation is sufficient (e.g., the potential blast radius of the suspicious item would not impact all departments in the healthcare facility).

- Consider developing an evacuation plan unique for IEDs, with several evacuation routes, including ones that are different from fire evacuation routes, to minimize exposure to a suspected IED or planted secondary devices. Ideally, inspect the chosen evacuation route before notifying people of the need to evacuate. First responders arriving to the healthcare facility can also support the evacuation if additional personnel are needed.

Evacuation

- Whether it's a partial, complete, horizontal, or vertical evacuation, the decision to move forward should happen soon after an incident occurs
- Conduct a sweep of the evacuation destination area to make sure it's safe before moving people
- If safe to do so, screen individuals on their way to the evacuation area to avoid bringing the assailant into the facility
- Establish a secondary method for identifying patient needs in case a paper-based system isn't feasible (e.g., use of permanent markers)

- If the decision is made to evacuate, identify exit points as far from the blast as possible, and direct the evacuation accordingly.
- Understand the advantages and disadvantages of partial, complete, horizontal, or vertical evacuation (e.g., horizontal evacuation utilizes doors as smoke/fire barriers and might benefit patients who cannot physically use stairs).
- Identify which floors/zones should move first
    - Areas in greatest danger should be first to move, followed by adjacent areas
    - If there is no immediate threat, evacuate facility top to bottom

Conclusion

Ensuring the safety of patients, visitors, and staff is a priority for all healthcare facility owners and operators. While each healthcare facility has unique preparedness needs based on its own vulnerability assessments, past incident data shows that bomb threats are likely to occur in healthcare settings on a frequent basis. Healthcare facilities should take preventive action to ensure their own preparedness for a potential IED incident as part of their overall security management efforts. By connecting with local authorities, developing plans to identify issues and support incident response, training staff, and reporting concerns to law enforcement, many incidents may be mitigated or avoided. The preventive measures outlined in this SRG C-IED Annex can help healthcare facility owners and operators create a safer environment for their patients, visitors, and staff while maintaining a commitment to delivering quality healthcare.

Figure 7: Healthcare facilities have a diverse set of stakeholders
Source: Shutterstock

Appendix 1: Healthcare Facility C-IED Tasks

The following image presents tasks for countering IED threats in and around healthcare facilities.

SECURITY OFFICE

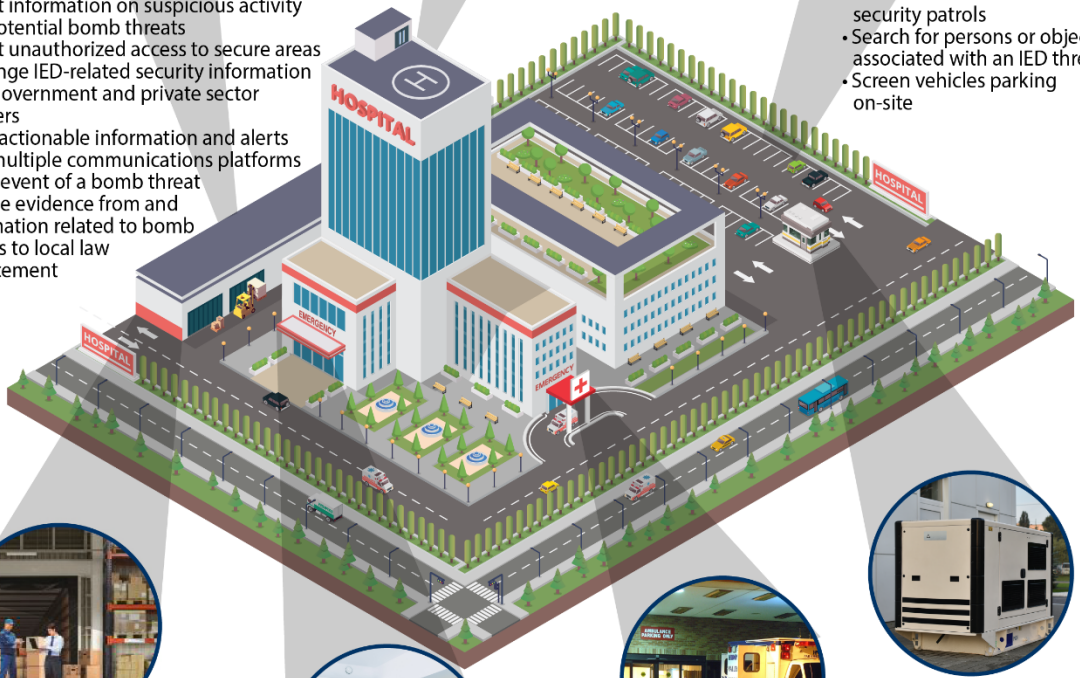
- Assess potential risks to facility
- Conduct or verify background checks on personnel prior to employment
- Issue credentials (e.g., badges) for access
- Control access to secure areas
- Assess potential risks posed by nearby facilities
- Educate stakeholders on how to recognize and report suspicious indicators
- Recognize IED components, precursors, and devices
- Report information on suspicious activity and potential bomb threats
- Report unauthorized access to secure areas
- Exchange IED-related security information with government and private sector partners
- Share actionable information and alerts over multiple communications platforms in the event of a bomb threat
- Provide evidence from and information related to bomb threats to local law enforcement

CLINICAL AREAS

- Implement appropriate protective measures
- Verify staff, patient, and visitor credentials (e.g., badges) for access
- Recognize out-of-place and suspicious or concerning behavior
- Recognize out-of-place and suspicious objects
- Search for persons or objects associated with an IED threat
- Plan for and conduct evacuations specific to a credible bomb threat or incident
- Report unauthorized access to secure areas

PARKING AREA

- Recognize IED components, precursors, and devices
- Recognize out-of-place and suspicious or concerning behavior
- Recognize out-of-place and suspicious objects
- Conduct continuous roving security patrols
- Search for persons or objects associated with an IED threat
- Screen vehicles parking on-site



LOADING DOCK

- Implement facility-related security measures such as lighting and cameras
- Verify delivery persons' credentials, as applicable
- Recognize IED components, precursors, and devices
- Recognize and report information on suspicious activity and potential bomb threats
- Report unauthorized access to secure areas

EMERGENCY DEPARTMENT ENTRANCE

- Screen visitors and inspect bags
- Verify staff, patient, and visitor credentials (e.g., badges) for access
- Recognize IED components, precursors, and devices
- Recognize out-of-place and suspicious or concerning behavior
- Recognize out-of-place and suspicious objects

AMBULANCE BAY

- Implement security measures, such as lighting and cameras
- Recognize out-of-place and suspicious or concerning behavior
- Recognize out-of-place and suspicious objects
- Report unauthorized access to secure areas

POWER/UTILITY STATION

- Implement security measures, such as lighting and cameras
- Recognize out-of-place and suspicious or concerning behavior
- Recognize out-of-place and suspicious objects
- Report unauthorized access to secure areas

Appendix 2: Aligning Role-Based Responsibilities

The following table shows the relationship between the C-IED goals and example tasks that are described in greater detail above and identifies the stakeholder(s) responsible for addressing them.

C-IED Capability-Based Goals and Tasks	Stakeholders			
	Security / Administration[6]	Reception Desk Staff	Facilities Staff	Clinical Staff
Goal 1: Use and share risk information to guide IED-related physical security, law enforcement, and emergency response activities				
Establish relationships with local law enforcement, fire, emergency medical services (EMS), and fusion centers	X			
Maintain open lines of communication within HCCs or regional organizations and with local utility companies	X			
Develop a communications plan	X			
Goal 2: Identify and report IED-related suspicious activity				
Educate all staff to understand potential IED threats	X	X	X	X
Recognize out-of-place and suspicious behavior	X	X	X	X
Recognize IED components and explosive precursors	X	X	X	X
Report any bomb threats or potential IED-related information to appropriate authorities	X	X	X	X
Goal 4: Implement site-specific protective measures to prevent and minimize the impact of IED incidents				
Implement facility-related security measures	X		X	
Conduct continuous roving security patrols	X			
Verify identity of full-time and temporary staff	X			
Control access to secure areas	X			
Incorporate blast-resistant features and materials into new and existing sites	X		X	

[6] For facilities without full-time security managers, the facility manager would likely accomplish these activities.

C-IED Capability-Based Goals and Tasks	Stakeholders			
	Security / Administration[6]	Reception Desk Staff	Facilities Staff	Clinical Staff
Goal 5: Utilize IED screening and detection methods in high-risk environments				
Screen patients, volunteers, and visitors and inspect bags upon entry	X	X		
Screen vehicles	X		X	
Screen incoming mail and deliveries	X	X	X	
Goal 6: Take immediate safety precautions for bomb threats, suspicious items, and IEDs				
Search for potential IEDs	X	X	X	X
Implement emergency operations plan and/or business continuity plan	X			
Goal 7: Safely coordinate response activities at IED incident sites				
Coordinate with first responders and provide support for response operations following an IED detonation	X	X	X	X
Consider types of lockdowns/lockouts	X			
Evacuate the healthcare facility	X	X	X	X

Appendix 3: Goals and Tasks Checklist

This appendix contains a version of the C-IED goals and tasks in a checklist format. Healthcare facility security staff can use this checklist to evaluate their C-IED preparedness and identify areas for improvement. Consider the following instructions prior to beginning an evaluation of C-IED preparedness:

- **Select tasks.** First identify which C-IED tasks are most relevant to the facility based on an assessment of the risk from IEDs.
- **Select participants.** Engage a subgroup of staff representing a broad cross-section of functions (e.g., reception desk staff, facilities staff, and medical staff) to examine C-IED processes and identify deficiencies.
- **Solicit responses.** Some tasks can be examined by one functional group; others require collaboration across functional groups. For those that require collaboration, gather input from all of the stakeholders that have a role in executing the task to determine a consensus for the facility as a whole.
- **Scope of the answers.** Considerable variation exists between different types of healthcare facilities. For example, healthcare facilities in urban or suburban areas may face differing IED vulnerabilities and protective measure options. Therefore, users of the checklist should think about how they want to be able to achieve each task and then assess whether they are able to perform that task successfully.
- **Use the results.** The information gathered can illustrate and enhance successful efforts, identify additional opportunities to strengthen C-IED preparedness and avoid redundant efforts. Additionally, a clear understanding of gaps enables managers to identify, prioritize, and justify key actions to take and equipment to purchase.

C-IED Goals and Tasks	Response (Yes—Partial—No—N/A)
Goal 1: Use and share risk information to guide IED-related physical security, law enforcement, and emergency response activities	
Assess potential risks, including threats, vulnerabilities, and consequences from an IED Incident.	
Assess potential IED risks posed by facilities adjacent to the healthcare facility (e.g., shopping center).	
Support local, state, tribal, territorial, regional, and national efforts to analyze and assess IED risk and resilience.	
Maintain the routine exchange of IED-related security information—including alerts, attack indications and warnings, and advisories—among government and industry stakeholders and nearby businesses.	
Monitor and act upon industry and government IED-related threat information.	

C-IED Goals and Tasks	Response (Yes—Partial—No—N/A)
Goal 2: Identify and report IED-related suspicious activity	
Educate staff to recognize and report suspicious behavior, activities, and objects that could be associated with IEDs.	
Recognize out-of-place and suspicious behaviors (e.g., persons loitering in the healthcare facility lobby wearing unusually bulky clothing that might conceal suicide explosives or individuals attempting to access restricted areas or conducting surveillance) that may indicate planning or execution of an IED attack.	
Recognize out-of-place and suspicious objects (e.g., unattended packages or items) that could be IEDs.	
Recognize IED components, precursors, and suspect devices in common areas, patient rooms, and junctions where critical lifelines (e.g., electricity, water) enter and exit the facility.	
Maintain control over explosive chemicals and precursors of concern found in healthcare facilities (e.g., cleaning supplies and gas tanks).	
Report information on suspicious activity and potential IED threats to appropriate authorities.	
Provide information that could be associated with IEDs (e.g., individuals conducting surveillance) to local law enforcement.	
Provide evidence to appropriate authorities to support the collection of intelligence information with respect to potential IED threats.	
Goal 4: Implement site-specific protective measures to prevent and minimize the impact of IED incidents	
Develop and implement protective security features, such as perimeter lighting and fences, and barriers that provide effective standoff distance from potential IED attacks.	
Deploy assets (e.g., surveillance cameras and security personnel) to interior and exterior areas to interdict, deter, or disrupt IED threats from reaching potential target(s).	
Verify the identity of patients and visitors for access to healthcare facilities during medical treatment or visitation.	
Screen personnel prior to full-time employment and/or use as temporary staff.	
Issue identification badges to verify identity of full-time and temporary staff.	

C-IED Goals and Tasks	Response (Yes—Partial—No—N/A)
Grant and control access to restricted areas, such as mechanical rooms, staff lounges, and security offices.	
Develop and implement mitigation measures and blast-resistant design, especially in high- risk areas, to limit the effects of an IED detonation.	
Goal 5: Utilize IED screening and detection methods in high-risk environments	
Screen patients and visitors to ensure they have reason to be at the healthcare facility.	
Screen vehicles upon arrival and in parking facilities to identify suspicious objects or devices that could be associated with IEDs.	
Screen bags coming into the facility to identify suspicious objects or materials that could be associated with IEDs.	
Screen all mail deliveries, including envelopes and packages intended for the healthcare facility or for patients, to identify anything suspicious that could be associated with IEDs (e.g., strange odors, ticking sounds, or protruding wires).	
Goal 6: Take immediate safety precautions for bomb threats, suspicious items, and IEDs	
Conduct intrusive and non-intrusive (e.g., use of CCTV) search and detection operations, as appropriate, to identify, discover, or locate persons or objects associated with an IED threat.	
Implement an established emergency operations plan and/or business continuity plan to support healthcare C-IED functions/operations in response to an IED threat or successful detonation.	
Goal 7: Safely coordinate response activities at IED incident sites	
Coordinate with local first responders during an IED threat or following an explosion to ensure unity of effort (e.g., healthcare security staff should coordinate with law enforcement personnel responding to a report of an IED threat).	
Share actionable alerts and messages with staff and patients, as appropriate, in the event of an IED threat.	
Communicate information and warning (e.g., protective measures for evacuation or shelter in place) to staff, patients, and visitors during an IED event.	
Consider types of lockdowns to secure the healthcare facility and protect the well-being of patients, visitors, and staff based on the type of IED incident.	

C-IED Goals and Tasks	Response (Yes—Partial—No—N/A)
Evacuate staff, patients, and visitors to a designated location in the event of a known or suspected IED threat.	
Provide support for mass care services (e.g., family reunification, emergency sheltering) that are taking place inside the healthcare facility following an IED explosion.	
Provide support for medical services (e.g., triage points, field care, or medical command posts) that are taking place inside the healthcare facility following an IED explosion.	
Provide additional resources, as requested by unified command and elected officials, following an IED explosion to support response and recovery efforts (e.g., food/shelter for victims, families, and/or responders).	

Appendix 4: Healthcare and Public Health Sector C-IED Resources

The resources appendix provides a number of pre-existing guidance documents and products (e.g., posters, pamphlets, and guides) for healthcare facility personnel who are interested in learning more about the C-IED tasks. Whenever possible, there is a link to the resource; to request those without a link (indicated with an asterisk), please contact OBP at OBP@cisa.dhs.gov.

Resource	Resource Description
Identifying explosive precursor chemicals	Awareness poster that highlights products commonly found in healthcare facilities that contain chemicals which can be used to make explosives
Identifying hazardous chemical materials	Awareness poster that highlights the IED implications for hazardous chemical products that could be found within a healthcare facility and used in a bomb.
Identifying peroxide materials	Awareness poster that highlights the IED implications for peroxide products that could be found within a healthcare facility and used in a bomb.
Counter-IED Training Courses	OBP develops and delivers a diverse curriculum of training to build nationwide counter-IED core capabilities. In-Person, Virtual Instructor-Led Training (VILT), and Independent Study Training (IST) courses provide public and private sector individuals with multiple platforms by which to complete counter-IED training. Examples of course topics include: IED Construction and Classification; Homemade Explosives (HME) and Precursor Awareness; Bomb Threat Management Planning; Protective Measures; and Surveillance Detection Course for Law Enforcement and Security Professionals.
Identifying and responding to a VBIDED	Instructional guide that provides guidance on VBIED preparedness, recognition, and response
Screening and searching vehicles *	Vehicle Inspection Guide that identifies safety procedures and best practices when screening vehicles entering your healthcare facility.
TRIP*wire* program tutorial	Tutorial video detailing DHS's TRIP*wire* program and the variety of C-IED resources available and how to sign up.
Public Venue Bag Search Procedures Guide	Instructional guide that provides suggestions for developing and implementing bag search procedures at public assembly venues, which can include healthcare facilities.

* To request this resource, please contact OBP at OBP@cisa.dhs.gov.

Resource	Resource Description
Identifying a suicide bomber *	Awareness poster that highlights the potential behaviors and indicators of a suicide bomber.
Conducting visitor screening	Informational guide that identifies best practices for screening visitors.
Bomb threat guidance	Informational guide to assist personnel in identifying critical steps and procedures to prevent and protect against a potential IED incident.
Steps to take when receiving a bomb threat	4-minute informational video describing what steps to take in the event of receiving a bomb threat.
Recording information during a phoned in bomb threat	Informational guide on what information to record in the event of receiving a bomb threat by phone.
Minimum evacuation distance for an IED incident	Informational poster that details the recommended minimum evacuation distance for IED incidents of different magnitudes.
Nationwide Suspicious Activity Reporting (SAR) Initiative	The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort to provide law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.
Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE)	The Technical Resources, Assistance Center, and Information Exchange (TRACIE) was created to meet the information and technical assistance needs of healthcare practitioners and facilities across the country through preparedness materials, technical assistance, and peer-to-peer information sharing.
"Whole building" design techniques and technologies for facilities	The National Institute of Building Sciences (NIBS) Whole Building Design Guide provides information on a wide range of building-related guidance, criteria, and technology from a "whole buildings" perspective, including guidance on explosive threats.
Identifying bomb-making indicators and explosive injuries	Awareness poster that highlights bomb-making indicators and injuries for safety and reporting purposes *Note: must be a registered TRIP*wire *user and logged in to access this poster*

* To request this resource, please contact OBP at OBP@cisa.dhs.gov.

Appendix 5: C-IED Planning Process

The following table illustrates key steps in the C-IED planning process, as outlined in Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans. The steps are flexible and enable planners to adapt the process to their own unique characteristics and situations. The SRG C-IED adapted the planning process to incorporate IED-specific actions and planning considerations. Planners may wish to consult CPG 101 for more detailed information on each step of the planning process.

Appendix 6: Healthcare and Public Health Sector C-IED References

The following is a list of references that informed the healthcare facility C-IED tasks:

- California Emergency Medical Services Authority. *Hospital Incident Command System Guidebook*. 2014. https://emsa.ca.gov/wp-content/uploads/sites/71/2017/09/HICS_Guidebook_2014_11.pdf.
- DHS. *Federal Interagency Operational Plans*. August 2016. https://www.fema.gov/federal-interagency-operational- plans.
- DHS. *Healthcare and Public Health Sector-Specific Plan*. 2016. https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf.
- DHS. *National Infrastructure Protection Plan*. 2013. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.
- DHS. *National Preparedness Goal 2nd Edition*. September 2015. https://www.fema.gov/national-preparedness-goal.
- DHS. *National Prevention Framework*. May 2013. https://www.fema.gov/media-library/assets/documents/117762.
- DHS. *National Mitigation Framework*. May 2013. https://www.fema.gov/national-mitigation-framework.
- DHS. *National Response Framework*. May 2013. https://www.fema.gov/media-library/assets/documents/117791.
- DHS. *National Protection Framework*. July 2014. https://www.fema.gov/media-library/assets/documents/117782.
- DHS OBP and FBI. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance*. 2018. https://www.cisa.gov/publication/security-and-resiliency-guide-and-annexes.
- The Joint Commission. Emergency Management Resources. 2019. https://www.jointcommission.org/emergency_management.aspx
- Joint Program Office. Countering Improvised Explosive Devices Report to the President. November 6, 2012.
- Joint Program Office. Countering Improvised Explosive Devices Implementation Plan. May 10, 2019.
- World Health Organization. *Attacks on Healthcare Dashboard*. 2016, 2017, 2018. https://www.who.int/emergencies/attacks-on-health-care/archive/en/