

## Hospitality Industry: Enhanced Suspicious Activity Awareness Assists in Terrorism Prevention

From family-owned lodging to chain properties and luxury resorts, the hospitality industry represents a diverse and complex environment, including an open and welcoming operating model, transient populations, multiuse facilities, conference spaces, bars, restaurants, casinos, gyms, pools, business centers, and ballrooms. With approximately 53,000 lodging properties and over 15 million people employed by the hospitality industry in the United States, a well-trained, security-conscious staff can act as a force multiplier for recognition and reporting of suspicious activity potentially indicative of terrorism in or adjacent to their respective facilities. Hospitality-security stakeholders are encouraged to develop a security culture to protect their staff, the public, and the property from terrorism.

**NOTE:** Some of the activities described in this document include constitutionally protected or innocuous activity. Evaluate the totality of behavioral indicators and other relevant circumstances when considering any law enforcement response or action. These activities should not be reported absent articulable facts and circumstances that support an assessment that the observed behavior is not innocent, but rather reasonably indicative of violent or criminal activity, including those associated with terrorism.

**STAFF TRAINING:** The best and most cost-effective security technique is a well-trained staff that can recognize and react appropriately to a potential or actual threat. Training should highlight the importance of security and include what to look for and what to do in the event of an incident or attack. Staff should be highly encouraged, to report situations that may be suspicious, hazardous or potentially dangerous. Hospitality facilities make security inherently challenging because of their size,

**SCOPE:** This product promotes awareness in the hospitality industry to enhance security and safety against terrorist activities. Hospitality industry security starts with complete comprehensive background screening during the hiring process, and includes suspicious activity awareness training, evaluation of policies and processes, and incorporates the latest technology.

The **TERRORIST ATTACK MODEL** consists of three primary phases, identified as decision, planning, and execution. In each phase, there are several activities, some of which may or may not be observable and may occur more than once or not at all. Awareness of the observable aspects of the model can help recognize indicators for mitigation. In addition, an attack of opportunity may present very few or no planning indicators, due to a spontaneous decision by the attacker against an already familiar target or one of chance.



12 NOVEMBER 2019  
 AUTHORED BY NCTC, DHS, FBI

**NOTICE:** This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, the FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies or procedures. For additional information, contact us at JCAT@NCTC.GOV.

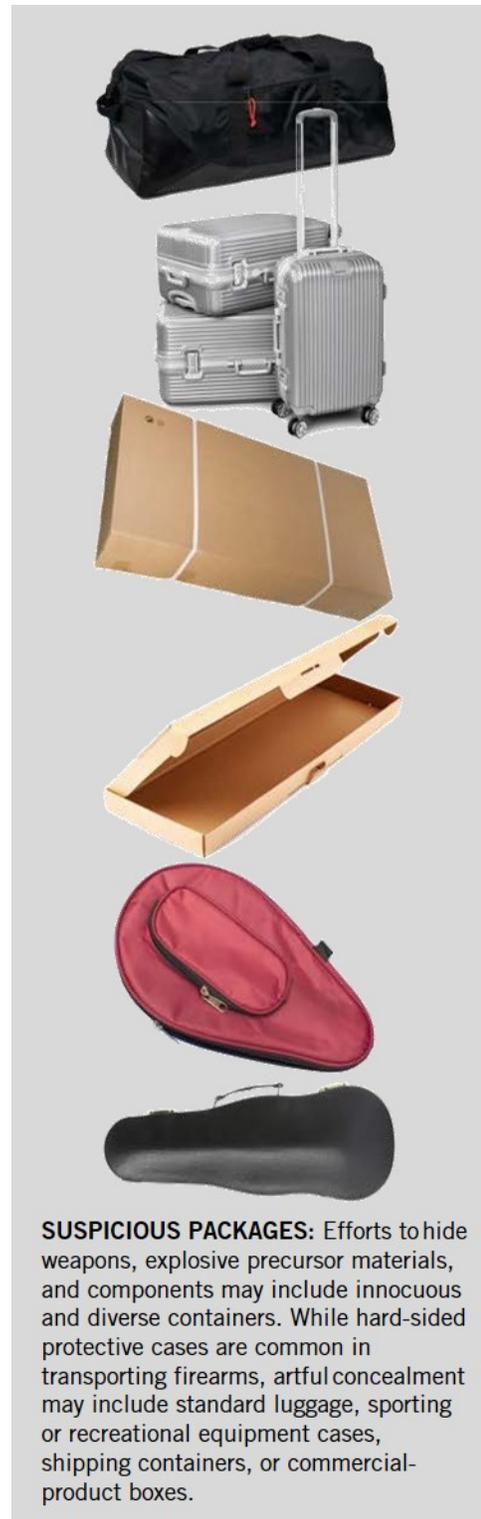
## FIRST RESPONDER'S TOOLBOX

layout, and amenities, and alert staff will be prepared to detect suspicious activity. Personnel may not retain information from a single training or briefing, so consider regularly delivering refresher and updated training to reinforce key messages and instruction. Hospitality industry staff should also understand the terrorist attack model, which will further enhance their ability to identify suspicious activity.

- Be observant. Report attempts to access restricted areas or to avoid security measures.
- Be attentive. Report unusual interest or inquiries about the facility, including hotel staff operating procedures, shift changes, closed-circuit TV (CCTV) systems, events, other guests, and neighboring sites, including government, military, police, communications, or infrastructure.
- Be watchful. Report unattended luggage, packages, or vehicles in or adjacent to facilities.

**REGISTRATION DESK:** Maintain security-minded service through responsive interactions with customers, while following established security protocols, especially those requiring identification, room cards, or tickets. Consider:

- Refusal to provide required professional or personal details on hotel registrations, such as place of employment, contact information, or place of residence.
- Requests to keep a guest's presence on the premises confidential.
- Recurring short-duration departure extensions over a prolonged period.
- Use of cash for large purchases or credit card in a name different from the registered guest.
- Making frequent or extensive modifications to the hotel registration, including removing or adding guests.
- Unusual interest in hotel security or hotel access points, including main, alternate, and emergency entrances and exits.
- Requests for specific rooms, floors, or other locations in the hotel—particularly those not



12 NOVEMBER 2019  
AUTHORED BY NCTC, DHS, FBI

considered premium choices—and when coinciding with special events located on or near the premises.

- Seemingly purposeful attempts to use entrances and exits that avoid the lobby, cameras, and hotel staff, or attempts to mask identity in vicinity of cameras.

**CONCIERGE:** Interaction with guests and visitors may reveal specific or unusual questions regarding security procedures, other access and egress points, facility infrastructure, or requests to circumvent a hotel policy. Watch for:

- Signs of unusual content in luggage, cases, bags, and boxes, including weight, size, or other noteworthy characteristics.
- Amount or type of luggage inconsistent with number of guests or length of stay.
- Strong desire to handle particular items of luggage or strongly refusing assistance with numerous or heavy luggage.
- Luggage that seems devoid of content.
- Seemingly unusual weight, size, or frequency of deliveries to an individual or room.
- Attempts at purposefully keeping packages out of camera or plain view.

**VALET AND TRANSPORTATION SERVICES** should be alert for attempts to access restricted parking areas, seemingly abandoned or illegally parked vehicles, and vehicles that appear unusually weighted down or modified. Look for:

- Presence of large items concealed by blankets or tarps, or emitting an unusual chemical odor.
- A liquid substance, not normally associated with a vehicle, observed leaking from the passenger compartment or the trunk.
- Deception techniques including cloned, rented, or stolen vehicles used to impersonate.
- Use of stolen or fraudulent documentation including passes, license plates, bills of lading, permits, or licenses.
- A driver who seems unfamiliar with the contents of the vehicle, the purpose of the visit, or the vehicle itself.

**MAINTENANCE, HOUSEKEEPING, AND ROOM SERVICE STAFF** during daily routines may observe behaviors, activities, or items that create suspicion, specifically weapons or explosive precursor materials, and their storage and use. Tipoffs include:

- Denial of cleaning or maintenance services.
- Altered, disabled, or removed fire alarms and smoke detectors.
- Weapons or ammunition.
- Unusual odors, such as cleaning solvents, fuel, chemical products, or evidence that these chemicals were in the room, including containers (which may have had the labels removed), wrappers, labels, as well as stains in the sink, shower, or tub.
- Laboratory equipment.
- Burn marks or discoloration on the walls, floors, or doors.
- Extended stays with little baggage or unpacked luggage.
- Not leaving room for extended period.
- Hastily departing a room without checking out, leaving behind luggage or seemingly



- significant belongings.
- Evidence of wiring or soldering, and presence of electronic components, electrical tape, batteries, soldering guns, and wires.
- Presence of materials that could be used as shrapnel, including nuts, ball bearings, screws or nails.
- Extensive notes, photos, technical drawings, or maps of the surrounding area of no tourist value.
- Publications associated with terrorism.
- Efforts by guest to change their appearance.
- Attempted access to areas that are restricted or otherwise designated for staff only.

**HOMEMADE EXPLOSIVES (HME) AND IED CONSIDERATIONS:** Most explosive precursor chemicals, components, and equipment used for HMEs have commercial uses and are legal to obtain, making the detection of explosives manufacture challenging. Familiarity with components, explosive precursors, equipment, and tools associated with HME manufacture is important to be able to recognize related activities. Staff are encouraged to conduct a follow-up with all guest complaints involving odd noises or strong odors, as well as unexplained stains and discoloration on floors, walls, or ceilings, as environmental indicators may uncover suspicious activity.

**NOTE:** Efforts to manufacture HME or construct IEDs are inherently dangerous as the explosive precursors used may be extremely sensitive to impact, friction, static electricity, and flames. Treat potential HMEs or IEDs accordingly until rendered safe by certified subject matter experts. Emergency plans should include instructions for rapid evacuation, isolation of the materials or devices, and notification to appropriate authorities to ensure the safety of staff and guests.

*Images from terrorist publications.*



**SURROUNDING AREAS:** Security may include all amenities in the hotel, including ballrooms, convention halls, physical fitness centers, business offices, restaurants, multiuse facilities, pools, casinos, parking garages, loading docks, and entertainment venues, but may also extend beyond the perimeter of the hotel and include neighboring venues and facilities. Special events create another set of challenges, which include potentially exposed locations during an emergency-incident response. Recommended actions include:

- Hotel security should periodically perform risk, threat, and vulnerability assessments, to develop tailored security approaches, and routinely reevaluate security measures and emergency-response plans against evolving terrorist trends and tactics whether overseas



or in the Homeland, including:

- Changes in surrounding landscape, neighboring buildings, adjacent streets, and alternative approaches (footpaths or off-road access points).
- Each new disrupted plot or successful attack offers an opportunity to ensure plans are up to date.
- Reassessment allows first responders to adjust standard response procedures, such as bypassing security barriers; identifying secure locations for the incident command post, casualty collection points, and asset staging; establishing traffic patterns for responding personnel and victim transport; and modifying communications protocols to conduct rapid and efficient emergency operations.
- Steady state-of-information sharing across all stakeholders plays a critical role in attack identification, mitigation, and response, as well as in effective communication, utility-services redundancy, and incident recovery.

**USE OF TECHNOLOGY:** While staff and guest vigilance is key to the identification and prevention of terrorist activity, technology also plays a crucial role in ensuring a safe and secure environment. CCTV— long established as a basic safety measure offering general surveillance—with more sophisticated advancements, can detect abandoned baggage, identify preregistered guests, employees, authorized deliveries, and can detect activity in restricted areas. Technology alone will not manage all security concerns because a determined adversary may be able to circumvent the most sophisticated of systems.

### RESOURCES:

- **DHS OFFICE FOR BOMBING PREVENTION (OPB)** offers training to build counter-IED capabilities and enhance awareness of IED threats is available in traditional classroom settings, online independent study, and virtual instructor led training platforms. [https://www.dhs.gov/bombing\\_prevention\\_training](https://www.dhs.gov/bombing_prevention_training)
- **BOMB MAKING MATERIALS AWARENESS PROGRAM (BMAP)** is a national outreach initiative to promote private sector point of sale awareness and suspicious activity reporting to prevent misuse of common household items as explosive precursor chemicals and IED components. <https://www.dhs.gov//bmap>
- **TECHNICAL RESOURCE FOR INCIDENT PREVENTION (TRIPwire)** is a secure, online, collaborative information-sharing and resource portal for the Nation's federal, State, local, and tribal government security and emergency services professionals. <https://tripwire.dhs.gov>
- **FBI ACTIVE SHOOTER RESOURCES** provides a list of resources for the public and first responders on a wide variety of active shooter topics. <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources>
- **DHS TERRORISM PREVENTION AND ACTIVE SHOOTER** web portal promotes information and intelligence sharing on a broad range of terrorism prevention and active shooter topics and promote information sharing and collaboration between federal, state, local, tribal, territorial, private, civilian, and international entities. <https://www.dhs.gov/cveas-portal>



- **DHS ACTIVE SHOOTER PREPAREDNESS** provides products, tools, and resources to help prepare and respond to an active shooter incident.  
<https://www.dhs.gov/active-shooter-preparedness>
- **RECOVERING FROM AN ACTIVE SHOOTER INCIDENT FACT SHEET:**  
<https://www.dhs.gov/publication/recovering-active-shooter-incident-fact-sheet>





## PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE:    LE    FIRE    EMS    HEALTH    ANALYSIS    PRIVATE SECTOR    DATE:

PRODUCT TITLE:



ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

