Assessment

(U) Threat Assessment: Hotels

IA-0469-10

Office of Intelligence and Analysis
ASSESSMENT

(U) Threat Assessment: Hotels

13 September 2010

(U) Prepared by the DHS/I&A Cyber, Infrastructure, and Science Division, Strategic Infrastructure Threat Branch; the DHS/I&A Homeland Counterterrorism Division, Tactics, Techniques, and Targets Branch; and the DHS/Office of Infrastructure Protection. Coordinated with the DHS/Office for Bombing Prevention, the National Counterterrorism Center, and the FBI. The Interagency Threat Assessment and Coordination Group has reviewed this product from the perspective of our nonfederal partners.

(U) Scope

(U//FOUO) This assessment is intended to support the activities of DHS and to assist federal, state, and local government counterterrorism and law enforcement officials, and the private sector in deterring, preventing, preempting, or responding to terrorist attacks against soft targets such as hotels in the United States. It is intended to support the national "See Something, Say Something" campaign.

(U) Key Findings

(U//FOUO) There is no evidence of specific threats to hotels in the United States, but terrorists have targeted overseas hotels serving Westerners and have regularly threatened attacks on U.S. soil.

- **(U//FOUO) The tactics used in overseas hotel attacks and plots during the past two years involved various combinations of disguise, improvised explosive devices (IEDs), vehicle-borne improvised explosive devices (VBIEDs), and small-unit assaults.**

- **(U//FOUO) While this assessment focuses on recent terrorist attacks against hotels, terrorists could potentially use similar tactics for attacks against other soft targets.**

(U//FOUO) DHS encourages security and law enforcement personnel at U.S. hotels to remain alert for potential indicators of terrorist activity and to implement a variety of protective measures.

(U) The United States Is An Enduring Target

(U//FOUO) The United States faces enduring but evolving threats from terrorists intent on attacking the Homeland. Public statements by al-Qa'ida leaders and spokesmen regularly threaten attacks on U.S. soil. Al-Qa'ida in the Arabian Peninsula regional commander and prominent ideologue Anwar al-Aulaqi[USPER] and al-Qa'ida media official Adam Gadahn[USPER] have called for Westerners to conduct simple, small-scale attacks against familiar targets in local areas that do not require extensive support and training. This message has been reinforced by *Inspire* magazine, an English language online magazine reportedly published by al-Qa'ida in the Arabian Peninsula. Preparations and planning for such attacks are often difficult to detect.

(U) Hotels Targeted Overseas

(U//FOUO) In targeting hotels serving Westerners, terrorists are probably motivated by several factors, some of which also apply to other lightly secured or publicly accessible targets in the United States:

- (U//FOUO) They likely view large, iconic hotels as symbols of Western culture.

- (U//FOUO) Attacks against hotels generally offer prospects for causing mass casualties, visually dramatic destruction, economic aftershocks, and fear—all of which are primary terrorist goals.

— (U//FOUO) The relatively open and public nature of hotels makes them potentially an easier target to access than other facilities with perimeter security and checkpoints, such as government or military facilities.

(U) Recent Overseas Attacks and Tactics

(U//FOUO) The DHS/Office of Intelligence and Analysis (DHS/I&A) has no evidence of specific threats to hotels in the United States, but analysis of successful and thwarted attacks abroad has identified a variety of potentially relevant terrorist tactics. Such tactics include the use of disguise, improvised explosives, and small-arms assaults. The array of attacks launched against overseas hotels illustrates terrorist capabilities that hotel security officials should consider when developing protective measures and employee security training programs.

(U//FOUO) **Use of Disguise:** Terrorists have posed as police and security personnel to confuse hotel security. Attackers have also posed as hotel guests and reportedly worked with insiders to facilitate attacks.

— (U//FOUO) On 24 August 2010, at least two members of the Somalia-based terrorist organization al-Shabaab—a gunman and a suicide bomber—stormed the Muna Hotel in Mogadishu disguised as police officers, killing at least 33 people, including four members of the Somali Parliament.

— (U//FOUO) On 17 July 2009, at least two suicide attackers posing as guests used IEDs to attack luxury hotels in Jakarta, Indonesia. They reportedly checked into a room two days before the attack and possibly received inside assistance from a hotel vendor.

— (U//FOUO) On 14 January 2008, Taliban militants, some disguised in police uniforms, attacked a hotel in Kabul, Afghanistan using small arms, grenades, and IEDs. One of the terrorists detonated a suicide vest at the entrance to the hotel, while others attacked guards outside the compound and guests inside the hotel.

(U//FOUO) **IEDs:** Explosives serve as a force multiplier for terrorists, affording greater damage to infrastructure and lethality. Their use can also be timed to target first responders upon arrival on scene.

— (U//FOUO) From 26 to 29 November 2008, 10 heavily armed gunmen, operating in teams of 2, simultaneously attacked several targets throughout the city of Mumbai, India, including two large hotels. IEDs prevented first responders from gaining access to the hotel and were detonated in taxis elsewhere in the city to sow chaos. The attackers seized hostages, took up defensive positions inside the hotel's upper floors, and engaged first responders with small arms and IEDs.

(U//FOUO) **VBIEDs:** As a subset of IEDs, VBIEDs have been used to attempt to breach hotel entry gates. In a 2008 Islamabad attack, a single VBIED with one driver was unable to breach the entry gate before the explosive detonated. Subsequent attacks incorporated second vehicles and multiple armed attackers to help the VBIED penetrate security.

— (U//FOUO) On 25 January 2010, terrorists used a combination of small arms and VBIEDs in coordinated attacks against three hotels in Baghdad.

— (U//FOUO) On 9 June 2009, a small group of attackers used a combination of small arms and two vehicles, one a VBIED, to attack a luxury hotel in Peshawar, Pakistan. The hotel's security cameras showed a sedan entering the hotel's entry control point and guards opening the gate. Gunmen in the vehicle then fired at the guards, allowing both the sedan and a VBIED to enter the compound, where they detonated the device.

— (U//FOUO) On 20 September 2008, a terrorist, after failing to breach the perimeter of a luxury hotel in Islamabad, Pakistan, detonated a VBIED at the vehicle access control point.

(U//FOUO) **Paramilitary and "Small-Unit" Assault Tactics:** Assaults with small arms have been used in conjunction with other tactics to attack hotels. The group of 10 Mumbai attackers used assault rifles, pistols, and grenades to defeat perimeter security, defend themselves, maximize casualties, and prolong the siege.

(U) Terrorist attacks against overseas hotels since 2008.

	Kabul 14 January 2008	Islamabad 20 September 2008	Mumbai 26-29 November 2008	Peshawar 9 June 2009	Jakarta 17 July 2009	Baghdad 25 January 2010	Mogadishu 24 August 2010
Tactic	Small Arms, IEDs	VBIED	Small Arms, IEDs	Small Arms, VBIED	IEDs	Small Arms, VBIEDs	Small Arms, IED
Disguise	Police Uniforms	None	None	None	Posed as Guests, Received Insider Assistance	None	Security Uniforms
Procedure	Three Caused a Distraction, Fourth Entered Hotel to Detonate Vest	Truck Rammed Gate, Smaller Explosion Dispersed Guards	Avoided Security, Entered Hotel Through Rear	Fired At Gate Guards, Allowed Vehicle to Enter	Smuggled Explosives Through Basement Cargo Dock, Rehearsed Attack	Fired At Gate Guards, Allowed Vehicle to Enter	Forced Entry into Hotel
Number of Assailants	More than 5	1	10	More than 5	3 captured, 5 more suspected	More than 5	4
Location of Detonation	Suicide Vest Inside, VBIED Outside	At Entry Control Point	In Hotel	On Compound	In Hotel	50 Feet from Hotel	In Hotel

(U) Indicators of Possible Suspicious Activity

(U//FOUO) Operatives associated with many of the hotel attacks overseas behaved in ways that are indicative of suspicious activity. Security and law enforcement personnel at U.S. hotels should be alert to potential indicators of terrorist activity, to include avoiding questions typically asked of hotel registrants, showing unusual interest in hotel security, attempting access to restricted areas, and evading hotel staff.

(U//FOUO) Although many of these behaviors may be innocuous by themselves, the observation of multiple indicators may represent—based on the specific facts or circumstances—possible suspicious activity at hotels:

- (U//FOUO) Not providing professional or personal details on hotel registrations—such as place of employment, contact information, or place of residence.
- (U//FOUO) Extending departure dates one day at a time for prolonged periods.
- (U//FOUO) Refusal of housekeeping services for extended periods.
- (U//FOUO) Extended stays with little baggage or unpacked luggage.
- (U//FOUO) Access or attempted access to areas of the hotel normally restricted to staff.
- (U//FOUO) Multiple visitors or deliveries to one individual or room.
- (U//FOUO) Unusual interest in hotel access, including main and alternate entrances, emergency exits, and surrounding routes.
- (U//FOUO) Use of entrances and exits that avoid the lobby or areas with cameras and hotel personnel.
- (U//FOUO) Attempts to access restricted parking areas with a vehicle or leaving unattended vehicles near the hotel building.
- (U//FOUO) Unusual interest in hotel staff operating procedures, shift changes, closed-circuit TV systems, fire alarms, and security systems.
- (U//FOUO) Leaving the property for several days and then returning.
- (U//FOUO) Abandoning a room and leaving behind clothing, toiletries, or other items.
- (U//FOUO) Noncompliance with other hotel policies.
- (U//FOUO) Interest in using Internet cafes, despite hotel Internet availability.
- (U//FOUO) Non-VIPs who request that their presence at a hotel not be divulged.
- (U//FOUO) Use of cash for large transactions or a credit card in someone else's name.
- (U//FOUO) Requests for specific rooms, floors, or other locations in the hotel.
- (U//FOUO) Use of a third party to register.

(U) Protective Measures

(U//FOUO) Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for hotels include:

(U) Planning and Preparedness

— (U//FOUO) Designate and train an employee to serve as security director to address all security-related activities.
— (U//FOUO) Conduct threat analyses, risk assessments, security consequence analyses, and security audits on a regular and continuing basis.
— (U//FOUO) Develop a comprehensive security and emergency response plan.
— (U//FOUO) Establish liaison and regular communication with local law enforcement and emergency responders.
— (U//FOUO) Conduct regular exercises with hotel employees to test security and emergency response plans.
— (U//FOUO) Conduct/participate in regular exercises with local law enforcement and emergency responders to test joint coordination on security and emergency response plans.

(U) Personnel

— (U//FOUO) Conduct background checks on all employees.
— (U//FOUO) Incorporate security awareness and appropriate response procedures for security situations into employee training programs.
— (U//FOUO) Maintain an adequately sized, equipped, and trained security force.
— (U//FOUO) Check guest identification upon check-in. Provide guests with information on how to report suspicious people or activities.

(U) Access Control

— (U//FOUO) Define the hotel perimeter and areas within the hotel that require access control for pedestrians and vehicles.
— (U//FOUO) Issue photo identification badges to all employees. Require that badges be displayed.
— (U//FOUO) Issue special identification badges to contractors, cleaning crews, vendors, and temporary employees.
— (U//FOUO) Restrict the storage of luggage to locations away from areas where large numbers of people congregate.

(U) Barriers

— (U//FOUO) Install appropriate perimeter barriers and gates.
— (U//FOUO) Implement appropriate level of barrier security.
— (U//FOUO) Install building perimeter barriers (e.g., fences, bollards, large boulders, large decorative flower pots, high curbs, shallow ditches).
— (U//FOUO) Install barriers to protect doors and windows from small-arms fire and explosive blast effects (e.g., blast-resistant and shatter-resistant glass, offset entryways).
— (U//FOUO) Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from buildings and areas where large numbers of people congregate.

(U) Communication and Notification

— (U//FOUO) Install systems that provide communication with all people at the hotel, including employees, security forces, emergency response teams, and guests.
— (U//FOUO) Install systems that provide communication channels with law enforcement and emergency responders.

(U) Monitoring, Surveillance, and Inspection

— (U//FOUO) Install video surveillance equipment (e.g., closed circuit television, lighting, night-vision equipment) and implement appropriate monitoring schedules.
— (U//FOUO) Consider acquiring luggage-screening equipment for use during high-threat or high-profile events.
— (U//FOUO) Implement quality control inspections on food supply to hotel restaurants and special events.

(U) Cyber Security

— (U//FOUO) Develop and implement a security plan for computer and information systems hardware and software.
— (U//FOUO) Regularly review the hotel's Web site to ensure no sensitive information is provided.

(U) Incident Response

— (U//FOUO) Ensure that an adequate number of emergency response personnel are on duty or on call at all times.
— (U//FOUO) Identify alternate rallying points where employees and others at the facility can gather for coordinated evacuation and for "head counts" to ensure all have evacuated.

(U) Implications

(U//FOUO) DHS/I&A has no specific information indicating terrorist plans to attack hotels in the United States. Nevertheless, the success of previous hotel attacks overseas and the significant media coverage those attacks garnered could encourage terrorist groups to use similar tactics against targets in the United States. As terrorists continue to refine their operational tradecraft, facility security personnel should remain vigilant, re-evaluate and enhance security as appropriate, and report any suspicious activity to law enforcement.

(U) Reporting Notice:

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the nearest state and local fusion center and to the local FBI Joint Terrorism Task Force. State and local fusion center contact information can be found online at http://www.dhs.gov/files/resources/editorial_0306.shtm. The FBI regional telephone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) DHS/I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

(U) Tracked by: HSEC-02-00000-ST-2009, HSEC-02-07000-ST-2009, HSEC-02-08000-ST-2009, HSEC-03-00000-ST-2009

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

I&A Customer Survey

Product Title: (U) Threat Assessment: Hotels

1. Please select the partner type that best describes your organization. Select One

2. How did you use this product in support of your mission?

- ☐ Integrated into one of my own organization's finished information or intelligence products
- ☐ Shared contents with federal or DHS component partners
  - If so, which partners?
- ☐ Shared contents with state and local partners
  - If so, which partners?
- ☐ Shared contents with private sector partners
  - If so, which partners?
- ☐ Other (please specify)

3. Please rank this product's relevance to your mission. ***(Please portion mark comments.)***

- ◯ Critical
- ◯ Very important
- ◯ Somewhat important
- ◯ Not important
- ◯ N/A

4. How could this product or service be improved to increase its value to your mission? ***(Please portion mark comments.)***

5. Was this product provided to you in response to a specific request to DHS I&A? ◯ Yes ◯ No

6. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Timeliness of product or support	◯	◯	◯	◯	◯
Responsiveness to your intelligence needs	◯	◯	◯	◯	◯
If you answered yes to question 5, please rate your satisfaction with DHS I&A's communication during the processing of your request	◯	◯	◯	◯	◯

To help us understand more about your organization so we can better tailor future products, please provide:

Your Name and Position

Your Organization

Your Contact Number or Email

Submit Feedback

Notice to DHS I&A Customers

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Paperwork Reduction Act Compliance Statement

Legal Significance of Office of Management and Budget Control Number: Your response to this feedback request is completely voluntary. The Paperwork Reduction Act requires that the Department of Homeland Security notify respondents that no person is required to respond to the collection of information unless it displays a currently valid OMB control number.

Privacy Act Statement: DHS's Use of Your Information

Principal Purposes: When you provide feedback on an Intelligence and Analysis (I&A) intelligence product, DHS collects your name, position, contact information, and the organization you are representing. We use this information to contact you if we have additional questions about the feedback and to identify trends, if any, in the feedback that you and your organization provide.

Routine Uses and Sharing: In general, DHS will not use this information for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. Aggregate feedback data may be shared within and outside DHS but without including the contact information. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or necessary for a specific purpose, as described in the DHS Mailing and Other Lists System of Records Notice, DHS/ALL-002 (73 FR 71659).

DHS Authority to Collect This Information: DHS requests that you voluntarily submit this information under its following authorities: 5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101.

Effects of Not Providing Information: You may opt not to provide the requested information or to provide only some of the information DHS requests. However, if you choose to provide any feedback information, you must provide a classification level as requested on this form. If you opt not to provide some or all of the requested information, DHS will not be able to contact you to fully address your feedback and any additional information needs.

Accessing and Correcting Information: If you need to access or correct the information collected on this form, you should send an email to *ia.feedback@dhs.gov*. You may also direct your request in writing to the appropriate FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts." Additional instructions are available at that website and in the DHS/ALL-002 System of Records Notice, referenced above.

Return to Form