Homeland Security

Office of Intelligence and Analysis/Office of Infrastructure Protection

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

(U) Distribution Notice: For any further questions regarding distribution please contact the Department of Homeland Security, Office of Intelligence and Analysis, Production Management Division, at IA.PM@hq.dhs.gov.

(U//FOUO) DHS/HITRAC was established in January 2005 to assess risks to domestic critical infrastructure and key resources through enhanced integration of intelligence reporting and analysis with information from respective infrastructure sectors. Analysis of suspicious activity reporting is part of DHS/HITRAC's mission to provide strategic, national-level analysis of information reported to the Department.

23 January 2007

Strategic Sector Assessment

(U//FOUO) Commercial Facilities Sector

(U) Attention: Federal Departments and Agencies, State Homeland Security Advisors, State Emergency Managers, State and Local Fusion Centers, Law Enforcement, Tribal Governments, Information Sharing and Analysis Centers, and the Sector Coordinating Councils.

(U) Scope

(U//FOUO) This Strategic Sector Assessment is one in a series that provides an overall assessment of the potential terrorist threats to critical infrastructure and key resources, and provides decision makers with the broad, analytically-based threat information necessary to inform investment priorities and program design. It also provides the overarching analytic foundation for incident reports and threat warnings produced by DHS and other federal partners. This assessment was prepared with input from federal infrastructure partners and the private sector.

(U//FOUO) This assessment describes DHS' knowledge and provides analysis of current terrorist threats to commercial facilities sector (CFS) assets within the United States. It also describes known terrorist goals and motives, their potential application to the CFS, vulnerabilities associated with sector facilities and assets, and the potential consequences of an attack.

(U) Key Findings

(U//FOUO) DHS continues to receive credible, specific, and corroborated reports indicating terrorist threats to the commercial facilities sector (CFS).

(U//FOUO) Al-Qa'ida continues to pose the greatest terrorist threat to the CFS. Al-Qa'ida desires to strike the United States again, and an attack against CFS assets could meet its targeting strategy of mass casualties, economic damage, and psychological impact.

(U//FOUO) Sunni extremists and homegrown radicals also pose a threat to this sector. Homegrown radicalization is an emerging, dynamic phenomenon that may spur individuals to attack CFS assets.

(U//FOUO) Terrorist casing reports uncovered in July 2004 on financial institutions in the New Jersey–New York area and in Washington, D.C. provide the greatest insight to date into al-Qa'ida's targeting strategy against high-profile financial institutions and the commercial facilities that house them, as well as the surveillance techniques and methods of operations.

(U//FOUO) The CFS is marked by its vast size and diversity of subsector assets. Several characteristics, such as open public access and proximity to the assets of other sectors that also are potential targets, challenge the development and implementation of protective measures for the sector.

(U) Threat Overview

(U//FOUO) International Terrorist Organizations' Interest in the Commercial Facilities Sector

(U//FOUO) Al-Qa'ida continues to pose the greatest terrorist threat to the CFS. DHS has specific and credible reporting from multiple sources indicating al-Qa'ida's historical interest in attacking specific elements of the CFS. DHS is not aware of any specific imminent threat to critical infrastructure in the sector, but an attack against a sector asset likely would meet al-Qa'ida's strategic targeting criteria, which are to inflict American casualties, cause psychological damage to the U.S. population by attacking symbols of U.S. culture or symbolic value, and damage the national economy.

(U//FOUO) Al-Qa'ida and affiliated terrorist groups have long been interested in striking populated buildings, as demonstrated by attacks on the Khobar Towers in Saudi Arabia, U.S. Embassies in East Africa, and the World Trade Center in New York City. Numerous al-Qa'ida operatives have expressed an intent to attack tall U.S. buildings using multiple attack methods such as vehicle-borne improvised explosive devices (VBIEDs) and explosions using natural gas.

— (U//FOUO) There are numerous examples of attacks overseas by al-Qa‘ida and al-Qa‘ida affiliates against commercial facilities such as resorts in Egypt, clubs and hotels in Indonesia, and shopping centers and hotels in Jordan.

(U//FOUO) DHS has no information to suggest that Islamic groups present in the United States such as HAMAS or Hizballah are currently targeting the sector. These groups, however, like al-Qa‘ida, may find commercial facilities attractive targets. The presence of established extremist networks could facilitate operational activity against critical infrastructure.

(U//FOUO) Homegrown Islamic Extremists a Growing Threat

(U//FOUO) Counterterrorist operations have forced al-Qa‘ida to decentralize since the 11 September 2001 attacks. The network continues to plot attacks against U.S. coalition and allied targets, but also encourages other Islamic extremists and homegrown radicals to conduct attacks of their own. Indigenous radical groups and lone wolf individuals driven by al-Qa‘ida ideology and anger toward the United States now pose a greater threat to U.S. infrastructure—including commercial facilities—than in the past. They can be U.S. citizens or legal permanent residents who operate freely in U.S. society. Their familiarity with U.S. cultural and social norms often makes it more difficult for law enforcement to detect planning or operational activity.

(U//FOUO) Homegrown radicals usually have less access to terrorist training and funding than established groups such as al-Qa‘ida. As a result, attack planning generally is simpler, requires less coordination and skill, and has a shorter time frame. Thus, these attack plots may be more difficult to predict and interdict.

(U//FOUO) Adam Gadahn a.k.a. Azzam al Amriki [USPER]

(U//FOUO) One of the most infamous cases of Islamic extremist radicalization is that of Adam Gadahn a.k.a. “Azzam the American.” After initially learning about Islam through the Internet, he converted in a ceremony at the Islamic Society of Orange County [USPER] ***in the mid-1990s. Saudi-funded extremist literature at the mosque likely contributed to his radicalization as did his association with extremists at the mosque, including Khalik al-Deek*** [USPER]***. Both he and al-Deek traveled to Pakistan in the late 1990s and subsequently took on larger roles in al-Qa‘ida. With his knowledge of Western audiences, the Internet, and technical aspects of media production, it is believed that Gadahn is behind several sophisticated and well-produced al-Qa‘ida propaganda videos since 11 September 2001.***

(U//FOUO) Other Domestic Extremists Also Pose a Threat

(U//FOUO) Attacks on CFS assets also are part of the goals of certain single-issue movements. In particular, the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF)—both of which are operationally active—have a history of targeting and attacking companies and facilities they deem are harmful to animals or the environment. The ALF has targeted companies that conduct product and medical testing using animals, and ELF advocates inflicting economic damage on those they believe to be profiting from destruction of the environment.

- (U//FOUO) These groups are difficult for law enforcement and intelligence organizations to monitor because of their diffuse and tenuous membership. Their actions often are taken by lone wolves or small groups acting independently and in response to information provided by ALF and ELF rather than in response to direct leadership instructions.

- (U//FOUO) These groups have had a measure of success in modifying the behavior of perceived offending businesses, and DHS expects them to continue their harassment tactics. They have targeted the homes, spouses, children, and business associates of personnel employed by commercial firms. In keeping with their ideology, these groups generally have targeted property rather than people, using nonviolent tactics such as Internet or telecommunications denial of service attacks, burglaries, and protests. During the past several years, however, the rhetoric of animal rights and environmental extremists has advocated increasingly violent actions, including arson and homicide.

(U//FOUO) Other domestic extremist groups such as white supremacist, neo-Nazi, and militia groups pose varying degrees of threat to security in the Homeland, but they have not shown interest specifically in the CFS. In the late 1990s an FBI Joint Terrorism Task Force arrested two antigovernment militia members in Sacramento, California for allegedly planning to blow up a storage facility that held approximately 24 million gallons of propane located about a mile from a residential subdivision.

(U) Sector Overview

(U//FOUO) The broad scope of the CFS provides terrorists with ample targets of opportunity. The Intelligence Community lacks current specific, detailed reporting of operational plans and terrorist interest in any of its eight subsectors. DHS analysis of historical reporting, previous worldwide attacks, and thwarted plots, however, provide some insight into the attractiveness of each subsector as a potential terrorist target.

(U//FOUO) **Entertainment and Media:** Historical reporting of al-Qa‘ida surveillance suggests that the network has considered using media vans to gain closer access to targets of opportunity. In addition, Islamic terrorists may consider entertainment and media assets as valid targets because of their role in disseminating Western culture.

(U//FOUO) **Lodging:** Attacks against lodging facilities overseas demonstrate terrorist interest in attacking these facilities. Moreover, these facilities often are located near other critical infrastructure/key resources (CI/KR) that also are potential targets, such as government facilities, transportation hubs, and sport venues.

(U//FOUO) **Outdoor Events, Sports Leagues, Public Assemblies, and Resorts:** DHS assesses al-Qa'ida operatives and Islamic extremists may view assets within these subsectors as desirable targets based upon guidance from the *Al-Qaeda Training Manual*. This manual specifically lists "…blasting and destroying the places of amusement, immorality, and sin…and attacking vital economic centers" as a required mission.

— (U//FOUO) In 2003 and 2004 al-Qa'ida directed an individual to case tourist targets in the United States.

(U//FOUO) **Real Estate:** Senior al-Qa'ida leaders have stated that large buildings in the United States are especially vulnerable to attack and easy to hit. In addition to the 11 September 2001 attack on the World Trade Center, al-Qa'ida also reportedly discussed a large Midwestern commercial building as an alternative or secondary attack target.

— (U//FOUO) In May 2002 U.S. officials disrupted a U.S. Person's plot involving the use of gas to blow up buildings in the Homeland.

— (U//FOUO) In February 2006 U.S. Government officials confirmed the disruption of a plot by al-Qa'ida members to fly hijacked planes into a West Coast commercial building as a follow-on to the 11 September 2001 attacks.

(U//FOUO) **Retail:** Overseas, terrorist groups have attacked a number of shopping malls in Israel, Peru, and the Philippines, using suicide bombers and improvised explosive devices (IEDs).

(U) Vulnerability Overview

(U//FOUO) Open Access Provides Unique Targeting Opportunities

(U) Commercial facilities are especially vulnerable to terrorist attack, because they are open to the public and accommodate a large number of people within specific known time periods making it difficult to detect operational planning and surveillance. Each commercial facility's engineering, design, size, age, purpose, and number of occupants influences its vulnerability to the various means by which terrorists could strike.

(U) Attacks against mass transportation systems overseas underscore the interdependent nature of the CFS with other CI/KR. Commercial facilities often are strategically located near other sectors and assets (for example, mass transportation, mass gathering locales, centers of

government), thus exposing sector assets to collateral damage from attacks directed primarily against the other sectors.

(U//FOUO) Disrupted Plot Provides Insight into Terrorists' Targeting

(U//FOUO) Al-Qa'ida operative Dhiran Barot, recently sentenced in the United Kingdom for his participation in preoperational terrorist activities, conducted surveillance operations against three major financial institutions in the New Jersey–New York area and against two international financial institutions in Washington, D.C. Barot's surveillance activities probably took place between late 2000 and early 2001, although some of the notes he took appear to have been revised in January 2004.

- (U//FOUO) These casing reports—discovered in July 2004—suggest that the terrorists' targeting strategy toward the CFS is aimed primarily at high-profile financial institutions and the commercial facilities that house them.

- (U//FOUO) The casing reports focused on the location, layout, and construction of the target, security measures, access to underground parking areas, traffic and pedestrian flow, access and escape routes, structural surveys, positions of closed circuit television (CCTV) cameras, and a host of other information, including recommendations for the type of attack.

- (U//FOUO) Although the seized casing reports cited specific buildings or areas, DHS assesses that the type of information that Barot sought would be applicable to terrorist surveillance of assets throughout the CFS.

(U//FOUO) The casing reports demonstrate a high level of detail and awareness of site vulnerabilities, security operations, and law enforcement and emergency response activities. DHS and the FBI found no further reporting to indicate that operations targeting these facilities have developed beyond the initial planning phase. No immediate short-term risk to commercial facilities has been identified, and sector owners and operators have addressed many of the vulnerabilities identified in the casing reports through a variety of protective measures. Nevertheless, the attention Barot paid to these potential targets reflects a sophisticated al-Qa'ida understanding of the complexity of the CFS.

(U//FOUO) Scenarios of Concern

(U//FOUO) Use of Vehicle-Borne Improvised Explosive Devices

(U//FOUO) VBIED attacks would inflict immediate casualties and destruction, create fear and panic among survivors, and paralyze businesses in the affected area. Moreover, a high-profile physical attack would attract the extensive media attention that al-Qa'ida seeks.

— (U//FOUO) The preferred method of attack cited in the casing reports by Barot was a VBIED loaded into a limousine or a service or delivery truck to discourage any undue attention or suspicion on the part of security personnel. Barot recommended parking a VBIED-equipped limousine in the VIP garage beneath a building after gaining access by deception or by compromising the security personnel. He described routes that would permit the attack team to escape before detonation. Ramming a truck such as an oil tanker through the main entrance was an alternative option.

— (U//FOUO) Barot surveilled building entrances, underground parking garages, and loading docks as possible points of attack.

(U//FOUO) Use of Improvised Explosive Devices

(U//FOUO) Alternatively, Barot calculated that several terrorists could bring bomb components into a building in small suitcases or small bags, since these items were not inspected by building security. The bomb could then be assembled in a restroom.

— (U//FOUO) Barot downplayed the effectiveness of a man-portable IED attack because it would likely cause little damage to a solidly-constructed building.

— (U//FOUO) Barot also considered the casualty-producing power of shattered glass in a building that has a large public atrium. He cited a television program that described the killing effects of fragmented glass during an explosion. His report noted the level of pedestrian traffic and the peak hours when large crowds congregated in front of the building.

(U//FOUO) Use of Aircraft as a Weapon

(U//FOUO) The Barot reports contained pamphlets and information about private helicopter companies and heliports, suggesting a possible aerial attack scenario against the CFS.

— (U//FOUO) Terrorists remain intent on using an aircraft as a weapon and have a number of options at their disposal. Alternatives include the suicide hijacking of a U.S.-bound commercial airliner or an international flight flying through U.S. airspace. Al-Qa‘ida explored similar plotting in the summer of 2003. Such a plot would allow terrorists to take advantage of the perceived less-stringent security procedures at foreign airports.

(U) Consequence Overview

(U//FOUO) DHS has identified three al-Qa‘ida strategic objectives of carrying out an attack operation against Homeland assets: inflicting mass casualties, striking targets that are symbolic of U.S. culture, and causing economic damage. A successful terrorist attack against the CFS has the potential to achieve all three objectives.

(U//FOUO) **Mass Casualties:** In a March 2003 speech Usama Bin Ladin stated, "You know that seeking to kill Americans and Jews everywhere in the world is one of the greatest duties [of Muslims] and the good deed most preferred by Allah." DHS analysis of foiled plots identifies al-Qa'ida's interest in employing attacks against commercial facilities such as commercial buildings, apartment buildings, or populated areas to inflict mass casualties. The large population densities present in commercial office complexes, apartment buildings, and retail facilities represent soft, target-rich locations that could enable al-Qa'ida to achieve its mass casualty objectives.

(U//FOUO) **Targets of Symbolic Value:** Terrorists focus on commercial facilities as symbols of Western capitalism. Khalid Shaykh Muhammad—mastermind of the 11 September 2001 attacks—emphasized during detainee interviews the importance of selecting targets of symbolic value. Foiled plots against commercial facilities—such as the mid-2002 al-Qa'ida plot to attack West Coast buildings and the alleged 2002 plot to blow up U.S. apartment buildings—underscore al-Qa'ida's interest in attacking U.S. commercial facilities even after the 11 September 2001 Homeland heightened security posture.

(U//FOUO) **Economic Damage:** In 2003 Bin Ladin lauded the 11 September 2001 hijackers because "they struck at the very heart of the economy." In an October 2004 statement, he quoted the finding of the Royal Institute of International Affairs to the effect that the total cost of the 11 September 2001 attacks—direct and indirect—to the United States was at least $500 billion, demonstrating al-Qa'ida's understanding and awareness of the economic impact of a successful terrorist attack against the United States.

(U) Actions to Reduce Risk

(U//FOUO) The 11 September 2001 attacks demonstrated that mitigating the most significant risks to commercial facilities probably lies outside the scope of what most owners and operators can do. Owners and operators of CFS assets, however, do have the capability to protect against the prevailing threats against the sector—suicide bombers and VBIEDs. Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Implementation of protective measures involves the commitment of resources in the form of people, equipment, materials, time, and money. Protective measures are designed to meet the following objectives:

(U//FOUO) **Devalue:** Lowering the value of a facility to terrorists makes it a less attractive target. Some common protective measures that would make a commercial asset a less useful target are:

- (U) Providing adequate perimeter fencing or walls around facility grounds.

— (U) Developing and maintaining a plan for communicating information to the public, including quelling rumors. Relationships should be cultivated with the media ahead of time with an identified public information officer.

— (U) Using temporary barriers to expand the zone around the buildings/facility and populated areas.

— (U) Providing inspection areas that are not visible to the public.

— (U) Evacuating personnel from any facility where a confirmed threat exists and considering closing the facility until the threat level is reduced.

(U//FOUO) **Detect:** Spotting the presence of adversaries or dangerous materials provides information needed to mount an effective response. Some protective measures that can be put in place for detection are:

— (U) Training security staff regularly to include countersurveillance techniques.

— (U) Incorporation of a screening process that denies access to patrons with hand-carried items until the items have been physically inspected.

— (U) Monitoring of all access points and restricted areas 24 hours, 7 days a week to include the use of CCTV.

— (U) Increasing the number of police patrols and providing additional weapons and equipment to the security force at any facility where a confirmed threat exists.

— (U) Prohibiting the presence of nonessential vehicles at the venue or facility grounds and thoroughly searching all vehicles entering the area, to include the undercarriage.

— (U) Providing daily security and awareness briefings to administrative and other essential personnel.

— (U) Employing advanced security surveillance technologies.

(U//FOUO) **Deter:** Make the facility more difficult to attack successfully. Common protective measures to deter an attack include:

— (U) Randomly screening guests, employees, event participants, and delivery, service, and emergency services personnel before they are allowed to enter the venue or facility.

— (U) Physically inspecting all vehicles and identifying the driver before he or she is allowed to approach the venue or facility.

— (U) Strategically placing barriers to guide the flow of vehicles for access to drop-off and pick-up points, parking areas, and delivery points.

— (U) Ensuring grounds are covered by plain view CCTV and are monitored 24 hours, 7 days a week.

— (U) Ensuring lighting illuminates the venue facility and is integrated with backup power in the event of an emergency.

— (U) Arranging for law enforcement vehicles to park randomly near entrances and exits before and during all high-profile events.

— (U) Coordinating with local authorities regarding closing of public roads and facilities.

— (U) Increasing stand-off by limiting parking in the vicinity of the structures.

— (U) Pre-positioning and mobilizing specially trained teams or resources.

— (U) Providing continuous guard visibility.

(U//FOUO) **Defend:** Defense involves responding to an attack to defeat adversaries, protecting the facility, and mitigating any effects of an attack. Some common protective measures that would be effective in the defense of an attack on a commercial asset include:

— (U) Ensuring that all appropriate personnel protection measures have been taken.

— (U) Ensuring that all security force and emergency responders have the appropriate tools, equipment, and personal protective equipment.

— (U) Notifying appropriate staff and employees of any change in the threat condition.

— (U) Implementing emergency and contingency plans, including plans to help carry out evacuation measures or to respond to emergency management requests.

— (U) Activating command and support centers and assigning staff members to local government emergency operations centers.

— (U) Ensuring that Unified Incident Command Teams work closely with law enforcement, fire departments, and other agencies to prepare for emergencies through planning and drills.

(U//FOUO) Implementation of protective measures changes the security posture for the individual asset and for the sector as a whole. Because the vast majority of the CFS assets are

privately-owned and operated, security decisions rest with individual asset owners and operators. For the most part, the adoption and implementation of security measures have been carried out on an ad hoc, voluntary, or industry-driven basis. Individual asset owners and operators are generally responsible for their own security measures, and many also develop partnerships with local law enforcement and emergency personnel. Additional security measures may be applicable to a wide range of facilities against a number of threat streams.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operations Center (NOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the NOC can be reached by telephone at 202-282-8101 or by e-mail at NOC.Common@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) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) Tracked by:

(U) HSEC 010000-01-05
(U) HSEC 021500-01-05
(U) HSEC 030000-01-05
(U) TERR 020000-01-05
(U) TERR 041000-01-05
(U) TERR 060000-01-05
(U) INFR 150000-01-05