Homeland Security

Office of Infrastructure Protection

Infrastructure Protection Note

(U) Infrastructure Protection Note: Evolving Threats to the Homeland

24 May 2010, 1400 EDT

(U//FOUO) The Office of Infrastructure Protection (IP) Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces Infrastructure Protection Notes to address issues impacting the infrastructure protection community's risk environment from terrorist threats and attacks, natural hazards, and other events. Based on the analysis within the DHS Office of Intelligence and Analysis product *Evolution of the Terrorist Threat to the United States* this IP Note outlines the evolution of terrorist threats and impacts to the Nation's critical infrastructure. [1]

(U) KEY FINDINGS

- **(U//FOUO) Given recent terrorist activity, homeland security partners should operate under the premise that other operatives are in the country and could advance plotting with little or no warning.**
- **(U//FOUO) Al-Qa'ida and its affiliates are focusing on smaller operations in the United States that are harder to detect but more likely to succeed than the large-scale attacks they once emphasized.**
- **(U//FOUO) The increasing prevalence and role of Westerners (including U.S. citizens) in al-Qai'da and associated groups, either as leaders or operatives, gives these individuals knowledge of Western culture and security practices.**
- **(U//FOUO) HITRAC assesses the sectors at greatest risk from these attack scenarios are Commercial Facilities, Government Facilities, Banking and Finance, and Transporation.**

(U) BACKGROUND

(U//FOUO) The U.S. Homeland faces a persistent and evolving terrorist threat from a number of violent "jihadist" groups that are aligned ideologically with, but not necessarily directed by, al-Qa'ida. These groups are driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities. [2]

(U//FOUO) Al-Qai'da and its affiliates will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. [3] Historically, al-Qa'ida has focused on prominent political, economic, and infrastructure targets with the intent to

---

[1] (U//FOUO) DHS Office of Intelligence and Analysis, Evolution of the Terrorist Threat to the United States, 21 May 2010.
[2] (U) National Intelligence Estimate: The Terrorist Threat to the US Homeland. July 2007.
[3] (U) Ibid

produce mass casualties, visually dramatic destruction, significant economic aftershocks, and fear among the population. The group is innovative in creating new capabilities and overcoming security obstacles.[4]

(U) ***Potential Attack without Warning***

(U//FOUO) There is an increased challenge in detecting terrorist plots underway because of the current trend and tactics which use individuals or small groups acting quickly and independently or with only tenuous ties to foreign handlers. State, local, tribal, and private sector partners play a critical role in identifying suspicious activities and raising awareness of federal counterterrorism officials.

(U//FOUO) Given recent terrorist activity, homeland security partners should operate under the premise that other operatives are in the country and could advance plotting with little or no warning.

(U) ***Increased Frequency of Attacks Possible***

(U//FOUO) Recent events suggest a trend in which terrorists seek to conduct smaller, more achievable attacks against easily accessible targets. Within the past year, attempted attacks and plots in the United States progressed to an advanced stage largely because of these groups' ability to use operatives that have access to and familiarity with the U.S. as well as their use of new and varied attack patterns.

(U//FOUO) The evolving threat and increasing resilience of al-Qa'ida and other terrorist organizations have been highlighted by a number of recent domestic events, including the Times Square bombing attempt, the Fort Hood attack and the December 2009 airline bomb plot. **The number and pace of attempted attacks against the United States over the past nine months have surpassed the number of attempts during any other previous one-year period.**

(U) Globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack – all without requiring a centralized terrorist organization, training camp, or leader.[5]

(U//FOUO) The increasing prevalence and role of Westerners (including U.S. citizens) in al-Qai'da and associated groups, either as leaders or operatives, gives these individuals knowledge of Western culture and security practices. U.S. persons who hold leadership positions in al-Qai'da and associated groups have also called publicly on Western individuals to wage jihad by conducting attacks locally.

(U//FOUO) The analysis below builds on these judgments by identifying the relative risk of attacks given the vulnerabilities and potential consequences of an attack on specific CIKR sectors.

---

[4] (U) National Intelligence Estimate: The Terrorist Threat to the US Homeland, July 2007.
[5] (U) Ibid.

(U) INFRASTRUCTURE RISK

(U//FOUO) The evolving and dynamic terrorist threat and the ever-increasing resilience of al-Qa'ida and other like-minded terrorist organizations, while less frequent than natural disasters or accidents, pose a significant threat to the Nation's critical infrastructure. Overall infrastructure risk is further amplified due to challenges in detecting terrorist plots underway because of the current trend of tactics which use individuals or small groups that can act quickly and independently or with only tenuous ties to foreign handlers.

(U//FOUO) The use of explosives continues to be a preferred tactic in terrorist attacks around the globe. Improvised explosive devices (IEDs) can be combined with suicide tactics for delivery against a wide array of critical infrastructure targets. Explosive devices may be man carried or vehicle borne (VBIED), used as the primary attack method or as a key element of an armed assault. IEDs are often assembled in situ using homemade explosives which are manufactured with readily available consumer products.

(U//FOUO) These attack scenarios have the potential to cause casualties and localized disruption within all critical infrastructure and key resources (CIKR) sectors. HITRAC assesses that Commercial Facilities, Government Facilities, Banking and Finance, and Transporation/Mass Transit face greatest risk from these attack scenarios due to their public accessibility, the high density of people in enclosed areas and the potential for psychological impacts beyond the initial attack.

(U) PROTECTIVE MEASURES

(U//FOUO) Protective measures have been identified for the above mentioned sectors that are specific to the techniques, tactics, and procedures and attack methods (suicide attacks, IEDs, and VBIEDS) discussed above. [6,7]

(U//FOUO) For additional information on protective measures, please see the source documents in this IP Note. Additionally, detailed information on IEDs is provided for law enforcement by the Department of Homeland Security at TRIPwire.dhs.gov or TRIPwire Community Gateway (http://cs.hsin.gov) if you are a member of the private sector. For access to either system, please contact help@tripwire.dhs.net. For further information on TRIPwire and bombing prevention contact the DHS Office for Bombing Prevention at obp@dhs.gov.

(U) *Commercial Facilities, Government Facilities and Banking and Finance*

(U//FOUO) DHS recommendations for protective measures in the Commercial Facilities, Government Facilities, and Banking and Finance sectors focus on planning and standards; accessibility and control; and operational security to deter terrorist operational planning and attack. These measures specifically aim to increase security, maintain awareness by both employees and the general public, and to ensure that facilities have adequately planned for emergencies and continuity of operations.[8,9,10]

---

[6] (U) DHS, Office of Bombing Prevention, TRIPwire, General Protective Measures for Vehicle Borne Improvised Explosive Devises.

[7] (U) DHS, Office of Bombing Prevention, TRIPwire, Protective Measures for Suicide Bombers.

[8] (U//FOUO) DHS Office of Infrastructure Protection, Protective Security Coordination Division, Characteristics and Common Vulnerabilities Infrastructure Category: Banking and Financial Institution Physical Facilities, 31 January 2008.

- (U//FOUO) Emergency planning, business continuity planning, and adhering to industry standards and building codes ensure that facilities and technology systems are adequately prepared for attempted attacks or disasters.

- (U//FOUO) Controlling access to facilities and technology reduces the ability of unidentified people, objects, and vehicles to enter the facility and technology systems.

- (U//FOUO) Maintaining operational security by employees and facilities' guards provides the capability to identify activities and items that are outside of the norm and have them reported.

- (U//FOUO) Follow other DHS approved protocols for protecting CIKR based on current threat levels.

(U) ***Transportation: Mass Transit***

(U//FOUO) DHS recommendations for protective measures in the transportation sector focus on regional collaboration, employee vigilance, and public awareness to deter terrorist operational planning and attack. These measures specifically aim to increase security, maintain awareness by both employees and the general public, and to ensure that facilities have adequately planned for emergencies and continuity of operations.

- (U//FOUO) Regional collaboration among federal, state, local, and private sector officials enhances the level of security awareness and expands the scope of security resources available in and around mass transit systems and passenger railroads.

- (U//FOUO) Employee vigilance provides additional capabilities to identify suspicious activities and items in and around trains, buses, rail lines, stations, terminals, tunnels, bridges, elevated track, and other key facilities. Employees are force multipliers for railroad and mass transit security programs.

- (U//FOUO) Public awareness is crucial to inspire vigilance and timely reporting of suspicious activities and items. Vendors and others who work at or near facilities can expand security efforts. Law enforcement officers should be familiar with and engage those with the ability to reinforce their security efforts.[11]

(U//FOUO) By following the recommended procedures above, facility owners can substantially impact the risks associated with an attack. DHS actively works with Federal, State, local, tribal, territorial, and private sector partners to implement this approach and consistently improve collaborative security efforts.

---

[9] (U//FOUO) DHS Office of Infrastructure Protection, Protective Security Coordination Division, High-Rise Buildings: Potential Indicators of Terrorist Activity, Common Vulnerabilities and Protective Measures, 31 July 2008.

[10] (U//FOUO) DHS Office of Infrastructure Protection, Protective Security Coordination Division, Large Federal Office Buildings: Potential Indicators of Terrorist Activity, Common Vulnerabilities and Protective Measures, 30 April 2008.

[11] (U//FOUO) DHS Office of Infrastructure Protection, Protective Security Coordination Division, Subway Systems: Common Vulnerabilities and Protective Measures, 05 October 2007.