Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
Homeland Security
Office of Infrastructure Protection
Office of Intelligence & Analysis
Infrastructure Protection Note

(U) Infrastructure Protection Note: Awareness Independence Day 2010

30 June 2010, 1700 EDT

(U) SCOPE

(U//FOUO) The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces Infrastructure Protection Notes to provide information on risks impacting the critical infrastructure community including terrorist threats, natural hazards, and other events. This IP Note is a joint publication of the DHS Office of Intelligence and Analysis (I&A) Homeland Counterterrorism Division and the Office of Infrastructure Protection (IP), and is designed to promote security awareness and to identify actions that the critical infrastructure community can take to mitigate risks to the Nation's critical infrastructure. As an update to the 26 May 2010 *IP Note: Preparing for an Evolving Terrorist Threat*, this IP Note serves as a reminder for the critical infrastructure community to remain vigilant during the 4 July 2010 Independence Day holiday.

(U) KEY FINDINGS

- (U//FOUO) There are no specific or credible terrorist threats to the 4 July 2010 Independence Day celebrations and associated events held across the country. The large gatherings at celebrations and events, however, could make them desirable targets for a violent organization or individual.

- (U//FOUO) Properly implemented protective measures will decrease the risk posed to the nation's critical infrastructure.

- (U//FOUO) HITRAC assesses that the Commercial Facilities, Government Facilities and Transportation/Mass Transit sectors face the greatest risk because of their public accessibility, the large numbers of people often present, and the potential for psychological impacts beyond the initial attack.

(U) BACKGROUND

(U//FOUO) DHS has no indications of specific or credible terrorist threats to the Homeland associated specifically with the Independence Day holiday. Most international terrorist attacks against targets in the West have not been timed to coincide with major dates or high-profile events. Terrorists could find an attack during Fourth of July celebrations attractive, however, because they attract large gatherings and prominent media attention.

(U//FOUO) On 12 May 2010, an unknown contributor to a known violent extremist website encouraged the placement of suspicious-appearing, but harmless, bags in multiple locations in

Washington, DC and New York City, NY, noting that repeated bogus threats would desensitize law enforcement authorities and the public to potential threats. This does not indicate a direct threat to any Independence Day celebrations, but we urge vigilance in identifying suspicious activities.[1]

(U) INFRASTRUCTURE RISK

(U//FOUO) The summer weather affords many Americans the opportunity to conduct activities outdoors, many of them in mass gatherings which provide potentially attractive targets for terrorists seeking to conduct mass casualty attacks. Special events, such as Independence Day celebrations warrant increased attention to security.

(U//FOUO) Explosive devices continue 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. These devices may be person borne or vehicle borne, and used as the primary attack method or as an element of an armed assault.

(U//FOUO) Many attack scenarios have the potential to cause casualties and localized disruption across multiple critical infrastructure and key resources (CIKR) sectors. HITRAC assesses that the Commercial Facilities, Government Facilities and Transportation/Mass Transit sectors face the greatest risk because they are publicly accessible, the potential for mass casualties, and the potential for severe psychological impact.

(U) PROTECTIVE MEASURES

(U//FOUO) DHS has identified measures suited for protecting these critical infrastructure against suicide attacks, IEDs, and vehicle borne improvised explosive devices.[2,3]

(U//FOUO) State, local, tribal, territorial, and private sector partners play a critical role in identifying suspicious activities and raising awareness of federal counterterrorism officials. The "If You See Something, Say Something,"[4] campaign developed by New York City's Metropolitan Transportation Authority (MTA) is a best practice that can be readily adopted nationwide. It effectively stresses that every individual can be a part of the first line of defense against a terrorist attack. The attempted 1 May Times Square bombing showcased the value of raising public awareness and the importance of remaining vigilant.

(U//FOUO) By following the recommended procedures, facility owners can mitigate some of the risks associated with an attack.

(U//FOUO) The principal objectives of protective measures are to complicate attack planning and surveillance, protect potential targets, and mitigate the risk of an attack. An effective approach should involve three phases: prevention, assessment and detection, and response.

---

[1] (U//LES) National Capital Region Summer Tourist Season Increases the Potential for Terrorist Threats, Federal Bureau of Investigation, 27 May 2010.
[2] (U) DHS, Office of Bombing Prevention, TRIPwire, General Protective Measures for Vehicle Borne Improvised Explosive Devises.
[3] (U) DHS, Office of Bombing Prevention, TRIPwire, Protective Measures for Suicide Bombers.
[4] (U) Metropolitan Transportation Authority, If You See Something, Say Something. 2010 http://www.mta.info/mta/security/index.html

(U//FOUO) **Prevention Phase**: This phase incorporates security procedures that complicate attack planning and execution, increase the safety of the public and response personnel in threat situations, and promote consistent reporting of suspicious activities. Best practices include:

- (U//FOUO) Establishing a public awareness and vigilance campaign that reinforces public awareness of threats, and ensuring that a simple and consistent mechanism is in place to report suspicious activities.
- (U//FOUO) Maintaining police presence at strategic locations within at-risk venues, specifically at all entrance sites or traffic choke points.
- (U//FOUO) Identifying and pre-designating primary and secondary evacuation routes and assembly areas for building or site occupants.

(U//FOUO) **Assessment and Detection Phase**: This phase addresses considerations of vehicle assessment to rule out potential threats or determine the need to request bomb squad response.

- (U//FOUO) Conduct random explosive detection canine searches to avoid taxing valuable resources.
- (U//FOUO) Stagger search times and patterns to implement counter-surveillance measures.
- (U//FOUO) Canvas area to garner information and/or witness information to determine "who, what, when, where, and why" for an unattended vehicle left at site, in order to rule out legitimate deliveries, etc.

(U//FOUO) **Response Phase**: This phase addresses protective actions necessary once a threat or attack is recognized.

- (U//FOUO) Evacuate the threatened or attacked area, ensuring that the evacuation site is far enough away to protect individuals from blast and fragmentation; suspicious vehicles should not be moved until cleared by bomb squad personnel.
- (U//FOUO) Maintain awareness of the possibility of a secondary device that targets an evacuation site, or a command post used by emergency responders.

(U//FOUO) DHS collaborates with federal, state, local, tribal, territorial, and private sector partners to implement and refine protective measures to improve critical infrastructure security. For additional information on protective measures, please see the source documents in this IP Note. Detailed information on sector-specific protective measures is provided for law enforcement by DHS at https://TRIPwire.dhs.gov and can be accessed through the Homeland Security Information Network (HSIN) https://cs.hsin.gov.