Assessment

(U//FOUO) Analysis of Incidents Directed Against Courthouses in the United States

IA-0218-10

Office of Intelligence and Analysis

ASSESSMENT

(U//FOUO) Analysis of Incidents Directed Against Courthouses in the United States

6 April 2010

(U) Prepared by the DHS/I&A Domestic Threat Analysis Division, Infrastructure Threat Analysis Branch to promote awareness of emergent threats to homeland security and identify resources that may assist in developing priorities for protective and support measures by the Department, other agencies of the federal government, state and local government agencies and authorities, the private sector, and other entities. Federal efforts to influence domestic public opinion must be conducted in an overt and transparent manner clearly identifying U.S. Government sponsorship. Coordinated with the DHS/Office for Bombing Prevention and the FBI/Directorate of Intelligence, Counterterrorism Division, Threat Review Unit. The Interagency Threat Assessment and Coordination Group reviewed this product from the perspective of our nonfederal partners.

(U) Scope

(U//FOUO) This assessment describes threats and other suspicious activities directed against courthouses in the United States over the past twelve months. Additionally, it provides indications of surveillance and suggested protective measures for vehicle-borne improvised explosive devices and homicide-suicide bombers to assist in the protection of courthouses and related facilities.

(U) Key Findings

(U//FOUO) The DHS/Office of Intelligence and Analysis (I&A) has no credible or specific reporting indicating preoperational activity or imminent plans by al-Qa'ida or other terrorist or violent extremist organizations to attack courthouses in the United States.

(U//FOUO) Based upon an analysis of the threats and suspicious activities listed below, the majority of threats likely were conveyed by individuals intending to delay, cancel, or harass court proceedings.

(U) Threats and Other Suspicious Incidents

(U//FOUO) Since the beginning of 2009, at least 23 reported incidents have been directed against federal and local courthouses—one fatal shooting, one attempted bombing, three suspicious packages, five hoax bomb threats, and eleven suspicious incidents involving photography. With the exception of the foiled September 2009 plot to bomb the Federal Building in Springfield, none of these incidents have any link to terrorism.

(U) Incidents Directed Against Courthouses

(U) The majority of incidents occurred in, or were directed at U.S. Federal Courthouses nationwide during the period 1 January 2009-present. The following is the breakdown of the reported incidents:

Bomb Threats:
Federal: 3
Local: 3

Attempted Bombing:
Federal: 2
Local: none reported

Shootings:
Federal: 1
Local: none reported

Suspicious Packages:
Federal: 2
Local: none reported

Photography:
Federal: 11
Local: 1

(U) Bomb Threats

— (U) 22 December 2009: An unidentified male claiming to be an employee of a county circuit court stated in a hoax call to the court that he had placed several bombs within the courthouse.

— (U) 15 December 2009: A sheriff's department received a hoax telephonic bomb threat to an unspecified U.S. courthouse.

— (U) 13 May 2009: An attorney's office received a hoax telephonic bomb threat to the county courthouse from an unidentified male who claimed to be an FBI agent.

— (U) 11 May 2009: An unidentified male made two bomb threats in hoax phone calls to a county courthouse.

— (U) 9 May 2009: An unidentified male called a 911 call center and threatened to blow up the "Federal Building" and release federal inmates.

— (U) 4 April 2009: A 911 call center received a hoax telephonic bomb threat from an unidentified male to a building which houses a federal court.

(U) Attempted Bombings

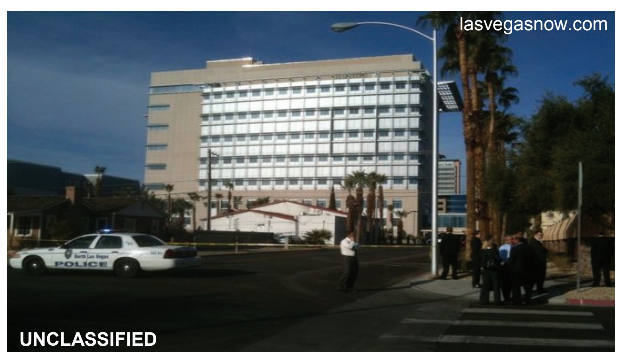
— (U) 24 September 2009: An Illinois man was arrested by federal law enforcement authorities for allegedly plotting to detonate a vehicle-borne improvised explosive device (VBIED) at the Paul Findley Federal Building and U.S. Courthouse. The plot was discovered as a result of an undercover operation conducted by federal law enforcement officials.

(U) Paul Findley Federal Building and U.S. Courthouse, Springfield, Illinois.

— (U) 17 May 2009: A suspicious package described as a small beer keg with a fuse sticking out of it was discovered by security personnel at the Robert T. Matsui Federal Courthouse in Sacramento, California. Police explosive ordnance disposal personnel safely removed the package that was later determined to be an incendiary device.

(U) Shootings

— (U) 4 January 2010: A lone gunman killed a federal court security officer and wounded a Deputy U.S. Marshall at the Federal Courthouse in Las Vegas before being shot to death by police.



(U) Lloyd D. George U.S. Federal Courthouse, Las Vegas, Nevada.

(U) Suspicious Packages

— (U) 24 March 2009: White powder, later determined to be crushed drywall powder, was poured outside the entrance to the Edward R. Roybal Federal Building and U.S. Courthouse in Los Angeles, California.

— (U) 27 January 2009: The U.S. District Court in Kansas City, Missouri received a suspicious envelope in the mail leaking an unknown yellowish-green powdery substance. The envelope was mailed from an identified correctional facility and was addressed to the chief clerk. Tests revealed the substance was not hazardous.

(U) Photography

(U) Photography is one of the most commonly reported suspicious activities around the majority of critical infrastructure assets in the United States. Activities such as suspected surveillance, photographing and videotaping facilities, and attempts to gain access possibly to test security procedures are similar to preoperational surveillance and attack planning techniques used by terrorists and violent extremists. During the past year, incidents of individuals photographing federal courthouses were reported, 2 of which were directed against the same location in California. These included:

— (U) 17 December 2009: An individual was questioned by a court security officer after he was observed videotaping in a San Diego courtroom. The video recording included footage of the interior and exterior of the courthouse as well as the weapons screening area.

— (U) 6 November 2009: An individual was questioned by the police after he was observed photographing the Niagara Falls City Courthouse.

— (U) 20 September 2009: A federal security officer observed two unidentified males photographing the Sandra Day O'Connor Federal Courthouse in Phoenix, Arizona.

— (U) 23 April 2009: A federal security officer observed an unidentified male photographing the Federal Courthouse in Alexandria, Virginia from a vehicle, using a camera equipped with a large telephoto lens.

— (U) 30 March 2009: A police officer observed an unidentified passenger in a vehicle using a digital camera to photograph the Edward R. Roybal Federal Building in Los Angeles.

— (U) 5 March 2009: An individual was questioned by the police after he was observed taking pictures of the Edward R. Roybal Federal Building from his vehicle.

(U) Indications of Surveillance

(U//FOUO) The following activities may suggest terrorist surveillance of courthouses and related facilities. Alone, each indicator can represent legitimate recreational or commercial activities as well as criminal activities not related to terrorism; multiple indicators, however, could suggest a heightened terrorist threat:

— (U//FOUO) Unusual or prolonged interest in security measures or personnel, entry points, access controls, or perimeter barriers such as fences or walls.

— (U//FOUO) Interest without justification in obtaining site plans for courthouses and related facilities such as parking garages and information on employees.

— (U//FOUO) Unusual behavior, such as staring at or quickly looking away from personnel or vehicles entering or leaving facilities or parking areas.

— (U//FOUO) Observation of security reaction drills or procedures.

— (U//FOUO) Increase in anonymous telephone or e-mail threats to facilities in conjunction with suspected surveillance incidents, indicating possible surveillance of threat reaction procedures.

— (U//FOUO) Surveillance by individuals using bicycles, scooters, motorcycles, cars, trucks, sport utility vehicles, limousines, boats, or small aircrafts.

— (U//FOUO) Prolonged static surveillance using operatives disguised as panhandlers, shoe shiners, food or flower vendors, news agents, or street sweepers not previously seen in the area.

— (U//FOUO) Discreet use of still cameras and video recorders, note taking, or use of sketching materials near a courthouse.

— (U//FOUO) Use of multiple sets of clothing and identification.

— (U//FOUO) Suspicious questioning of security or facility personnel.

— (U//FOUO) Unexplained presence of unauthorized individuals.

(U//FOUO) Courthouse officials are encouraged to review and update evacuation plans and security and emergency policies. In addition to courthouses and the first responder community (law enforcement, emergency medical services, and fire departments), planning and exercises should involve the local medical community to ensure that mass casualty contingencies are fully covered.

(U) Protective Measures

(U) Courthouses and related offices and facilities pose complex security challenges for law enforcement. The principal objectives for implementing protective measures against an attack on a courthouse are to complicate attack planning and surveillance, protect potential targets, and mitigate the risk of attack. Attacks can come in the form of single or multiple shooters, biological contamination by agents such as anthrax-laced letters or packages, and improvised explosive device (IED) attacks, among others. To reduce vulnerabilities to an attack from various forms of explosive devices and improvised incendiary devices (IIDs), the DHS Office for Bombing Prevention (OBP) recommends the protective measures listed in the appendices.

(U) Outlook

(U//FOUO) DHS/I&A has no credible or specific information to suggest that transnational terrorists or violent extremists plan to attack courthouses in the United States. Nevertheless, the shooting at the Federal Courthouse in Las Vegas and the foiled plot to detonate a VBIED at the Federal Courthouse in Springfield, Illinois are reminders that facility security personnel should remain vigilant, adapt and enhance security as appropriate, and report any suspicious activities.

(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. The nearest state and local fusion centers contact information can be found online at http://www.dhs.gov/files/resources/editorial_0306.shtm. The FBI regional phone 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) Detailed information on improvised explosive devices 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. If you need access to either system, please contact tripwirehelp@dhs.gov. For further information on TRIPwire and bombing prevention contact the DHS Office for Bombing Prevention at obp@dhs.gov.

(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, then follow a few simple steps to complete and submit your response. Thank you.

(U) Tracked by: HSEC-02-15000-ST-2009, HSEC-03-00000-ST-2009

Survey

(U) Appendix A: General Protective Measures for Vehicle-Borne Improvised Explosive Devices

(U) Scope

(U) The principal objectives for implementing protective measures are to complicate attack planning and surveillance, protect potential targets, and mitigate the risk of attack. An effective approach should consider these phases:

— (U) Prevention
— (U) Assessment and Detection
— (U) Response

(U) Prevention Phase

(U) Security procedures should complicate attack planning and execution, increase public and responder safety in threat situations, and promote consistent reporting of suspicious activities and vehicles.

— (U) Establish a public awareness and vigilance campaign that reinforces public awareness of any looming threat.

— (U) Ensure a simple and consistent mechanism is in place to report suspicious activities.

— (U) Consult the responsible bomb squad commander to develop a routine policy that ensures a simple and consistent mechanism is in place to report suspicious vehicles and categorize incidents.

— (U) Maintain police presence at strategic locations in and around at-risk venues, specifically at all entrance sites or traffic choke points.

— (U) Have agencies review surveillance detection and countersurveillance procedures to enhance awareness of possible attack planning.

— (U) Establish evacuation protocols for VBIED threats (for example, fire drills, code words) and identify and pre-designate primary and secondary evacuation routes and assembly areas for building or site occupants.

— (U) Identify pre-designated vehicle screening points or marshalling areas to check identification and manifests of approaching service vehicles.

— (U) Create serpentine vehicle access and choke points to impede approach of a VBIED toward a possible target.

— (U) Emplace vehicle barriers where appropriate and necessary; use multiple layers of barriers to prevent or impede use of multiple VBIEDs to breach a high risk or high consequence target or conduct follow-on attack.

— (U) Include surveillance detection considerations within crowd control protocols.

— (U) Identify potential sources of bomb-making materials and precursor components for IEDs; develop awareness programs to inform point-of-sale employees when and how to alert authorities to suspicious purchases.

— (U) Identify routine shipments and thefts of explosives or bomb-making materials to determine possible sources of IED components and identify potential locations which could be used as staging, assembly, or rehearsal sites.

— (U) Inform service industry and hotel employees to be alert to potential indicators of attack planning activities such as maps, photographs, and communications equipment.

(U) Assessment and Detection Phase

— (U) Conduct random explosive detection canine searches; stagger search times and patterns to implement counter-surveillance measures.

— (U) Canvas area to garner information 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) Review and identify local use-of-force policies that can be applied to challenge a potential suicide VBIED, should it be encountered.

— (U) Make approaches and negotiations by use of remote means.

(U) Response Phase

— (U) Evacuate the area surrounding a suspect vehicle, moving evacuees a considerable distance away to avoid blast and fragmentation; suspect vehicles should not be moved until cleared by bomb squad personnel.

— (U) Maintain vigilance for the possibility of a secondary device that may also be a VBIED. An additional device may be used to target an evacuation site or command post areas used by the response community.

— (U) Maintain awareness of possible remote initiation of a suicide VBIED, or a timer back-up should the VBIED fail to function.

(U) Appendix B: General Protective Measures for Homicide-Suicide Bombers

(U) Scope

(U) The principal objectives for implementing protective measures against a homicide or suicide bomber are to complicate attack planning and surveillance, protect potential targets, and mitigate the risk of attack. An effective approach should consider these phases:

— (U) Prevention
— (U) Assessment and Detection
— (U) Response

(U) Prevention Phase

(U) Security procedures should complicate attack planning and execution, increase public and responder safety in threat situations and promote consistent reporting of suspicious activities and persons.

— (U) Establish a public relations campaign that reinforces public and private sector awareness of explosive devices threats.

— (U) Develop a routine policy that ensures a simple and consistent mechanism is in place to report suspicious activities and persons, and to categorize incidents.

— (U) Ensure employees, responders, and the public understand the associated hazard distances from blast and fragmentation and basic procedures and distances for personnel safety.

— (U) Maintain visible police and security presence such as access control and perimeter security at various locations within at-risk venues, specifically all entrance sites and choke points.

— (U) Institute random security procedures around potential targets to complicate attack planning, including screening of baggage, packages, and parcels which enter facilities.

— (U) Have law enforcement agencies and security personnel review surveillance detection and countersurveillance procedures to enhance awareness of possible attack planning.

— (U) Establish and rehearse evacuation protocols for homicide or suicide bombing threats (for example, fire drills, code words) and identify and pre-designate primary and secondary evacuation routes and assembly areas.

— (U) Identify potential sources of bomb-making materials and precursor components for explosive devices; develop awareness programs to inform point-of-sale employees when and how to alert authorities to suspicious purchases.

— (U) Identify routine shipments and thefts of explosives or bomb-making materials to determine possible sources of IED components and identify potential locations which could be used as staging, assembly, or test sites.

(U) Assessment and Detection Phase

— (U) Conduct random explosives detection canine searches; stagger search times and patterns to implement countersurveillance measures.

— (U) Do not make approaches and negotiations with suspected suicide bombers; approach to suspicious packages should be attempted only by bomb squads by use of remote means.

— (U) Create physical stand-off area at a safe distance from the potential target.

(U) Response Phase

— (U) Evacuate the area surrounding the person that is considered a threat, ensuring that the evacuation site selected is a considerable distance away to avoid blast and fragmentation from surrounding materials or buildings.

— (U) Maintain vigilance of a possible secondary bomber, handler, or device nearby or among the victims of an initial attack. An additional device may be used to target an evacuation site or command post areas used by the response community.

Office of
Intelligence and Analysis

I&A Customer Survey

Product Title:

Product Classification: Select One   Type of Partner: Select One

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

- ☐ Integrated into one of our 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)

2. *Please rank this product's relevance to your mission.*

Critical: ○ Very important: ○ Somewhat important: ○ Not important: ○ N/A: ○

Comment:

3. *How could our product or service be improved to increase its value to your mission?*

Comment:

4. *If this product was supplied in response to a specific request - please rate your satisfaction with each of the following services provided by I&A:*

	Very Satisfied	*Somewhat Satisfied*	*Somewhat Dissatisfied*	*Very Dissatisfied*	*N/A*
(a) Timeliness of Product or Support	○	○	○	○	◉
(b) Communication During Processing of Your Request	○	○	○	○	◉
(c) Responsiveness to Your Questions	○	○	○	○	◉

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

Your Organization:

Your Name/Position:

Your contact # or email:

Submit to IA.feedback@hq.dhs.gov - **Submit Feedback**