Transportation Security Administration

(U) Transportation Suspicious Incidents Report

15 October 2010

Executive Summary

(U//FOUO) The Transportation Suspicious Incident Report (TSIR) provides a weekly comprehensive review of suspicious incident reporting related to transportation. The TSIR includes incident reporting, analyses, images, and graphics on specific incidents. In addition, selected articles focus on security technologies, terrorism, and the persistent challenges of securing the nation's transportation modes. This product is derived from unclassified incident and law enforcement reporting and does not represent fully evaluated intelligence. Questions and comments may be addressed to the Transportation Security Administration, Office of Intelligence, Field Production Team at (703) 601-3142.

Sector Incidents and Trends

Transportation Highlights

Information Bulletins, Notes, and Assessments

Incident Follow-Ups and Closures

Technologies and Tactics

Appendix

Transportation Security Administration

Sector Incidents & Trends

(U) Summary of Suspicious Incidents

(U//FOUO) Field reporting continues to capture incidents or activities in transportation modes that may be construed as suspicious – as defined by the Department of Homeland Security (DHS). For this reporting period, 23 incidents were considered suspicious.

(U//FOUO) The vast majority of suspicious incidents are not terrorism related. Incident reporting continues to reveal most involve members of the traveling public who do not have intent to cause harm. Intoxicated passengers, people traveling without proper identification or with propaganda materials, and persons with mental health needs are generally not considered suspicious and are generally not included in the weekly summary. However, some incidents are more serious and are reported for situational awareness. Incidents involving notable drug or weapons concealment, possible surveillance, laser targeting of aircraft, possible insider collusion, exploitable gaps in security, and some unusual behaviors at transportation venues are discussed as they may involve technologies or tactics which may lend insight to future terrorist tradecraft.

(U) Aviation Incidents

(U//FOUO) New York: Suspicious Incident at John F. Kennedy International Airport. On 29 September, an identified passenger at John F. Kennedy International Airport (JFK) was approached by an individual in the sterile area and asked to carry a locked, black backpack onboard a flight (New York-San Francisco). The unidentified individual stated that he did not have enough money for the flight and offered the passenger money to transport the backpack for him. The passenger refused the request and reported the incident to the airline gate agent. Local Law Enforcement Officers (LEOs) responded and interviewed the passenger who repeated his story and provided a description of the unidentified man. TSA and the airline reviewed closed-circuit television (CCTV) tapes and observed the gate area in an attempt to locate and identify the suspicious individual with no success.

(U//FOUO) According to the Field Intelligence Officer at JFK, further identification of the individual was not possible as his face was not visible on CCTV cameras at the airport. While an investigation into this incident continues, it is not yet known if the individual was a ticketed passenger, or how he entered the sterile area.

(U//FOUO) TSA Office of Intelligence Comment: *In this instance, the solicitation of the passenger was done in the sterile area, suggesting the individual and item in question should have been screened at the passenger screening checkpoint. The investigation continues to determine if this occurred. Transportation security personnel are reminded that there have been incidents in the past where unwitting passengers have been duped into carrying items that were later found to conceal weapons, and in at least one instance, an improvised explosive device (IED). On 21 December 1988, an IED planted in unaccompanied baggage exploded onboard Pan Am 103 over Lockerbie Scotland, killing 259 passengers and*

crew as well as 11 people on the ground. **[Sources: TSA-09-10316-10; TSA Field Intelligence Officer JFK; Open Source Research]**

(U) Surface Incidents

(U//FOUO) United States, Mexico: Drug Traffickers Use Trucking Program to Transport Illicit Cargo. Reporting assessing vulnerabilities of the Customs-Trade Partnership Against Terrorism (C-TPAT) Program highlights drug trafficker use of C-TPAT companies in order to smuggle drugs across the border. The CBP Office of Intelligence and Operations Coordination reported that border seizure statistics do not reveal a pattern suggesting targeted operations.

(U) Customs-Trade Partnership Against Terrorism Overview

(U) C-TPAT offers U.S. and foreign companies shorter wait times and fewer inspections at U.S. ports of entry in exchange for enhanced security measures prior to arriving at the border as well as an on-site review of supply chain security procedures. C-TPAT companies can become Free and Secure Trade (FAST)-certified to use designated FAST lanes that provide these benefits.

(U//FOUO) Drug traffickers also have been known to hijack and clone legitimate commercial trucks to transport illicit cargo across the border. According to a highway cargo trade group, in 2010, criminals hijacked over 10,000 commercial trucks in Mexico.

(U//FOUO) Although DHS Office of Intelligence and Analysis (I&A) lacks evidence that drug trafficking organizations are able to clone FAST-certified trucks, it remains a concern for the private sector. DHS I&A "…believes the possibility that drug traffickers can use FAST-certified trucks remains low based on the numerous requirements for certification." That said, DHS I&A cannot discount the potential threat based on widespread cloning by drug traffickers of other commercial trucks.

(U//FOUO) TSA Office of Intelligence Comment: *Although drug trafficking organizations have used C-TPAT program companies to smuggle illicit cargo, program vulnerabilities may also provide opportunities for terrorist organizations to cross international land borders with less scrutiny.* **[Sources: DHS I&A Monitor, Border Security Volume IV, Number 7, July 2010]**

Transportation Highlights

(U) Homeland Security

(U) Explosives manual notes

(U) Jihadist Posts Handwritten Explosives Manual. On 2 October, a jihadist posted scanned images of a manual that provides instructions on electronics, explosives, and poisons to the Shumukh al-Islam forum. Manual instructions include how to prepare and use various chemical compounds, including ammonium hydroxide, hydrochloric acid, hydrogen peroxide, nitric acid, and sulfuric acid. Other pages contain illustrations of electric circuits, including those from Casio F91-W and Databank digital watches.

(U//FOUO) TSA Office of Intelligence Comment: *The Shumukh Al-Islam Network is a major jihadi forum on which propaganda videos, articles by extremists, and statements by jihadi groups are posted.* **[Sources: SITE; Open Source Research]**

(U) International Security

(U) Department of State Issues Travel Alert for Europe. On 3 October, the U.S. Department of State issued a 'travel alert' advising U.S. citizens living or traveling in Europe to take more precautions regarding their personal security. The alert stated in part: *"Current information suggests that al-Qa'ida and affiliated organizations continue to plan terrorist attacks. European governments have taken action to guard against a terrorist attack and some have spoken publicly about the heightened threat conditions. Terrorists may elect to use a variety of means and weapons and target both official and private interests. U.S. citizens are reminded of the potential for terrorists to attack public transportation systems and other tourist infrastructure. Terrorists have targeted and attacked subway and rail systems, as well as aviation and maritime services."*

(U) U.S. and European authorities believe that terrorists have been dispatched to Europe to conduct 'commando-like' attacks similar to the 2008 terrorist attack in Mumbai, India. According to unconfirmed press reports, among possible terrorist targets are public areas in at least five major European airports. One scenario authorities fear is a repeat of the December 1985 attacks on the Rome and Vienna airports where terrorists affiliated with the Abu Nidal Organization (ANO) threw hand grenades and fired assault rifles at travelers near airline ticket counters, killing 19 and injuring as

many as 140 people. For more information about this threat, please refer to the DHS information bulletin on page 7. **[Sources: OSAC; Press]**

(U) Bermuda: Security Breach at L.F. Wade International Airport. On 1 October, an unemployed aircraft mechanic reportedly admitted to breaching airport security and gaining unauthorized access to a passenger aircraft during the early morning hours of 28 September, at L.F. Wade International Airport (BDA). The individual, who had previously worked at the airport as a mechanic, used a ladder to get into the aircraft as it sat on the tarmac. Security officers at the airport spotted the ladder and confronted him as he exited the plane. He reportedly told local police that he climbed onboard the aircraft to look at instruments in the cockpit, but was not able to gain access because the door to the flight deck was locked. The former mechanic pleaded guilty.

(U) The individual holds the following FAA ratings and certificates: Private Pilot – Single Engine Land; Instrument Airplane; and Mechanic – Airframe and Powerplant.

(U//FOUO) TSA Office of Intelligence Comment: *While no terrorism nexus was established in this incident, the relative ease in which the individual was able to gain access to the air operations area and the aircraft is of concern. Individuals who are able to gain unauthorized access to a passenger aircraft could sabotage or vandalize avionics equipment, leave behind (conceal) a weapon or IED, or possibly attempt to stowaway in the passenger cabin, cargo hold, or wheel well.* **[Sources: Press; Open Source Research]**

(U//FOUO) India: Fraudulent E-Ticket Use Raise Security Concerns. According to open source reporting, there have been at least nine incidents involving the use of fraudulent E-tickets at Indian airports in the past year. Of these nine incidents, five took place at Delhi, two at Mumbai, and two at Calicut. Security officials judge that the number of individuals using fraudulent E-tickets may be higher.

(U//FOUO) TSA Office of Intelligence Comment: *According to a 20 July Intelligence Bulletin, the FBI assessed that the ability to print E-tickets from a personal computer prior to arriving at an airport could be exploited by terrorists or criminals wishing to keep their travel undetected. According to a reliable FBI source with excellent access, E-tickets printed from home can be duplicated and altered to allow travelers to conceal their identity. According to the FBI, individuals using this method of identity concealment could hinder law enforcement and intelligence efforts to identify, investigate, and disrupt criminal or terrorist activities in the United States and overseas. Terrorists could also use fraudulent E-tickets to circumvent watch listing and board commercial passenger aircraft.* **[Sources: Open Source Center SAP20101001535002; FBI Intelligence Bulletin, *Memphis Division, Loophole in the Airline Security System Could Lead to Undetected Travel by Terrorists or Criminals*, 20 July 2010]**

Info Bulletins, Notes and Assessments

(U) Information Bulletins, Notes, and Assessments

(U//FOUO) DHS Information Bulletin: Al-Qa'ida Threat to Europe. On 3 October, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) published a Joint Intelligence Bulletin in response to the heightened threat environment in Europe, as well as actions European governments have taken to increase surveillance and to guard against potential terrorist attacks. At this time, there is no indication that the reported threat is directed specifically toward the United States, its citizens, or infrastructure; however, DHS assesses that al-Qa'ida and its affiliates continue to plot against the Homeland and U.S. allies.

(U//FOUO) Previous al-Qa'ida terrorist plots, such as the organization's effort in August 2006 to bring down multiple transatlantic commercial airliners using liquid explosives, were initially assessed to be a Europe-focused attack. It was not until later in the investigation that it was revealed that the plot involved U.S. commercial aviation. In 2009 and 2010, investigators discovered previously unknown links between al-Qa'ida external operational planners and U.S. citizens inside the United States, including Najibullah Zazi (USPER), David Coleman Headley (USPER), and Raja Khan (USPER). Based on these instances, DHS continues to operate under the premise that al-Qa'ida and like-minded terrorist groups are determined to recruit and place terrorist operatives inside the United States and that attacks could occur with little or no warning.

(U//FOUO) In recent years, Europe has been the target of a variety of attacks by al-Qa'ida and other extremist groups. Many of these attacks focused on the general public, not military installations or government institutions. DHS assesses that the scale and complexity of an attack are dependent upon a variety of factors, to include the sophistication and training of the attackers, the parameters of their targets, and the local security environment.

- **(U//FOUO)** June 2007: Two men crashed a vehicle loaded with compressed gas cylinders into the doors of Glasgow International Airport's main terminal, setting fire to the entrance.

- **(U//FOUO)** July 2005: British authorities reported four suicide bomb blasts during the morning rush hour. Three of the attacks were within London's underground train system and the fourth attack occurred on a city bus, killing 52 people and injuring approximately 700.

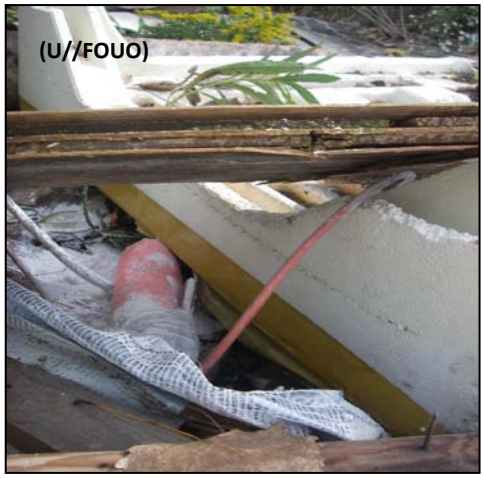
- **(U//FOUO)** March 2004: 10 bombs hidden in sports bags exploded on four commuter trains during the morning rush hour in Madrid, Spain, killing 191 people and wounding approximately 1,700. A Europe-based group claiming affiliation with al-Qa'ida claimed credit for the attack. **[Source: DHS]**

Info Bulletins, Notes and Assessments

(U//FOUO) TSA Office of Intelligence: Terrorist Attack Methods in Airport Terminals (Re-Issue). This assessment, which was originally published on 15 July 2009 and re-issued on 7 October, was developed at the request of the TSA Office of Security Technology to look at possible terrorist tactics that could be used inside the public areas of an airport terminal. This assessment was created to assist in the development of security procedures and the deployment of threat detection technology to this area. It reviewed a number of unclassified sources detailing disrupted plots, bombings, suicide bombers, and armed assaults conducted in the public areas of airports from the 1960s to the present. Additionally, attacks on other critical infrastructure targets were reviewed in order to assess which tactics are more likely to be considered by terrorists targeting airport terminals. **[Source: TSA]**

Incident Follow-Ups & Closures

(U) Follow-Ups and Closures



(U//FOUO) Explosive device found in Chicago

(U//FOUO) Illinois: Explosive Device Reportedly Found near CSX Rail Line. **Background:** On 4 October, an explosive device was discovered "near" the CSX Rail Line in Chicago, Illinois, in piles of garbage. Local LEOs responded and, after the K-9 team alerted on the explosive, established a two-block perimeter and evacuated the surrounding buildings. The Bomb and Arson Team confirmed that the "salami-shaped" item contained 2-4 pounds of what appeared to be a commercial-grade explosive device that was set and ready to explode. The Bomb and Arson Team disrupted the device.

***(U//FOUO) Follow-Up and Closure**: According to the TSA Field Intelligence Officer assigned to Chicago (ORD), the device was discovered by workers cleaning up a wooded area near the rail line. The device was not located on railroad property. The explosive device was described as a 'slurry sausage,' (also known as a water gel and is orange in color)—an explosive material containing substantial portions of water, oxidizers, and fuel, and is rigged with a non-electric blasting cap. Speculation is that a construction company or employee dumped their site trash at this location instead of paying a fee for the city dump. There was no terrorism nexus for this incident.* **[Sources: TSOC Surface Desk; TSA Field Intelligence Officer ORD]**

Transportation Security Administration

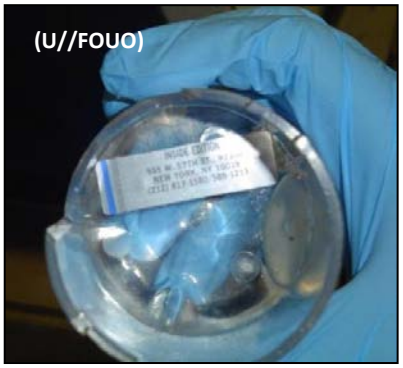
Technologies & Tactics

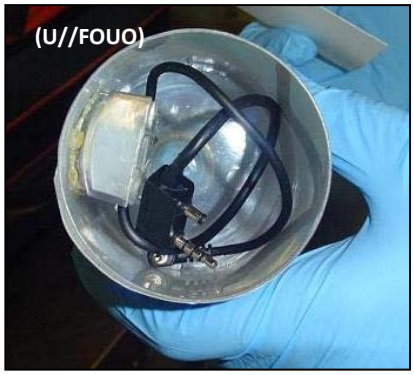
(U) Suspicious Objects, Weapons, & Concealment Methods

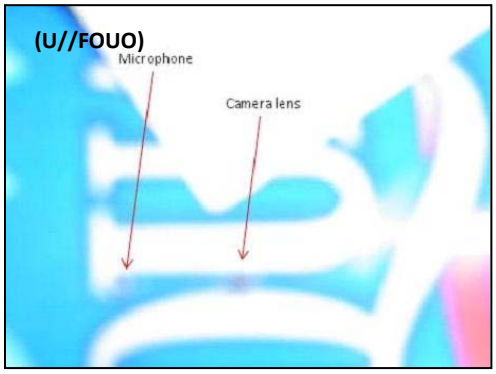
(U//FOUO) Camera in water bottle - LGA

(U//FOUO) New York: Modified Water Bottle Encountered at LaGuardia; Possible Test of Security. On 4 October, TSA Transportation Security Officers (TSOs) at LaGuardia International Airport (LGA) detected a water bottle with a hidden compartment containing a camera, in the carry-on bag of an identified passenger. TSOs detected the suspicious item while conducting an open bag search for liquids. The bottle, which also contained an unidentified liquid, had a false bottom where the camera had been concealed. The passenger and his traveling companion stated they worked as investigative reporters for a news program. The passengers elected not to fly and left the airport.

(U//FOUO) In March 2009, TSA TSOs at St. Louis International Airport (STL) encountered a suspicious water bottle in the checked bag of an identified passenger. The bottle contained wires, a power source, and unidentifed electronics. TSA interviewed the passenger who stated he was a 'special projects photographer' for a news program, and identified the item in the bottle as a camera with a microphone. The passenger also advised that he had two other non-operating cameras in his bag, and that he was not engaged in a test of airport security at STL. The bag had numerous audio/video cables and assorted chargers, but no prohibited items.







(U//FOUO) Suspicious water bottle - STL

(U//FOUO) TSA Office of Intelligence Comment: *The concealment incident at LGA is unusual because it involves a camera. TSOs regularly encounter passengers who hide items in a "diversion safe," such as a bottle or book. This method is also linked to the concealment of drugs and drug paraphernalia. These bottles could also be used to conceal small weapons, explosive mixtures, or IED components. Variations of these bottles are sold on the Internet under different*

Technologies & Tactics

brand names (e.g. soft drink or bottled water labels). While the bottles may appear to be empty (no visible liquid), the hidden compartment could still contain contraband or prohibited items, or as noted in the above incidents, surveillance-related equipment. **[Sources: TSA-10-10547-10; TSA Field Intelligence Officer CLE; BAO Team STL; Open Source Research]**

(U//FOUO) Suspicious item detected at Manchester Airport

(U//FOUO) United Kingdom: Suspicious Item Detected at Manchester Airport (MAN). On 3 October, an identified passenger (MAN-CDG) presented her carry-on luggage for X-ray examination at a security screening point at Manchester Airport. During X-ray screening, the operator identified a suspicious item inside the bag and referred the bag for additional screening and a hand search. A subsequent interview of the passenger determined the item to be a 'prototype electronic sensor' which was being carried on behalf of the passenger's company. The passenger was allowed to continue travel; however, the sensor was not allowed into the restricted area or onboard the plane. **[Source: UK Department of Transport - TRANSEC Threats Office]**

(U//FOUO) Concealment Method: External Body Packing

(U//FOUO) New York: Cocaine Taped to Passenger's Legs. On 16 September, Customs and Border Protection (CBP) officers at John F. Kennedy International Airport (JFK) selected an identified passenger arriving on a flight from the Dominican Republic for an inbound enforcement examination. During the pat down search, the officers detected packages taped to the passenger's legs. The packages were later determined to contain cocaine (5.58 pounds). The passenger was turned over to Immigration and Customs Enforcement (ICE).

(U//FOUO) Cocaine taped to legs - JFK

Transportation Security Administration

Technologies & Tactics

(U//FOUO) New York: Heroin Concealed on Legs, Stomach, and Back. On 20 September, CBP officers at JFK selected an identified passenger arriving on a flight from Ecuador for an inbound enforcement examination. During the pat down search, the officers detected packages on the passenger's stomach, back, and both of his legs. A total of 10 packages were removed from the passenger's body, which field tested positive for heroin (13.68 pounds). The passenger was turned over to ICE for federal prosecution.

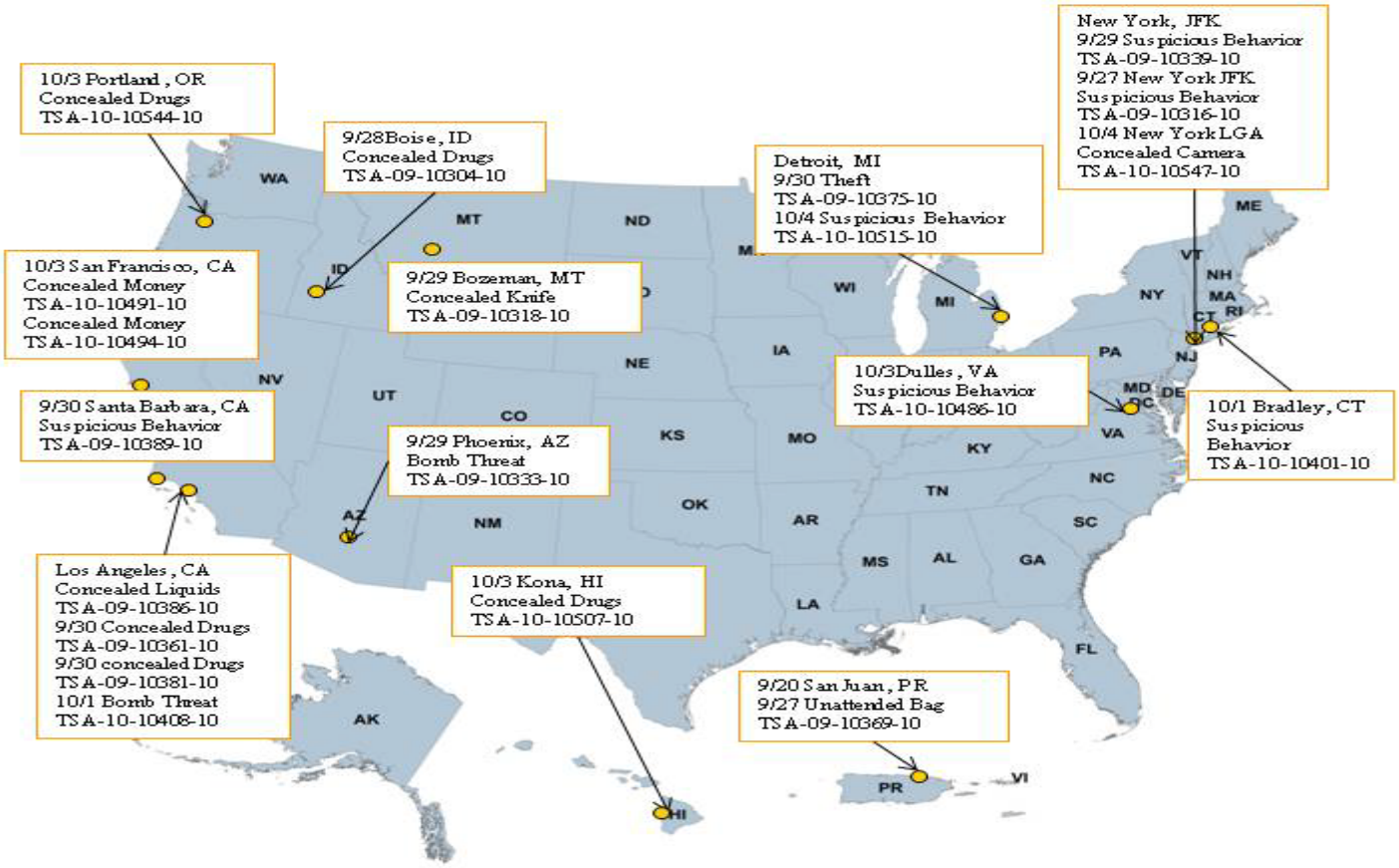
(U//FOUO) Heroin taped to stomach, back, and legs - JFK

(U//FOUO) TSA Office of Intelligence Comment: *Concealing narcotics, bulk cash, and other contraband underneath clothing (external body packing or carrying) is a fairly common smuggling tactic that has also been adapted for use by terrorists. The Liberation Tigers of Tamil Eelam (LTTE) successfully employed this method in multiple suicide attacks in Sri Lanka and India, as did Chechen guerillas and terrorist groups in the Levant in the August 2004 bombings of two Russian passenger aircraft. More recently, in December 2009, al-Qa'ida in the Arabian Peninsula used external body packing in the attempted in-flight bombing of Northwest Airlines Flight 253. The bomber concealed the device, which malfunctioned, in his underwear in order to evade security screening.* **[Sources: CBP; Open Source Research]**

Tracked by: HSEC-02-03001-ST-2009; HSEC-02-03003-ST-2009; HSEC-01-00000-ST-2009; HSEC-01-02000-ST-2009; HSEC-02-00000-ST-2009, HSEC-03-00000-ST-2009

Appendix

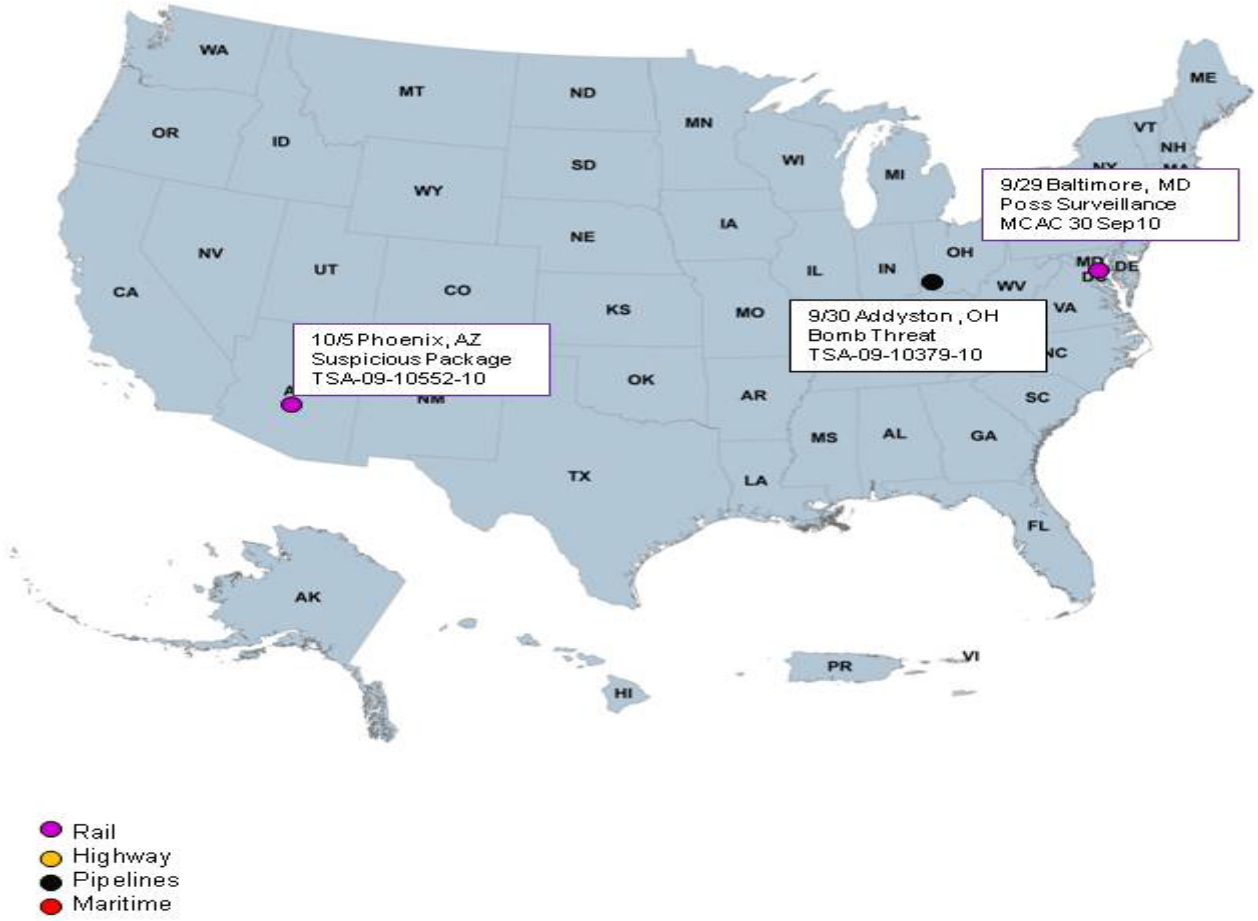
(U) Aviation Incidents 29 September – 5 October 2010



(U//FOUO) For additional information about any of the above reference incidents, please contact your regional Field Intelligence Officer.

Appendix

(U) Surface Incidents 29 September – 5 October 2010



(U//FOUO) For additional information about any of the above reference incidents, please contact your regional Field Intelligence Officer.

Transportation Security Administration

Appendix

Suspicious Incident Reports Selection Standards Extracted from: DHS Information Sharing Environment (ISE), Functional Standard (FS), Suspicious Activity Reporting (SAR), version 1.5 (ISE-FS-200), Part B – ISE-SAR Criteria Guidance	
CATEGORY	**DESCRIPTION**
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems, or functions.