JOINT REGIONAL INTELLIGENCE CENTER

Intelligence Assessment

(U) Guardian Incident Review: August 2009

30 September 2009

LAW ENFORCEMENT SENSITIVE: This information is the property of the Los Angeles Joint Regional Intelligence Center (JRIC) and may be distributed to state, tribal, or local government law enforcement officials with a need-to-know. Further distribution without JRIC authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

INTELLIGENCE ASSESSMENT **30 September 2009**

(U) Guardian Incident Review: August 2009

(U) Summary of Findings

- (U//FOUO//LES) The number of Guardian incidents reported in August 2009 totaled 109.
- (U//FOUO//LES) Four "high-interest" incidents were reported, including one instance of possible sabotage targeting rail assets, and one improvised explosive device placed in a residential mailbox. Fifty-five "moderate interest" incidents were reported, including nineteen threats to use explosives, and ten threats to cause injury or death.
- (U//FOUO//LES) Incidents involving suspicious photography or suspicious vehicles continued to dominate reporting.
- (U//FOUO//LES) The transportation sector reported the highest number of incidents, many involving aviation assets.
- (U//FOUO//LES) Private citizens, private/corporate security officers, and municipal law enforcement personnel submitted the greatest number of suspicious incident reports.

(U) Scope

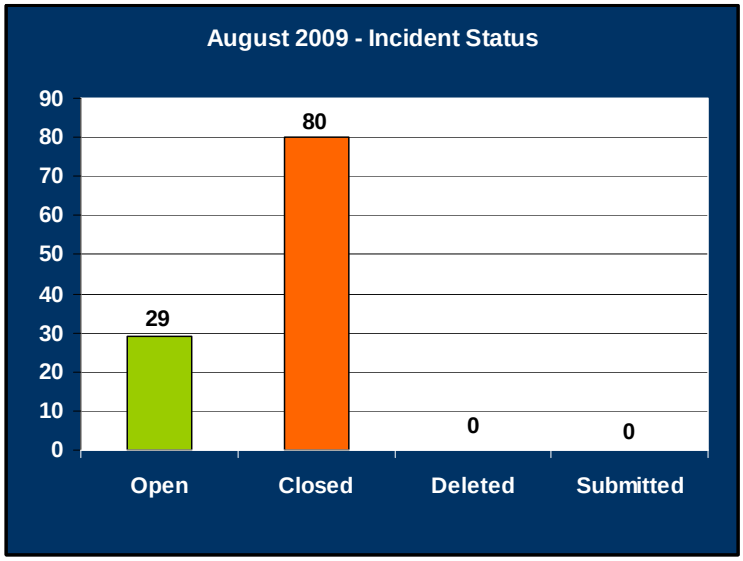
(U//FOUO//LES) The Joint Regional Intelligence Center (JRIC) conducted a statistical review of 109 incidents referred to, received by, created by, or assigned to the FBI Los Angeles Field Office (LAFO) between 1 August 2009 and 31 August 2009 and tracked in the FBI's Guardian database.[i] Duplicate incidents were discarded prior to analysis.

[i] (U//FOUO//LES) The Guardian database is populated several ways. Leads may come directly to the FBI for entry by FBI personnel. They may come from e-Guardian – an unclassified, law enforcement sensitive reporting portal available to vetted account holders at the Law Enforcement Online (LEO) Web site – for later transfer into Guardian. Or they may come first to the JRIC via online lead sheets, by facsimile, or by phone for selective entry into e-Guardian. The FBI's Threat Squad assesses and investigates all Guardian leads. Based upon their findings, incidents are closed, transferred to another agency for follow-up, or referred internally for additional investigation.

(U) Status and Disposition of August 2009 Guardian Incidents

(U//FOUO//LES) As of 22 September 2009, nearly three quarters of the incidents reported in August (80 of 109) had been investigated by the LAFO Threat Squad and closed. Twenty-nine remained open (representing 26 percent).

(U//FOUO//LES) Fifty-two of the 109 incidents were found to have no nexus to terrorism; twenty-eight were deemed inconclusive. One incident had an identifiable nexus to terrorism. Nine incidents involved Terrorist Screening Center (TSC) hits. Six incidents were referred for follow-up: four to the FBI counter-terrorism unit; and one each to units dealing with criminal activity and possible misuse of chemical/biological/radiological/nuclear (CBRN) materials.



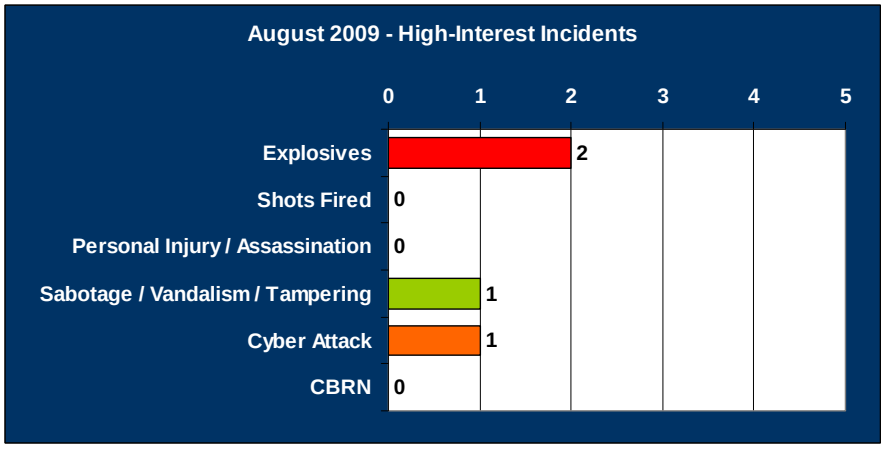
(U//FOUO//LES) Status of Incidents as of 22 September 2009.

(U) Overview: Incidents by Activity Type

(U//FOUO//LES) All incidents were manually examined to determine the full scope of activities reported. Many incidents involved more than one activity type; for this reason, activity type totals presented in charts and graphs may occasionally exceed 109.

(U//FOUO) High-Interest Incidents

(U//FOUO//LES) Incidents involving activities in which there was potential for loss of life, injury, or significant property damage were deemed "high-interest." Four such incidents were recorded in August 2009. An improvised explosive device was left in a mailbox at one residence; a vehicle exploded in the garage of another residence while repair work was being conducted. One instance of sabotage was reported by the rail sector. The remaining incident involved a cyber attack against a business for the purposes of theft.

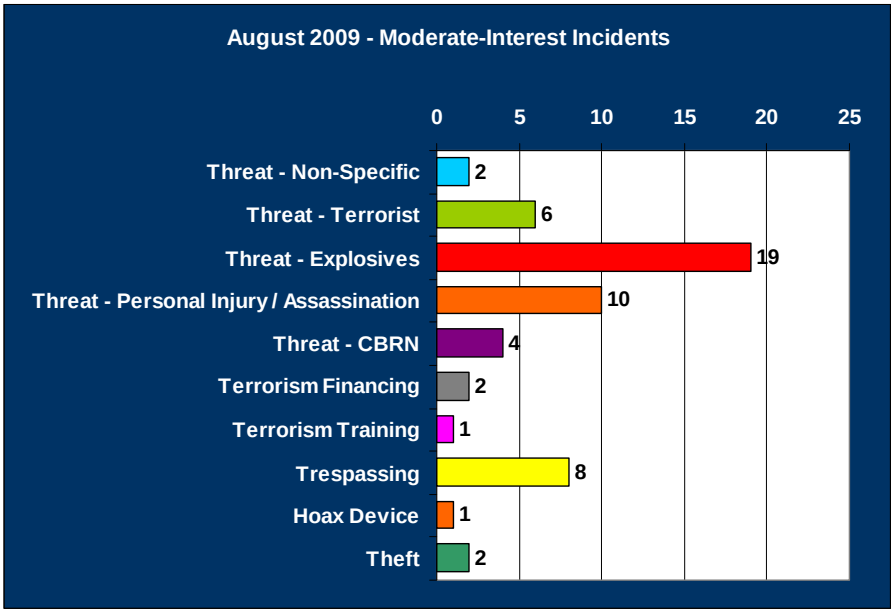


(U//FOUO//LES) None of the "high-interest" incidents reported in August 2009 caused significant injury.

(U//FOUO) Moderate-Interest Incidents

(U//FOUO//LES) Incidents involving threatening statements or behaviors, potential terrorist fundraising or training, use of hoax devices, trespassing, or theft were deemed "moderate-interest." Fifty-five such incidents were reported in August 2009.

(U//FOUO//LES) Nineteen bomb threats were recorded against varied targets: resorts and casinos (four); hotels (two); defense assets (two); border/immigration processes (two); private residences (two); and one each at business, banking, aviation, government, public health, and retail facilities. One threat did not specify a target.



(U//FOUO//LES) In August 2009, bomb threats outpaced all other reported "moderate interest" incidents.

(U//FOUO//LES) Ten threats of personal injury were reported in August 2009, directed at personnel associated with educational (five) and government (two) facilities; military assets, a casino, and a foreign government facility each reported one incident. Eight trespassing incidents took place, two incidents each at nuclear, energy, and defense facilities, and one incident apiece at port and educational facilities. Six threats mentioned potential terrorist activity; five of these centered on hotels, casinos, and military assets, while one reported a possible visa violation.

(U//FOUO) Other Suspicious Incidents

(U//FOUO//LES) By far, the most commonly-reported activities in August 2009 involved suspicious vehicles (27 incidents) and suspicious photography (22 incidents).[ii]

(U//FOUO//LES) Six of the suspicious vehicle incidents took place on roads or highways. An additional nine took place at or near assets from the aviation (three), energy (two), government (two), and defense (two) sectors. Personnel from the emergency services sector, defense industrial base, a hotel, and a dam each reported one incident. Four incidents were recorded involving businesses (two), and residences (two). Four of the suspicious vehicle incidents did not involve a critical infrastructure sector.

[ii] Generalized "suspicious behavior" reports declined significantly (from 51 in July 2009 to eight in August 2009) because the JRIC, seeking to disambiguate this category, this month introduced an expanded, more precise set of activity/behavior descriptions. This allowed JRIC analysts to reclassify many incidents that would previously have fallen under this generalized heading.

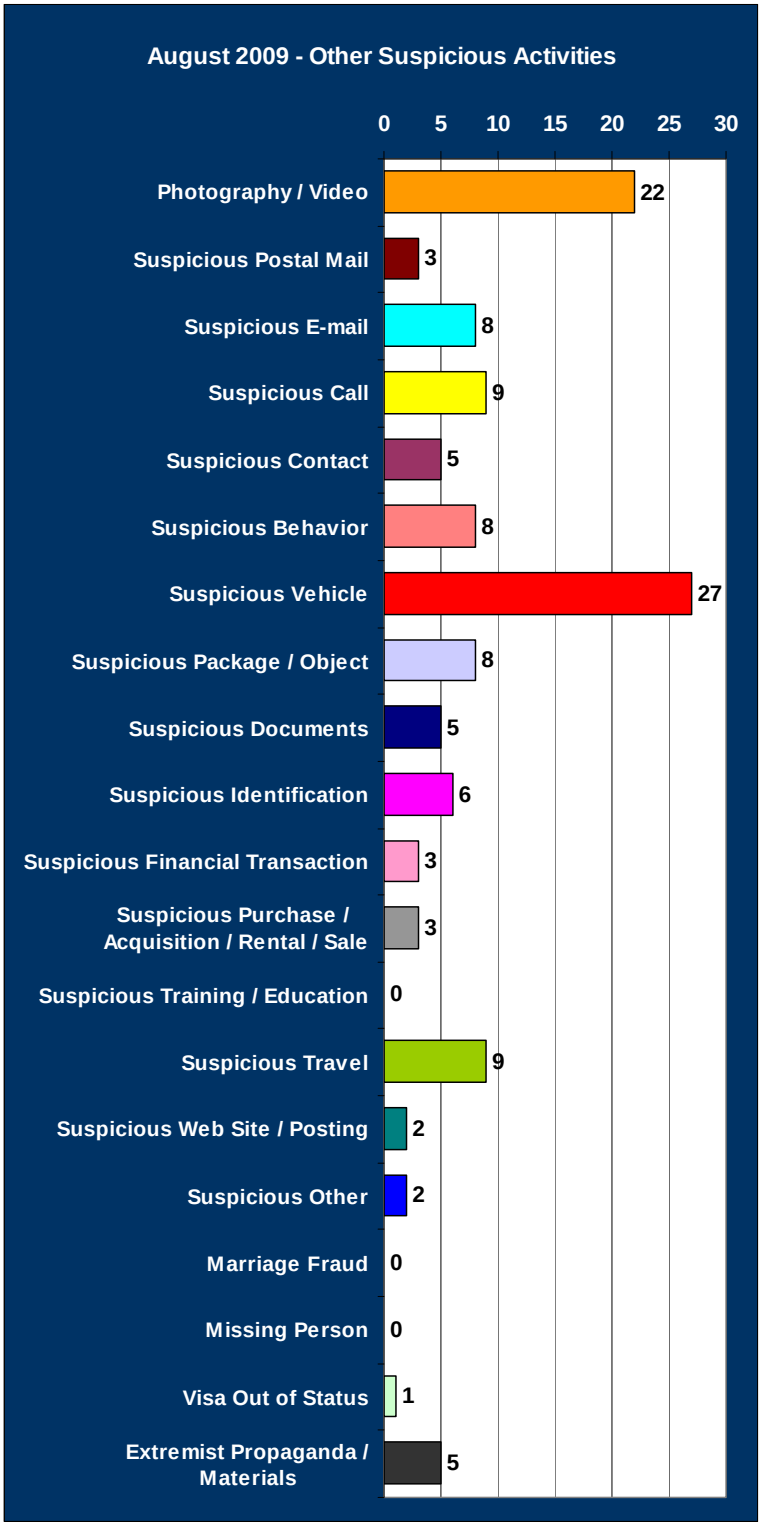
(U//FOUO//LES) Of the 22 suspicious photography incidents, five took place at or near energy sector facilities. Two incidents were reported by motorists on highways; two more were reported by businesses. Personnel from the transportation sector reported three incidents, one each at/near rail, port, and aviation assets. Security personnel at dam and water treatment sites each reported a single incident, as did personnel from the emergency services sector, a hotel, a casino, and government and public health facilities. Three incidents did not identify a sector.

(U) Overview: Incidents by Sector

(U//FOUO//LES) All incidents were manually examined to determine if they involved an identifiable critical infrastructure (CI) sector.[iii] Twenty incidents (or 18 percent) had no such connection.

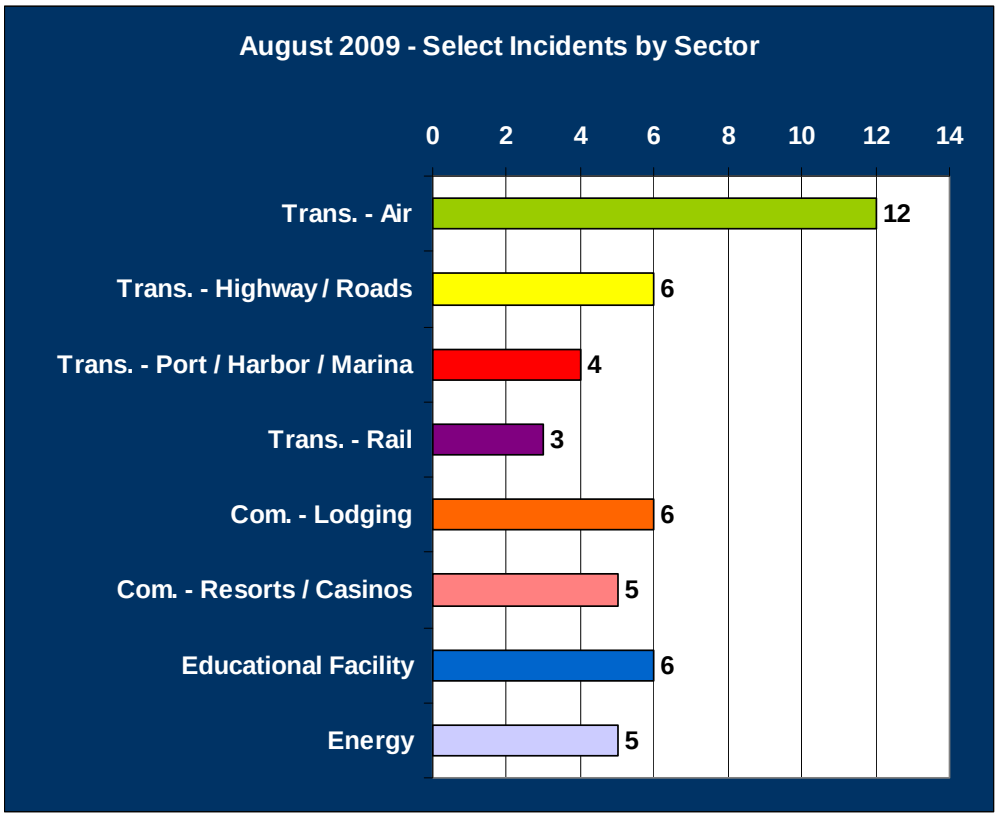
(U//FOUO) Transportation Sector

(U//FOUO//LES) A total of 25 incidents were reported by personnel from the transportation sector. Many of these (12 of 25, or 48 percent) involved the aviation industry, which reported suspicious travel, identification, and packages. An instance of possible sabotage was reported by rail personnel, who noted the removal of pandrol clips from the tracks at a Metrolink station. Port personnel reported one instance of trespassing and one possible security breach. Several incidents stemmed from routine traffic stops conducted by law enforcement personnel of suspicious vehicles. Suspicious photography of roads, highways, or bridges, and suspicious packages left at or near transportation facilities were also reported.



(U//FOUO//LES) Incidents involving suspicious vehicles or suspicious photography dominated August 2009 reporting.

[iii] (U//FOUO) A brief description of each CI sector appears in Appendix A.



(U//FOUO//LES) The transportation sector continued to receive a high volume of reports in August 2009. The education sector received a high number of false 9-1-1 reports.

(U//FOUO// LES) JRIC Note: The high volume of reports emanating from the transportation and energy sectors should *not* be taken as an indicator that these facilities are being targeted at a higher rate than facilities in other CI sectors. Security personnel in both the transportation and energy sectors in the JRIC area of responsibility have historically been more proactive and responsive than the other CI sectors with regard to reporting suspicious activities.

(U//FOUO) Additional Critical Infrastructure Sectors

(U//FOUO//LES) Personnel from defense, military, and government assets/facilities reported a total of thirteen incidents. Most of these involved threats: possible terrorist activity; possible use of explosives; and personal injury. Several sectors reported possible attempts to test or breach security protocols. Together, the hotel and resort/casino sectors reported eleven incidents, including personal injury and bomb threats.

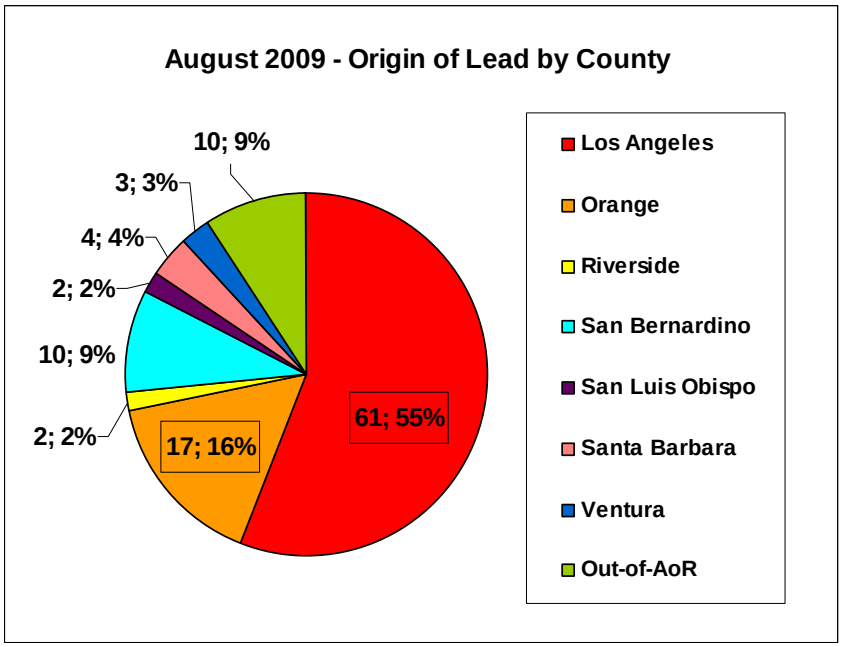
(U//FOUO) Non-Critical Assets

(U//FOUO//LES) Twenty-two incidents were reported by individuals from facilities or assets that fall outside defined critical infrastructure sectors,[iv] including businesses (seven), private residences (six), and three unidentified properties.

(U//FOUO//LES) Six educational facilities reported incidents. Of these, five involved bogus 9-1-1 calls concerning a "cutting" or "shots fired" at Jewish boys' and girls' schools in the city of Los Angeles. None of the incidents proved legitimate, and in a few instances, the facilities were actually closed for summer break. At around the same time, law enforcement personnel reported a rash of similar hoax calls, some of which may have originated from Washington DC and Maryland.[v]

(U) Overview: Source of Reports

(U//FOUO//LES) Three sources comprise the bulk of incidents reported during August 2009: private citizens (29 of 109, or 26 percent); private or corporate security employees (25 of 109, or 23 percent); and municipal law enforcement agencies (23 of 109, or 21 percent). Thirty-two additional incidents were reported by a variety of defense, federal, state, county, municipal, and local sources.



(U//FOUO//LES) Los Angeles and Orange counties continue to receive the most reports. Incidents reported by San Bernardino increased in significantly August 2009.

[iv] (U//FOUO) A brief description of each CI sector appears in Appendix A.

[v] (U//FOUO) These calls appear to be a variation of an activity known as "swatting". The US Department of Justice defines swatting as "falsely reporting an emergency to a police department to cause a Special Weapons and Tactics (SWAT) response to a physical address, or making a false report to elicit an emergency response by other first responders, such as adult protective services, to a specific physical address." For additional information, refer to the May 2008 JRIC Intelligence Bulletin *Swatting: Internet Hoax Diversion of Police SWAT Resources.*

(U//FOUO//LES) The greatest number of incidents were reported by sources within Los Angeles County (61 of 109, or 56 percent), followed by Orange County (17 of 109, or 16 percent). Twenty-one additional incidents were reported by San Bernardino, Santa Barbara, Ventura, Riverside and San Luis Obispo counties. Ten incidents were received from sources outside the LAFO area of responsibility.

(U) Los Angeles County

(U//FOUO//LES) Many incidents reported in Los Angeles County in August 2009 involved suspicious vehicles (18 of 61) or photography (16 of 61); suspicious travel and identification were also reported. Threat content centered on possible use of explosives or personal injury; targets of the latter included current and former Presidents of the United States (POTUS) Barack Obama and George W. Bush. Los Angeles County reported four TSC encounters in August 2009. Five "swatting" incidents were reported, part of a larger series of hoax 9-1-1 calls made to various law enforcement and public safety agencies in the county. (See page 6 for further discussion.)

(U//FOUO//LES) Ten incidents reported by Los Angeles County had no identifiable connection to critical infrastructure. Aviation, energy, educational facilities, and hotels were the predominant focus of CI-specific incidents.

(U) Orange County

(U//FOUO//LES) As with Los Angeles County, a substantial number of incidents reported in Orange County in August 2009 involved suspicious photography (16 of 17). Six threats to use explosives were recorded. An improvised explosive device was left in the mailbox of a retired municipal law enforcement agent; the device did not detonate. Suspicious vehicles and calls were also frequently recorded. Orange County reported two TSC encounters in August 2009.

(U//FOUO//LES) Three Orange County incidents had no identifiable connection to critical infrastructure. Defense and military assets were the prime focus of CI-specific reports in August 2009.

(U) San Bernardino County

(U//FOUO//LES) San Bernardino County reported ten incidents in August 2009, up from four in July 2009. Significant incidents included threatened use of explosives and a threat of personal injury. No TSC encounters were reported. Transportation assets were the focus of most critical infrastructure reporting; businesses and residences were among the top-ranking non-critical assets.

(U) Santa Barbara County

(U//FOUO//LES) Santa Barbara County reported four incidents in August 2009. All significant incidents involved e-mail, telephonic or written threats, including potential terrorist activity, use of explosives, and a possible chemical/biological incident (CBRN). The latter concerned employees who found a note with white powder in a public drop box; the substance was later deemed harmless. No TSC encounters were reported in Santa Barbara County in August 2009.

(U) Ventura County

(U//FOUO//LES) Ventura County reported three incidents in August 2009: a suspicious attempt to purchase airline tickets; a suspicious vehicle near a Coast Guard facility; and suspicious activity in the port area. No TSC encounters were reported.

(U) Riverside and San Luis Obispo Counties

(U//FOUO//LES) Riverside and San Luis Obispo Counties each reported two incidents in August 2009. Notably, Riverside County reported a bomb threat against a hotel; San Luis Obispo County reported trespassers near a nuclear energy facility. Neither county reported any TSC encounters.

(U) Other Sources

(U//FOUO//LES) Sources outside the JRIC area of responsibility reported ten incidents in August 2009, the same number reported in July 2009. Significant activity included a bomb threat against a Texas hospital that had connections within the JRIC region, and several instances of suspicious travel reported by the aviation, rail, and road/highway sectors. Three TSC encounters were reported.

(U//FOUO) Weekly Averages

(U//FOUO//LES) Activity averaged 21 incidents per week, peaking in the first week, when 34 incidents were reported. This was a change from July 2009, when the activity at the beginning of the month was slow. Activity was also high in the second and fourth weeks, when 26 incidents were reported each week. The end of the month was slow, with only two incidents reported in the fifth week.

(U) Concluding Remarks

(U//FOUO//LES) Together, the June, July, and August 2009 Incident Reviews will form a baseline from which to develop later reports; future monthly data sets will allow for trend and pattern analysis.

(U) Appendix A – Critical Infrastructure Categories

(U) The categories used to expand upon and clarify references to critical infrastructure (CI) within incident narratives were derived from a Department of Homeland Security (DHS) list found on the DHS Web site at http://www.dhs.gov/files/programs/gc_1189168948944.shtm and categories native to the FBI Guardian threat tracking system and the JRIC suspicious reporting incident database Memex.

(U) None/Unidentified – The incident had no nexus to CI, or there was not enough information in the incident narrative to assign it to a CI sector.

(U) Agriculture – Businesses or facilities connected to the growth, simple processing, and packaging of food crops and other crops used to feed, clothe, or fuel.

(U) Banking/Finance – Primarily owned and operated by the private sector. Includes, but is not limited to, depository financial institutions (banks, thrifts, and credit unions,) insurers, securities brokers/dealers, investment companies, and certain financial utilities.

(U) Borders/Immigration – Agencies, institutions, businesses or facilities that patrol, enforce, coordinate, monitor, or facilitate movement of individuals across US international borders.

(U) Chemical/Hazardous Materials – Divided into five segments, includes businesses and facilities that produce basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products.

(U) Commercial Facilities – Businesses and facilities that operate on the principal of open public access. The JRIC separately evaluated eight sub-sectors identified by DHS, plus two legacy categories from Guardian:

- (U) Entertainment/Media – motion picture studios, broadcast media, and others
- (U) Food / Beverage Manufacturing – commercial kitchens, breweries, and others
- (U) Lodging – hotels, motels, conference centers
- (U) Outdoor Events – theme and amusement parks, fairs, campgrounds, parades, and others
- (U) Public Assembly – arenas, stadiums, aquariums, zoos, museums, convention centers, and others
- (U) Real Estate – office/apartment buildings, condominiums, mixed-use facilities, self-storage
- (U) Resorts/Casinos – commercial establishments or locations that attempt to provide a variety of entertainment/relaxation activities in a self-contained environment.

- (U) Restaurant – also includes nightclubs, food carts, and others
- (U) Retail Establishment – retail centers and districts, shopping malls, and others
- (U) Sports Leagues – professional sports leagues and federations

(U) Critical Manufacturing – businesses and facilities that design, produce, or distribute products or machines that are essential in varying capacities to other CI sectors. Critical manufacturing is divided by DHS into nine sub-sectors; the JRIC did not evaluate these sub-sectors independently.

- (U) Primary metal manufacturing
  - Iron and steel mills, and ferro-alloy manufacturing
  - Alumina and aluminum production and processing
  - Nonferrous metal (except aluminum) production and processing
- (U) Machinery manufacturing
  - Engine, turbine, and power transmission equipment manufacturing
- (U) Electrical equipment, appliance, and component manufacturing
  - Electrical equipment manufacturing
- (U) Transportation equipment manufacturing
  - Motor vehicle manufacturing
  - Aerospace product and parts manufacturing
  - Railroad rolling stock manufacturing
  - Other transportation equipment manufacturing

(U) Dams – comprises the assets, systems, networks, and functions related to dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, or similar water retention and/or control facilities that bear upon hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.

(U) Defense/Military Facilities – includes but is not limited to bases, testing ranges, harbor facilities, docks, and off-base offices and facilities such as recruitment and induction centers.

(U) Defense Industrial Base – includes Department of Defense, government and private sector businesses, facilities, or consortiums that research, design, develop, produce, deliver, or maintain military weapons systems, subsystems, components, or parts.

(U) Emergency Services – comprised of federal, state, local, tribal and private agencies, businesses, facilities, or other groups who provide emergency management, emergency medical, fire, hazardous material, law enforcement, and search-and-rescue services, as well as bomb squads, tactical operations teams, and special weapons assault teams.

(U) Energy – includes agencies, businesses, facilities, and other groups engaged in the development, creation, maintenance or safeguard of major energy sources, to include electricity, petroleum, and natural gas, as well as pipelines, wind farms, solar arrays, and other non-conventional power generation, capture, storage, and transmission facilities.

(U) Government Facilities – buildings and cyber elements owned or leased by federal, state, territorial, local, or tribal governments, located domestically and overseas. Includes general-use office buildings, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions.

(U) Information and Technology – Virtual and distributed physical hardware, software, and IT systems and services that maintain and reconstitute networks, including the Internet.

(U) Maritime – includes cruise ships, private vessels, and others that carry people; differentiated thereby from maritime transportation systems designed to facilitate the movement of goods.

(U) National Monuments/Icons – Assets listed in the National Register of Historic Places, on National Historic Landmarks list, or that share three common characteristics:

- (U) They are a monument, physical structure, object or geographic site.
- (U) They are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national culture, religious, historical or political significance.
- (U) Their primary purpose is to memorialize or represent some significant aspect of the nation's heritage, tradition, or values, and to serve as points of interest for visitors and educational activities.

(U) Nuclear – Agencies, businesses, and other entities that develop, maintain, support, supply, or otherwise facilitate nuclear power generation. This includes, but is not limited to: nuclear power plants; non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; decommissioning reactors; and the transportation, storage, and disposal of nuclear material and waste.

(U) Postal and Shipping – Differentiated from general cargo by its focus on small- and medium-size packages, includes high-volume processing facilities; local delivery units; collection, acceptance, and retail operations; mail transport vehicles, including vans, trucks, tractor trailers and aircraft; and information and communications networks operated by this sector.

(U) Public Health – Private, local, tribal, territorial, state, regional, and national entities, agencies, businesses, facilities, assets, and equipment used to safeguard public health, and deliver health services to the populace, and others.

(U) Telecommunications – Businesses, agencies, organizations, and others who provide and maintain terrestrial, satellite, and wireless transmission systems for communication.

(U) Transportation - The JRIC separately evaluated five sub-sectors identified by DHS, plus one legacy category from Guardian:

- (U) Aviation – includes aircraft, air traffic control systems, commercial airports, and other airfields, including civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
- (U) Rail – includes locomotives, freight cars, track, switching stations, rail yards, and other assembly/transfer points.
- (U) Highway/Roads – roadways and supporting infrastructure – with the exception of significant bridges and tunnels (see below) – as well as vehicles moving within the system, to include automobiles, buses, motorcycles, and all types of trucks.
- (U) Bridges/Tunnels – major and minor bridges and tunnels that could serve as choke points for traffic and transport were they to be damaged or destroyed.
- (U) Maritime transportation system – to include ports, harbors, marinas, navigable waterways, and intermodal landside connections that allow the various modes of transportation to move goods to, from, and on the water.
- (U) Other – small transport such as bicycles/trails, and others.

(U) Water/Water Treatment Systems – any facility, asset, agency, organization, or business involved in the design, development, maintenance, supply, treatment, transport, or distribution of potable and wastewater supplies, including the cyber systems used to achieve these ends.

(U) Additional Categories

(U) The JRIC also evaluated several categories of non-critical assets that appear frequently in reporting:

(U) Residence – private homes and associated property.

(U) Educational Facility – public, private, chartered, and special-focus preschools, kindergartens, elementary, middle, and high schools, universities, and community colleges, as well as continuing education or adult learning centers.

(U) Community Facility – halls, daycare centers, senior centers, gymnasiums, lodges, and other facilities that provide a venue for organized, small-scale community activities.

(U) Place of Worship – churches, synagogues, mosques, and other sites where religious observations take place. Includes activities and services provided by the religious community on site.