(U//FOUO) Winter 2013: DHS/I&A Analyst Suspicious Activity Reporting (SAR) Topics of Interest

(U//FOUO) DHS/I&A is interested in the following SAR topics, which have been updated based on current issues of national interest. Previous topics remain relevant, and law enforcement, first responders, and other homeland security professionals should continue to submit reports on these issues. Per the SAR Functional Standard, only information validated as reasonably indicative of preoperational planning related to terrorism should be reported as a SAR. I&A is reviewing SAR reports on these topics but would welcome any additional context, ideas or local analysis on these topics and opportunities for joint production. We will discuss key findings and assessments during scheduled HS-SLIC Weekly threat briefs.

(U//FOUO) **Reports of threats to religious or cultural facilities.** Reports of surveillance; verbal or telephonic threats of violence; trespassing; property damage, including vandalism or arson; or tests of security at religious or cultural facilities. [HSEC-8 TERRORIST OPERATIONS: HSEC-8.3.1 General suspicious activities; HSEC-8.4.2.20 Targets of elicitation – Specific sites]

(U//FOUO) **Reports of suspicious activities or incidents associated with state, local, tribal, territorial, or private sector computer networks and Web sites**. Reports of denial of service (DoS) attacks against Web sites; Web page defacement; physical entry resulting in unauthorized access to computer networks or hardware; suspicious e-mails that install malware on the network; data exfiltration, or other unusual network access or activity, where there are indicators that the cyber incident is reasonably indicative of links to terrorism. [HSEC-1 CYBER ATTACKS AND EXPLOITATION: HSEC-1.3 Suspicious activities and behaviors, HSEC-1.10 Incidents]

(U//FOUO) **Reports of suspicious activities or incidents associated with mass gatherings, and special events.** Reporting on observed casing activities; breaches or attempted intrusions at event locations or related venues; suspicious inquiries about security protocols for events or VIPs; testing of security; expressed or implied threats to specific events; incidents of suspicious acquisition of explosive precursor materials; or findings of caches or unusual amounts of weapons or explosives. [HSEC-8 TERRORIST OPERATIONS: HSEC-8.3.1 General suspicious activities; HSEC-8.4.2.21 Targets of elicitation – Special events].

(U//FOUO) **Reports of suspicious activities, queries, theft, sabotage, tampering, or vandalism within the transportation sector—including mass transit, aviation, maritime, ground and surface, rail, and pipeline systems.** Reporting on attempts to elicit information such as unusual questions about routes, capacities, peak travel time, training, and security; suspicious behavior by passengers or employees; testing of security; and expressed or implied threats by individuals or groups towards this sector. Reporting on the theft, loss, or diversion of personnel identification or credentials, uniforms, equipment, or training materials. Reporting on sabotage or loss of knowledge-based materials for maintenance of fleet. [HSEC-8 TERRORIST OPERATIONS: HSEC-8.3.1 General suspicious activities; HSEC-8.4.2.17 Targets of elicitation – Transportation sector]

(U//FOUO) **Reports of efforts to artfully conceal improvised explosive devices in innocuous items, such as satchels, backpacks, suitcases, jars, bottles, cans, shoes, clothing, parcels, or toys.** Reporting on potential security probes by individuals trying to enter secure areas with devices that resemble explosive devices. Reporting on unsolicited or unusual parcels delivered from unfamiliar overseas addresses, noting the identification of the sender and recipient and whether the recipient has reported multiple suspicious parcels in recent weeks or months. Reporting on the use of special materials, such as lead or other dense metals or liquids, to prevent the discovery of illicit goods by technical detection equipment, such as x-ray radiography equipment or chemical detectors. [HSEC-8 TERRORIST OPERATIONS: HSEC-8.3.1 General suspicious activities; HSEC-8.8 Methods, capabilities, and activities of adversaries]

(U//FOUO) Note: In the course of official activities, and to the extent permitted by law, police, fire, EMS, and security personnel are encouraged to report activities of a suspicious nature; however, this information should not be collected solely on First Amendment protected activities or on the basis of any racial, ethnic, religious, or other profile.

(U) Prepared by the Office of Intelligence and Analysis (I&A) Homeland Counterterrorism Division and the I&A Field Analytic Support Taskforce. This product is intended to assist federal, state, local, tribal, and territorial first responders in developing deterrence, prevention, preemption, or response strategies. Coordinated with I&A Cyber Intelligence Analysis Division and Collection and Requirements Division.