ROLL CALL RELEASE

In Collaboration with the ITACG

7 February 2012

(U//FOUO) Suspicious Activity Reporting (SAR): Eliciting Information

(U//FOUO) Terrorists or criminals may attempt to identify critical infrastructure vulnerabilities by eliciting information pertaining to operational and security procedures from security personnel, facility employees, and their associates. Persistent, intrusive, or probing questions about security, operations or other sensitive aspects of a facility by individuals with no apparent need for the information could provide early warning of a potential attack. Notable examples of suspicious elicitation:

— (U//FOUO) May 2011: A gas station attendant asked an employee of a nearby chemical manufacturing plant a series of questions about the types of chemicals produced at the plant, whether any were explosive, and whether employees were allowed to take chemicals home. The attendant also asked if the plant employee worked with chemicals, whether certain chemicals become explosive when combined, and whether the plant was hiring.

(U//FOUO) **Nationwide SAR Initiative (NSI) definition of 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.

— (U//FOUO) February 2011: An individual asked a security officer at a train station about station security practices including shift times and changes for security personnel, the number of guards on duty, location of the security company, and whether security continues after midnight. He also asked if the security officer had a key to the electrical room, contact instructions for security personnel in the event of an emergency, the time most people exit trains, and the purpose of "little black balls" (closed-circuit cameras) mounted at points around the station.

(U) Possible Indicators of Suspicious Elicitation

(U//FOUO) The following activities can indicate efforts to elicit sensitive information for potentially malicious purposes. Depending on the context—time, location, personal behaviors, and other indicators—suspicious inquiries should be reported to appropriate authorities:

— (U//FOUO) Inquiries by individuals with no need for the information about a facility's specific security procedures and personnel, including schedules for shift changes, variations in levels of security activity, entry points, types of locks, or the accreditation required to access the facility.
— (U//FOUO) Questions by individuals lacking proper credentials about policies or procedures that would provide insight into a facility's operations.
— (U//FOUO) Persons without a need to know seeking knowledge about evacuation procedures, response times and routes, and procedures used by emergency response personnel.
— (U//FOUO) Nervous or unusual behaviors by individuals asking probing questions, such as refusing requests for identification and becoming agitated when questions are not answered to their satisfaction.

(U) This report is derived in part from information reported under the NSI. This report is part of a series based on SAR intended to help identify and encourage reporting of activities that, in some cases, could constitute preparations for terrorist attacks.

IA-0079-12

(U) Prepared by the I&A Homeland Counterterrorism Division, the FBI Directorate of Intelligence, and the Interagency Threat Assessment and Coordination Group. This product is intended to assist federal, state, local, tribal, territorial, and private sector first responders in effectively deterring, preventing, preempting, or responding to terrorist attacks against the United States. Coordinated with the I&A Cyber, Infrastructure, and Science Division, Strategic Infrastructure Threat Branch and the National Protection and Programs Directorate Office of Infrastructure Protection.

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL