ROLL CALL RELEASE

In Collaboration with the ITACG

14 September 2012

(U) Suspicious Activity Reporting (SAR): Misrepresentation

(U//FOUO) Terrorists might use disguises, fraudulent or stolen credentials, and cloned or repurposed vehicles to gain access to restricted areas, to blend in with their surroundings when conducting surveillance, or to conceal other activities while planning or executing an attack. Anders Breivik, the gunman who was sentenced to 21 years in prison for the July 2011 attack on the Workers' Youth League summer camp in Norway, wore a police uniform and displayed false identification to gain unauthorized access to the camp. Depending on the target, disguises might be aimed at impersonating law enforcement, emergency services, or officials of an institution who have legitimate access to secured/restricted sites.

(U) Nationwide SAR Initiative (NSI) Definition of Misrepresentation: Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity.

(U) Depiction of firefighter's helmet and law enforcement vehicle.

(U//FOUO) The following SAR incidents from the NSI shared space demonstrate types of behavior terrorists might exhibit during planning or actual attacks. Although none were linked to terrorist activity, we consider the examples relevant for situational awareness and training:

- (U) A security officer at a critical infrastructure site approached two individuals who displayed badges and holstered hand guns and claimed to be "homeland security" personnel conducting an investigation. The individuals refused to identify themselves and directed the officer to stay back. Subsequent investigation revealed the individuals were not authorized homeland security/law enforcement officials.

- (U) A subject, who falsely claimed to be an undercover FBI agent, contacted a security officer at an indoor concert arena in an attempt to obtain security plans for the building. He presented a fake business card that identified him as a special agent with the FBI and was later arrested and charged with impersonating a police officer.

(U) Possible Indicators of Misrepresentation

(U//FOUO) The following activities might indicate attempts at misrepresentation and fraudulent impersonation. Depending on the context—time, location, personal behaviors, and other indicators—suspicious persons who attempt to access restricted areas under disguise or using questionable credentials should be reported to appropriate authorities.

- (U//FOUO) Presentation of outdated, expired, tampered with, or otherwise invalid credentials, including documents displaying photographs that don't match the individual.
- (U//FOUO) Display of uniform without proper identification, or use of partial uniforms and props such as mock weapons to access restricted areas.
- (U//FOUO) Attempt to gain entry by using stolen access cards or special keys.
- (U//FOUO) Attempt to discourage security personnel from requesting proof of identification by evoking authority or displaying intimidating behavior.
- (U//FOUO) Use of one's legitimate credentials to access areas outside his or her scope of responsibilities (insider threat).
- (U//FOUO) Use of cloned emergency vehicles where the identifiers (decals, markings, logos) differ slightly from the official government or industry vehicles.

(U) This report is derived in part from information reported under the NSI. It 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-0195-12

(U) Prepared by the Office of Intelligence and Analysis (I&A) Homeland Counterterrorism Division, the FBI Directorate of Intelligence, the Interagency Threat Assessment and Coordination Group, and the New Jersey Regional Operations Intelligence Center. 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 I&A Cyber, Infrastructure, and Science Division, Strategic Infrastructure Threat Branch; the Office of Infrastructure Protection, National Protection and Programs Directorate; and the Washington State Fusion Center.