# ROLL CALL RELEASE

In Collaboration with the ITACG

20 November 2012

## (U) Suspicious Activity Reporting (SAR): Testing of Cybersecurity

(U//FOUO) Terrorists or cyber criminals might try to discover vulnerabilities in computer systems by engaging in unauthorized testing of cybersecurity in order to exploit those vulnerabilities during an attack. These attempts might include port scanning, phishing, and password cracking. "Social engineering," another technique, leverages unwitting insider access by eliciting information about operational and security procedures from employees, personnel, and their associates.

**(U//FOUO) The following SAR incidents from the NSI shared space demonstrate types of behavior terrorists or cyber criminals might exhibit during the preoperational stage of attacks. Although none were linked to terrorist or other criminal activity, they are cited as relevant examples for awareness and training purposes:**

- (U) An individual sent an e-mail to a state government office requesting information on public access to a local reservoir. The e-mail included a link to a Web site that contained malicious software (malware).
- (U) A review of a first responder's computer system revealed an attempted hacking incident; several Internet Protocol (IP) addresses associated with the probes originated from out-of-state and foreign locations, suggesting that the actual IP addresses were being masked and that the probes were malicious.
- (U) In a likely social engineering attempt, a private business received unsolicited telephone calls from a caller attempting to obtain or confirm information regarding names, titles, e-mail addresses, and access badge numbers for its employees. When asked, the caller provided no contact information and only gave her first name.

**(U) Nationwide SAR Initiative (NSI) Definition of Testing of Security**

(U) Interactions with or challenges to installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities.

(U) **Port Scanning** – a process of scanning for open computer port(s), enabling attackers to identify potential targets.

(U) **Phishing** – type of social engineering; fraudulent e-mail or other electronic communications to deceive computer users into disclosing private information or downloading malware.

(U) **Password Cracking** – attempting to guess passwords, possibly by synchronizing multi-computer attempts using automated utilities that try every possible password.

**(U) Note: The Functional Standard v 1.5 defines SAR as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."**

### (U) Possible Indicators of Cybersecurity Testing

(U//FOUO) The following activities may indicate efforts to test cybersecurity for potentially malicious purposes. Depending upon the context—time, location, and other indicators—suspicious cyber activity should be reported to the appropriate authorities, particularly if a terrorism or criminal link is suspected.

- (U//FOUO) Unsolicited phone, e-mail, or in-person inquiries asking for employee or organizational information, including official or proprietary information such as organizational structure and networks.
- (U//FOUO) Requests for access to cyber infrastructure physical areas, electronic files, or escalated computer access privileges not required to complete the requestor's job or task.
- (U//FOUO) Increase in network reconnaissance activity—such as pinging (verification that an IP address exists and accepts requests), port scanning, and intrusion detection system alerts—observed and recognized by IT personnel.
- (U//FOUO) Missing or added computer equipment in the work area, such as laptops, CDs, external hard drives, or thumb drives.

(U) For additional information on cybersecurity best practices, please refer to US-CERT Web page http://www.us-cert.gov/security-publications.

**(U//FOUO) First Amendment activities should not be reported in a SAR or Information Sharing Environment SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).**

(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-0028-13

*(U) Prepared by the Office of Intelligence and Analysis (I&A) Homeland Counterterrorism Division, the I&A Cyber Intelligence Analysis Division, the Interagency Threat Assessment and Coordination Group, the FBI Directorate of Intelligence, and the New Jersey Regional Operations Intelligence Center and the Colorado Information Analysis 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 the Transportation Security Administration Office of Intelligence and Analysis and the National Protectorate and Programs Directorate Office of Infrastructure Protection.*