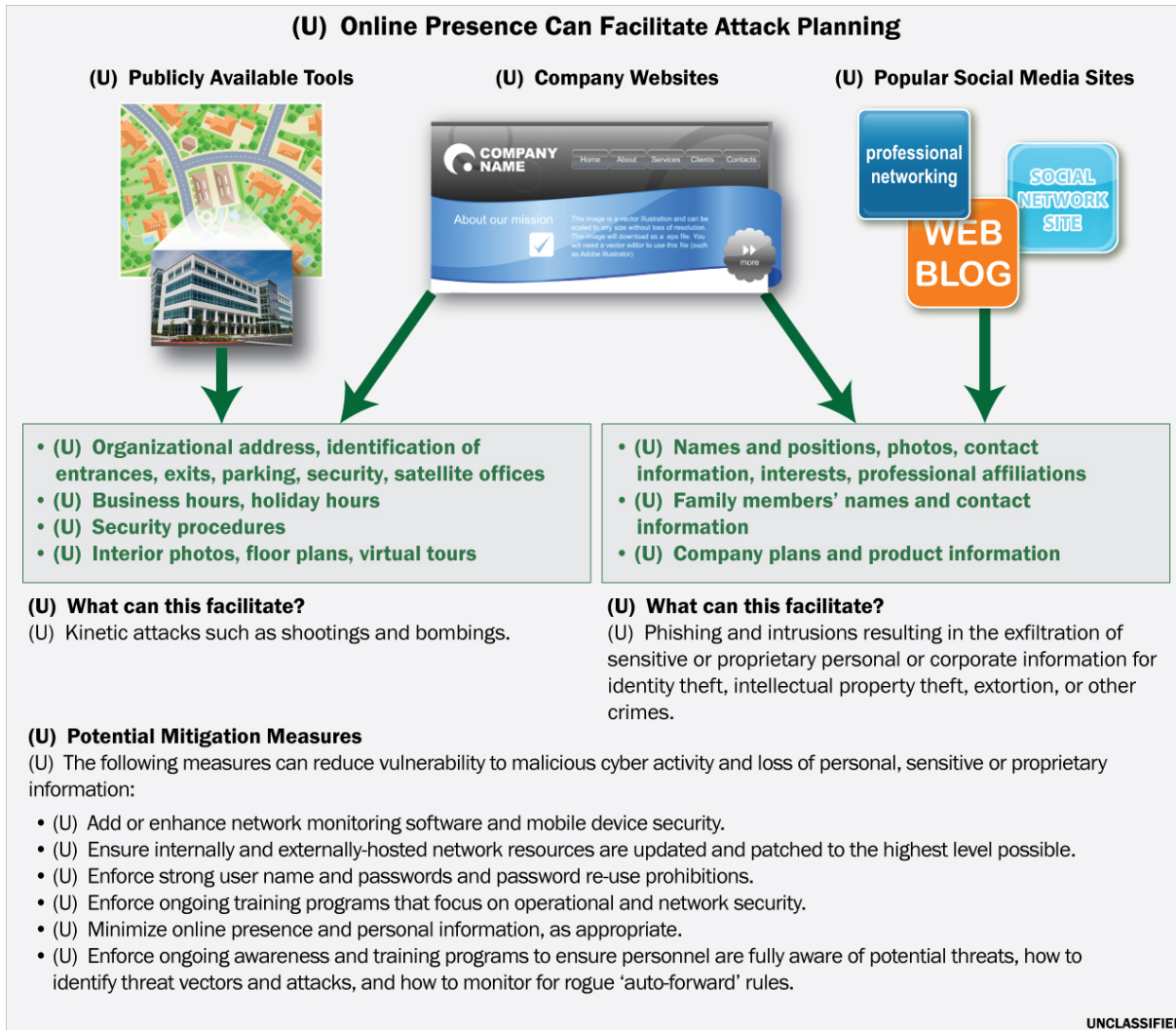# ROLL CALL RELEASE
FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

24 April 2013

(U) Use of the Internet for Attack Planning

(U//FOUO) Malicious actors may leverage the Internet to gain information against a potential target to support pre-operational planning efforts for kinetic or cyber attacks. Malicious actors can use Internet search engines for information such as maps, company photographs or blueprints, and gain additional details from social media sites and Web blogs. Some actors may use more sophisticated techniques—such as phishing, spear phishing, or actual penetration of an organization's network or devices—which can be used to gather personal, sensitive, or proprietary data.

(U) Online Presence Can Facilitate Attack Planning

(U) Publicly Available Tools **(U) Company Websites** **(U) Popular Social Media Sites**

- (U) Organizational address, identification of entrances, exits, parking, security, satellite offices
- (U) Business hours, holiday hours
- (U) Security procedures
- (U) Interior photos, floor plans, virtual tours

- (U) Names and positions, photos, contact information, interests, professional affiliations
- (U) Family members' names and contact information
- (U) Company plans and product information

(U) What can this facilitate?
(U) Kinetic attacks such as shootings and bombings.

(U) What can this facilitate?
(U) Phishing and intrusions resulting in the exfiltration of sensitive or proprietary personal or corporate information for identity theft, intellectual property theft, extortion, or other crimes.

(U) Potential Mitigation Measures
(U) The following measures can reduce vulnerability to malicious cyber activity and loss of personal, sensitive or proprietary information:

- (U) Add or enhance network monitoring software and mobile device security.
- (U) Ensure internally and externally-hosted network resources are updated and patched to the highest level possible.
- (U) Enforce strong user name and passwords and password re-use prohibitions.
- (U) Enforce ongoing training programs that focus on operational and network security.
- (U) Minimize online presence and personal information, as appropriate.
- (U) Enforce ongoing awareness and training programs to ensure personnel are fully aware of potential threats, how to identify threat vectors and attacks, and how to monitor for rogue 'auto-forward' rules.

UNCLASSIFIED

(U) Report Suspicious Activity

(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement**. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.

IA-0107-13