Webinar Questions and Answers

Elements of a Suspicious Contact Report

Webinar guests submitted several questions before and during the **11 September 2014 Elements of a Suspicious Contact Report** session. The following responses are provided by the Center for Development of Security Excellence (CDSE):

Question: What is the difference between a Suspicious Contact Report (SCR) and an unsolicited contact report [sic]?

Answer: The difference between an SCR and Unsubstantiated Contact Report (UCR) is the CI Special Agent's evaluation of whether or not the reported action can be linked to a nefarious action by a foreign actor. DSS CI HQ reviews the SCR and UCR to validate the CI Special Agent's (CISA) evaluation of the reporting. SCRs are frequently referred to Federal law enforcement or counterintelligence agencies for a determination if action is warranted. UCRs are frequently reproduced as intelligence information reports and published in national intelligence data libraries. All SCR and UCR reporting is databased at DSS CI HQs and used to evaluate all future reporting, establishing trends, and anomalies that can further refine threats to cleared industry. Every SCR and UCR has value and can further DSS's understanding of the threat posed to cleared industry.

Question: What is the best method to process/disseminate an SCR when received by an employee working for a cleared company?

Answer: First and foremost, make every effort to obtain complete information regarding the who, what, when, where, why, and how of a particular event. Facility Security Officers (FSO) should be the singular focal point for SCR reporting within their facility. FSOs should encourage all their (cleared and uncleared) employees to immediately forward them suspicious requests or contacts. FSOs, who are most familiar with reporting requirements and foreign threats to their technology, should immediately forward those reports they deem potentially suspicious to their Industrial Security Representative (ISR) and CISA for consideration. The FSO can greatly assist DSS by submitting timely reporting that answers why the contact was suspicious. The FSO should discuss with their ISR or CISA any questions concerning reporting requirements.

Question: Would you please explain what is mandatory to report, what is recommended but not mandatory, and what might not be worthy to report (e.g., spam email, email scams, spear fishing, etc.)?

Answer: Please see the DSS website for a comprehensive listing of those incidents that DSS considers reportable. The DSS CI pamphlet entitled, *Counterintelligence Best Practices for Industry*, is a great starting point. Keep in mind, the FSO's perspective and intuition on other incidents not covered in DSS CI literature but they deem "suspicious" should be reported. FSOs should discuss with their ISR or CISA any questions concerning reporting requirements. DSS's preference is "when in doubt, REPORT IT."

Webinar Questions and Answers

Question: Are phishing emails generated outside of a company that target the general public using a company brand or pseudo recruiting employment tactics considered reportable under suspicious contact?

Answer: Yes.

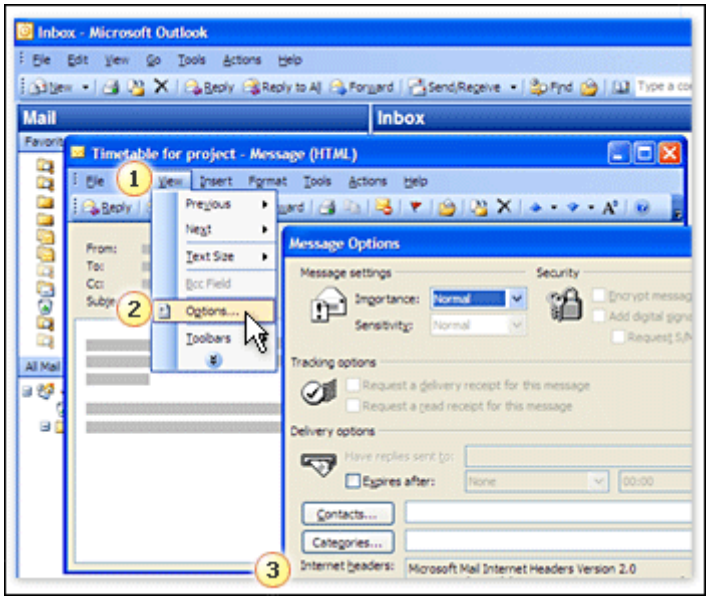
Question: How can header information on a suspicious email be forwarded without opening the email?

Answer: Expanding the headers of the original e-mail often allows the origin of the e-mail to be identified. The following information applies to Microsoft Office Outlook 2003 and Microsoft Outlook 2000 and 2002.

To view e-mail message headers within Outlook, perform the following:

1. Open a message.
2. On the *View* menu, click *Options*.
3. Header information appears under *Delivery options* in *the Internet headers* box.

Note: If you do not see the *Options* command, make sure to click *View* on the toolbar in an open message window. The *View* menu on the standard Outlook toolbar does not have the *Options* command.



Please contact your ISR and CISA for further guidance.

Question: When forwarding suspicious emails as attachments, should they be reported to DSS, CI, local FBI, state fusion center, or all three?

Answer: In accordance with the NISPOM (para 1-302b), cleared contractors shall report all suspicious contacts to their cognizant security organization, which in most cases is DSS. No other government agency can direct cleared industry to ignore this NISPOM requirement. In

cases of suspected espionage, sabotage, terrorism, or subversion (para 1-301), the FBI must be notified immediately; DSS must also be notified.

Under the NISPOM, DSS is the designated cognizant security agency. DSS maintains active professional relationships with all military service, DoD and federal law enforcement, counterintelligence, and intelligence community agencies. DSS evaluates each report received and refers the information, as appropriate, to other government agencies with authorities and jurisdiction for the information provided. Cleared industry may send suspicious contact reports directly to additional government agencies; however, DSS must be notified.

Question: Why do reporting parties not receive any feedback or status updates from the government? What is a typical turnaround time?

Answer: DSS strives to provide timely feedback to the fullest extent possible. If a FSO has provided a report to DSS and has not received feedback, the FSO should contact the CISA (and/or ISR) and request a status of the submission. The FSO should wait 30 days after submission before requesting an update on the status; this allows the CISA to appropriately triage, report, and refer potential actionable information. In some cases other government agencies may request feedback be delayed to facilitate government investigations and operations.