Webinar Questions and Answers

What Information is Reportable as a Suspicious Contact Report (SCR)?

Question: Are there any particular email SCRs that are so obviously spam that we need not report them? Is there a threshold for such emails as reportable or not?
Answer: Emails which are obviously spam—and not an attempt to target sensitive or restricted cleared contractor information, or to gather information that furthers the targeting of cleared personnel or classified information—are not reportable. However, attempts that appear to be specifically targeting a cleared facility or a DoD-related or protected technology, or to obtain classified, export-controlled, or proprietary/sensitive information from your company are valid SCRs and should be reported. Bottom line: If there is any doubt as whether to report a suspicious email or not, you should always report it.

Question: At what point does a person "complaining" about their personal financial situation cross the line into being reportable? Waiting until the situation mysteriously/greatly improves for no apparent reason seems too late.
Answer: The Facility Security Officer (FSO) and contractor employees are required to report to DSS any adverse information coming to their attention on cleared employees. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. In some cases, as from the above question, reporting the information may be a judgment call. If the FSO believes the cleared employee's complaints about their personal financial situation may have an effect on that person's ability to adequately safeguard classified information, then a report should be made to DSS. It is advisable to contact the cleared contractor's assigned DSS Industrial Security Representative (ISR) or Field Counterintelligence Specialist (FCIS) for guidance on the particular situation in question. Note: Even though the adverse information may not meet Joint Personnel Adjudication System (JPAS) reporting criteria, it still may be of CI concern to your supporting FCIS. For further information regarding adverse information, please review Industrial Security Letter 2011-04, (1-302a) at http://www.dss.mil/isp/fac_clear/download_nispom.html.

Question: Discuss the relationship with Defense Industrial Based (DIB) and how that impacts Suspicious Contact Reports (SCRs).
Answer: Assuming the question is about the DIB CS/IA FA (vice the Defense Industrial Base), DSS' execution of the NISP and the DoD CIO's DIB CS/IA FA are complementary missions. The DoD's DIB

CS/IA program is a voluntary program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The National Industrial Security Program (NISP) covers over 10,000 cleared contractors which require access to classified information from, not only the DoD, but 24 other federal agencies as well. Those cleared contractors are required to execute a Defense Security Agreement which is a legally binding document that obligates the company to abide by the security requirements of the National Security Industrial Program Operating Manual (NISPOM). Once a company is cleared, DSS has oversight authority to evaluate the security operations of the organization for compliance with the NISPOM. In as much, execution of the NISP requires threat information from across every domain (air, land, sea, space, cyber space) to depict a comprehensive picture of threat posed to cleared industry. Long standing NISPOM requirements, accordingly, mandate all cleared contractors report suspicious contacts, regardless of domain or classification to DSS and, for certain incidents, to the FBI as well (see NISPOM 1-301). Indeed, anything shy of full scope reporting unwittingly enhances the threats posed by our adversaries.

The following are examples of cyber incidents for Cleared Contractor reporting:

- Evidence of an advanced persistent threat (cyber incident, attack, or espionage).
- Evidence of unauthorized exfiltration or manipulation of information (unauthorized data removal or system changes).
- Evidence of system or network preparation for future unauthorized exploitation (intrusions or malicious code).
- Cyber activity that appears to be out of the ordinary, representing more than nuisance incidents.
- Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent.

Question: Do you just want the facts or do you want us to tell you why we think the incident is suspicious?
Answer: When reporting a suspicious contact report, FCIS are looking for the following:

A short paragraph of why the incident is suspicious to you or your employee. This should also include information relating to the item the "bad guy" is asking about.

Is this item export-controlled (ITAR/EAR), classified, related to a classified program, or does your company not know what the item is or sell it entirely?

If the incident is cyber related, please let us know if the attachment or link was opened. Was adverse impact noted on the involved company networks after the attachment or link was opened? Did anyone else in your company receive the same email? Was the email forwarded within your company or to other companies?

If your company received the SCR in email form, we request the expanded headers. If you're not sure how to acquire the expanded header from an email, please contact your local FCIS.

Remember, there are no wrong answers. Your input helps us understand your day-to-day operations and why this incident stood out.

Question: Garnishments: Are they reportable when automatically put in place by States as a result of divorce judgments?
Answer: In accordance with NISPOM 1-302a, Adverse Information, garnishments on cleared employees are recognized by DSS as adverse information and must be reported to your local ISR and to JPAS. It does not matter if the garnishment is divorce related or not. If you do not report the garnishment, it could be identified

as vulnerability during your next assessment. From a counterintelligence perspective, financial concerns are always important issues to address. Some questions worthy of examination are:

Did the individual self-report the financial issue?
Has the individual also had a security violation or other HR concerns in the past?
Does the individual have any foreign ties? These could include, but are not limited to foreign travel, relatives, foreign adopted children, hosting foreign exchange students, etc.?
Has the individual been seen working hours inconsistent with their job assignment?
Has the individual attempted to gain access to restricted areas?
Does the individual desire not to perform classified work or no longer wish to be processed for a clearance?

If you have a combination of wage garnishments and any other possible counterintelligence indicator(s), these should be reported to your local FCIS. If you have questions about what qualifies as a counterintelligence indicator, contact your local FCIS.

Question: Large companies have processes in place to deal with unwanted email or spam. Employees are told to forward spam or delete it. How do we make the employee report SCRs if this is in place?
Answer: Field Counterintelligence Specialists (FCIS) are not interested in receiving SCRs based on spam when spam is defined as "electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages." Cleared company policies on handling likely spam should describe factors of security and CI interest and, if present, employees should forward the email to the designated company security authority for further review.
However, one challenge FCIS face is helping companies identify the difference between spam and a suspicious contact. Many times intelligence is lost because the threat is not recognized. Counterintelligence education is key, especially for engineers and employees with positions in business development and upper management. You can find counterintelligence training materials at http://www.dss.mil/isp/count_intell/count_train_mat.html, http://www.cdse.edu/catalog/elearning/index.html or contact your local FCIS to request a briefing.
One idea to aid in the identification of threats is to include the FSO on business development emails derived from the company's website. FSOs and other security personnel receive considerable more training in identifying threats. This provides the FSO an opportunity to recognize possible threats within these emails and prevent them from being deleted or sent to the spam box.

Question: Please provide more definition between casual contact and personal contact (when to report).
Answer: The difference between casual and personal contact is the context of the contact. When an employee meets a foreign official for official business for the first time and they exchange pleasantries such as "how are you and how is your family?", that is casual contact. If an employee meets a foreign official for

the tenth time and they exchange pleasantries such as "How is your wife Ann?" and "How is William liking his kindergarten teacher?", that is broaching personal contact. If an employee invites a foreign official to his residence for dinner or vice versa, that is personal contact. When the context of the contact has moved from general personal information—terms such as your wife and your children—to specifics such as names and places, the contact has become personal and should be reported.

Question: Please provide examples of what an FSO can do to bolster "Insider Threat" prevention, indicators, etc.
Answer: FSOs should include Insider Threat awareness in their annual security awareness training and ensure employees are aware of potential espionage indicators: undue affluence; unreported foreign contact or unreported foreign travel; efforts to expand access without need-to-know; unusual work hours that are not consistent with duties; anomalies that make employees uncomfortable; and exploitable behaviors such as sexual deviance, adultery, drug or alcohol abuse, gambling, and loyalty issues. Use examples from news media as training tools. Encourage reporting and provide anonymity.

Question: Questions posed by foreign persons under contract with the cleared entity that have approved Technology Assistance Agreement (TAAs) and Export licenses. Cleared industry does not always see a question posed outside the scope of the TAA to be reportable.
Answer: National Industrial Security Program Operating Manual (NISPOM), paragraph 1-302b states, "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee." Any questions posed outside the scope of the TAA should be reported. Tiny bits of "seemingly unimportant" information, whether relating to the TAA or not, could be combined to give an adversary a better understanding of critical program information. NISPOM Paragraph 5-508, Disclosure of Export Controlled Information to Foreign Persons, instructs that "Contractors shall not disclose export-controlled information and technology (classified or unclassified) to a foreign person, whether an employee or not, or whether disclosure occurs in the United States or abroad, unless such disclosure is in compliance with applicable U.S. laws and regulations." The situation you describe appears to be a violation of this provision if the contractor's response is outside the TAA or export licenses.

Question: What contact should not be reported with respect to Foreign Nationals?
Answer: The best way to answer this question is by discussing foreign contact that should be reported. According to Paragraph C9.1.4.2 of DoD 5200.2-R, Personnel Security Program, "Individuals having access to classified information must report promptly to their security office: Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which: Illegal or unauthorized access is sought to classified or otherwise sensitive information, or the employee is concerned that he or she may be the target of exploitation by a foreign entity."

Question: What happens to the SCRs that are reported?
Answer: FCIS discern if the reported information is responsive to national-level collection requirements as outlined by the Defense Intelligence Agency or that pertain to potential criminal activity. FCISs conduct follow-up activities to substantiate or further develop the reported contact. At that time FCIS write formal SCRs on the incident and submit to DSS Headquarters for formal intelligence analysis. Once DSS HQ completes the formal intelligence analysis, they submit an intelligence information report to the national community, if warranted, and return analytical findings back to the FCIS. This analyzed information is shared with Intelligence Community and federal law enforcement partners to help understand the threats facing DoD technologies and for potential investigative action or other counterintelligence related activities.

Question: What should you do when the command takes their time in the notification process, or when they choose to do nothing or to not report?
Answer: Paragraph 1-302b of the National Industrial Security Program Operating Manual (NISPOM) provides requirements for reporting suspicious contacts/activities. The NISPOM reference relates "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee." Additionally, Paragraph 1-301 pertains to reports to be submitted to the FBI that the "Contractor shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA." DSS is the designated CSA; therefore, a copy should be also submitted to your DSS ISR or FCIS. It is incumbent upon the Contractor to comply with the NISPOM per their agreement with the Government and non-reporting of suspicious contacts could be considered non-compliance. Therefore, the FSO should stress these points with their leadership in order to remain compliant with the NISPOM.

Question: Can we as security professionals be too suspicious?
Answer: Most FCISs would agree that security professionals can never be too suspicious. It is the security professional's job and duty to "trust but verify" and remain vigilant in the protection of property and information. You are your company's front line of defense and the government is counting on you as a force multiplier in the protection of national security interests.

Question: For clearer guidance, I would like some definitive examples of recurring foreign contacts which would also be considered suspicious in nature and therefore reportable by industry employees.
Answer: Paragraph 1-302b of the NISPOM provides requirements for reporting suspicious contacts/ activities. The NISPOM reference says "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee." Additionally, 1-301 pertains to reports to be submitted to the FBI that the "Contractor shall

promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA" (DSS).

The most common examples of suspicious contacts reported to DSS include email solicitations requesting information on technologies or products and services. Other examples include academic solicitations or seeking employment, solicitations or marketing of services, and suspicious network activity. Lastly, foreign business travelers or foreign visitors at cleared contractor facilities are other examples most commonly reported.

Example: A presumed South and Central Asian national contacted a cleared contractor in an attempt to acquire export-controlled parts used in counter-battery radar systems. A little later in the year, a different U.S. cleared contractor received an unsolicited e-mail from the same individual expressing interest in purchasing the same radar system that was requested in the first incident. The suspicious individual was a representative of a trading company from his home country. Multiple sources indicated that his home government established the trading company as a front company to procure export-controlled technology and equipment for the national military, and that the trading company had previously sought products on behalf of several military services and defense-affiliated entities. The trading company was the subject of several other suspicious contact reporting attempts to purchase export-controlled electronics products and communications equipment used in military aircraft.

For more information and examples of foreign targeting of U.S. Technologies, refer to the DSS Collection Trends booklet.

Question: How does one determine if a phishing attempt is worth reporting?

Answer: Spear-phishing attacks are pervasive throughout the cyber domain and are effective methods to bypass network security protocols in order to gain varying levels of access to the network. Spear-phishing is an attempt to do something nefarious to the company or its employees, and all spear-phishing incidents should be reported to DSS under the authority of Paragraph 1-302b of the National Industrial Security Program Operating Manual (NISPOM), which stipulates reporting requirements for suspicious activities. Also, providing the originating IP addresses, via expanded email headers, is crucial to meaningful intelligence analysis.

Question: I want to confirm these questions are non-attributional. We are providing our CI Rep. with all of our foreign visitors prior to the visit and he is opening a SCR on all visitors. We are then encouraged to follow-up with the host/escort to inquire about suspicious activity and report back to the CI Rep. He then closes the SCR. Is this a requirement? We don't have an issue with providing the names, but the follow-up is becoming an administrative burden. Our employees are instructed to notify security if any suspicious activity occurs during the visit or at any time. Again, I want to confirm non-attribution.

Answer: There is a requirement to report suspicious contacts in accordance with Paragraph 1-302b of the National Industrial Security Program Operating Manual (NISPOM). The activities described in this question appear to be consistent with effective counterintelligence activities to ascertain if nefarious activity has taken place after a foreign visit. While employees are routinely instructed to report suspicious activities in general, a significant portion of intelligence is gleaned as a result of direct contact during follow-up activities. Nuances displayed by an adversary's intelligence officer or proxy may be missed unless explored, verbally, with those in contact with the visitors. Recommend the questioner contact their servicing FCIS to discuss the specific administrative burdens that are being faced to develop practical yet effective solutions.

Question: I would like to help my employees better recognize what is a suspicious contact and help our security program.
Answer: While there are various ideas discussed elsewhere in this forum, probably the best way is to contact your servicing FCIS directly for assistance. DSS FCIS can provide an array of services, including counterintelligence awareness and training briefings, various products to inform and educate the reader on foreign threats, and other helpful advice and sources of information. Additionally, various intelligence publications and other informative products can be found on DSS public website at www.dss.mil.

Question: Is medication prescribed for anxiety or depression reportable?
Answer: According to DoD Instruction 5200.2-R, Personnel Security Program, Paragraph C2.2.1, the criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to various conditions that include Paragraph C2.2.1.10, which states that "Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case." Additionally, Paragraph C2.2.1.14 discusses the Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug. In essence, it appears that the prescription of anxiety or depression medication in and of itself is not the issue that requires reporting, but potentially the reasons behind the prescription are what need to be evaluated. When in doubt, contact your FSO for further guidance.

Question: Please discuss the conditions that would warrant reporting contact with a foreign national friend, dorm mate, roommate, family member (including in-laws), home maintenance or service providers (e.g. maid, landscaper), etc. as a suspicious contact.
Answer: Paragraph C9.1.4.2 of DoD 5200.2-R, Personnel Security Program, states: "Individuals having access to classified information must report promptly to their security office: Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which: Illegal or unauthorized access is sought to classified or otherwise sensitive information, or the employee is concerned that he or she may be the target of exploitation by a foreign entity." Your understanding of exploitation tactics is based on how much security training you have received. DSS

provides numerous educational handouts and briefings that help educate personnel on exploitation methods.

Question: Should evaluation of degree of suspicion (suspiciousness?) be unbiased, i.e., without regard to country of origin or citizenship and without regard to (for example) religion? If so, in theory, it is really possible to be unbiased?
Answer: If any foreign national is asking about technology that is classified or ITAR/export controlled (needing U.S. approval) to have technical discussions, that attempt to get the information is reportable. They are attempting to collect information illegally. It doesn't matter if the contact occurs at work, a tradeshow, a professional society meeting, or at a little league game. For CI purposes, a foreign national is considered a representative of that country.

Question: To what extent does an inquiry seeking information about a company's proprietary information, rather than classified information, constitute the need for an SCR?
Answer: If the information pertains to defense related material, that would more than likely require an export license to sale to the foreign requestor, so you should report it. Just because you generate an SCR does not mean the requestor is definitively doing something wrong; you are reporting because you are suspicious about the activity. Always err on the side of caution and report—in most cases, if the government finds any pertinent information concerning the requestor, we will share that information with the FSO.