SUSPICIOUS CONTACTS

The partnership between cleared defense contractors and the Defense Counterintelligence and Security Agency (DCSA) has contributed to significant strides in the understanding of the collection threat directed against industry. The value of the Suspicious Contact Reports from Industry to DCSA is of a very high level as they assist the DOD in understanding methods and targets of collectors. These reports are used to educate both Government and Industry on which DOD Technologies are targets of the foreign intelligence services.

What qualifies as a suspicious contact?

1. Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.
2. All contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

What are examples of suspicious contacts?

1. Requests for protected information under the guise of a price quote or purchase request, market survey, or other pretense (this could come from *both* US citizens and foreign nationals).
2. Foreign entities targeting cleared employees traveling overseas via airport screening or hotel room incursions.
3. Attempts to entice cleared employees into situations that could lead to blackmail or extortion.
4. Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file.
5. Attempts to place cleared personnel under obligation through special treatment, favors, gifts or money.
6. Former cleared or trusted employees attempting to gather controlled or classified information from previous co-workers.

Here are explanations on how certain methods can be used to gather information from US companies:

Co-opting Former Employees – There have been several reports that highlight a modus operandi (MO) in which formerly cleared U.S. employees go to work for a foreign company or institute, where their work concerns a project or technology similar to what they were working on for a cleared U.S. company. They may be recruited for employment by a foreign national and may be expected to use their U.S. contacts to obtain additional information. The use of a visit by a formerly cleared U.S. employee is a good method to collect export-restricted and perhaps classified technical information from unwitting former coworkers. US citizens, working for foreign companies or institutes, may wittingly or unwittingly take

advantage of their former U.S. coworkers by incorrectly convincing them that "unclassified" technical discussions are appropriate or authorized.

Use of Contract Bidding to Elicit Information - Officials of a U.S. defense contractor reported an incident in which their company was invited to prepare a proposal and bid on a foreign defense contract for an avionics system for a Western European government. The U.S. defense contractor officials prepared what they believed was the best, most detailed proposal of all other bidders for the foreign government contract. Despite this, after all the bids were in, the foreign government decided to build the system themselves. Later, while attending an international trade show, U.S. defense contractor personnel saw a foreign-built system, from the country to which they submitted the bid, which looked identical to their own. Other governments and foreign companies may use this modus operandi (MO) to acquire proprietary information.

Who Should Submit Suspicious Contacts?

Cleared personnel are *required* under the National Industrial Security Program to report any suspicious contacts. Additionally, it is *highly recommended* that un-cleared company personnel also report any incidents or communications which result from a suspicious contact. Un-cleared personnel may have access to unclassified company proprietary information as well as controlled or dual-use technology which may be restricted under the International Traffic in Arms Regulations (ITAR). This information may be targeted by foreign persons or organizations. Additionally, intelligence agents may attempt to contact un-cleared individuals in order to circumvent other restrictions or to gain better access to other cleared employees at the same facility.

How to Report a Suspicious Contact

You should immediately contact your Facility Security Officer (FSO) if you are faced with an incident or communication that is similar to one of the examples listed above. You should also report if *you* feel for any reason that a contact is somehow unusual or out of the ordinary. Deployed personnel working in overseas locations, or at government sites, can also contact the local government security officer.

When making a report it is important to provide as much information as possible. Try to assemble the 5 W's (Who, What, When, Where, Why).

1. Who contacted you and how they contacted you. This should include as much information as possible on who contacted you such as name, contact info, company, and country of origin.
2. What did they contact you for? Was it in regards to a specific contract, type of technology, or a certain person or capability?
3. When did they contact you (date and time)?
4. Where were you when they contacted you and where did they identify themselves as being located.
5. Why did they make contact with you? Was it due to your position on a certain contract, did they locate your contact information on a company site, or were they recommended to you by a third party?

Also please try to forward any records of communications, such as e-mails or letters, which were originated by the suspicious contact.

Once you annotate the available information you can contact the FSO via phone, e-mail, or in person to document the contact. The FSO may ask additional questions in order to gather as much information.

Additional Training

The Defense Security Service sponsors several training programs which increase counterintelligence training and understanding. The following link will allow you to take the "Thwarting the Enemy" on-line training course. This training takes approximately 35-45 minutes and is highly recommended.
http://cdsetrain.dtic.mil/thwarting/index.htm

The DCSA Counterintelligence Directorate has released the unclassified publication, "Targeting U.S. Technologies: A Trend Analysis Reporting from Defense Industry." This report analyzes suspicious contact reports received from defense industry in fiscal year 2010. It is available online in PDF format.
http://www.DSS.mil/counterintel/2011-unclassified-trends.pdf

REMEMBER!

You may be the first, last, and only opportunity
for the U.S. Government to obtain the
information being reported to you

Additional Material – Part 1 of 2

CASE STUDIES

Here are a few recent examples compiled by the DCSA Counterintelligence (CI) Office, culled from the many thousands of "Suspicious Contact Reports" made annually by cleared facilities in accordance with the requirements of the National Industrial Security Program Operating Manual (NISPOM):

- A defense contractor employee, working on military grade technologies for a cleared U.S. defense company, was contacted via email by a suspected representative of a foreign firm; however, it was noted that the requestor's firm's name did not match the incoming email address. The email correspondent claimed his firm had an "urgent requirement" for military-grade technology being developed at the contractor facility and wanted to establish a business relationship. Subsequent analysis revealed that the email address used by the correspondent was associated with a second foreign company having a history of end-user certificate fraud.

- A representative of a foreign research center contacted a cleared U.S. defense facility and subsequently provided product design schematics in an apparent attempt to justify obtaining export-controlled materials. A review of the schematics submitted by the foreign research center revealed that they were associated with a military critical technology program. At first, the foreign research center denied that the product in the schematics had any military applications, but when challenged, eventually recanted, admitting that the product design presented could indeed be used for military purposes. Despite this exposed deception, the foreign firm's representatives continued to maintain they had no intention of utilizing the final product for such purposes.

- A cleared U.S. defense company reported receiving multiple deceptive emails that (when opened) resulted in malicious software being automatically installed on the company's internal computer system. Numerous employees within this cleared defense company were victims of this ruse. Following the extraction and analysis of one of the malicious payloads, cleared U.S. defense analysts discovered additional malicious codes embedded in .gif and .jpg image files in the software.

- Over several months, a foreign firm repeatedly contacted an employee of a U.S. cleared defense company, cultivating his assistance in procuring components for the foreign firm's use. Although the contact had begun with a seemingly innocuous request for components that were not controlled, the foreign firm subsequently amended its list to include dual-use export controlled items. The foreign firm eventually shared the contractor employee's contact information with multiple sections inside the foreign firm, resulting in a flood of additional requests to the same contractor employee. Within a month, this same foreign firm shifted focus to a second employee within the defense company, requesting new technology known to be of interest to the military research and development efforts of the foreign firm's country of origin.

- An individual apparently posing as a foreign student contacted an employee working for a cleared U.S. defense company performing aerodynamics research, asking for what amounted to classified information on the cleared defense company's UAV applications. The foreign student, supposedly an aerodynamics major at a major foreign university, also inquired about the possibility of an intern position in the company's aerodynamics research branch. The "student's" requested information and research interests related to classified and export restricted technology known to be actively sought by the student's country of origin.

- An engineering team from a U.S. defense contractor participated in an approved exchange with a foreign counterpart team during which approved, and unclassified, technical information was commonly shared between participants. Following the exchange program's completion, representatives of the US defense contractor discovered several "export restricted" documents among a large volume of printed material left on-site by the foreign engineer team. Upon further review of the printed materials left by the foreign engineers, the U.S. company representatives discovered the foreign team had acquired a large amount of open source information on military programs clearly outside the scope of the unclassified contract with the cleared U.S. defense company.

Additional Material – Part 2 of 2

SITUATIONAL FAQs

Presented here are a series of scenarios and a recommended REPORT/NO REPORT for each type of incident. Please remember that each encounter is unique and rarely will a situation fit an exact mold. These circumstances are presented only as a basic guideline and you should always report an incident if you feel that something suspicious has occurred.

1. While traveling overseas you are approached by a local national who offers to sell you quality DVD movies. NO REPORT

2. After returning from an overseas deployment you find a 'Friend Request' on your social networking site (Facebook, MySpace, LinkedIn, etc.) from a foreign national who you met while overseas. REPORT

3. While working at the corporate office you receive an unsolicited e-mail from an unknown source inquiring as to the capabilities of company equipment that was used on a government contract. REPORT

4. You receive an unsolicited request which is poorly written, handwritten, or printed on letterhead which is not similar to current industry standards. REPORT

5. You receive a resume from a foreign national for an open position which the company has advertised for. The job posting identifies that the position requires that the individual be a US Citizen or have a clearance. REPORT

6. You receive a resume from a foreign national for an open position which the company has advertised for. The job posting is open ended and for a location in a foreign country. The posting *does not* have a requirement that the individual be a US Citizen and there is no reference for a clearance requirement. NO REPORT

7. You receive an unsolicited request from an individual, identifying themselves as a student, who states that they are interested in interning on a project that is classified or restricted. REPORT

8. You receive an e-mail stating that the King of Kukastaniania (or other random location) needs your help to transfer a million dollars and will give you a percentage for your assistance. NO REPORT

9. Upon arriving at the office you notice an unknown individual hanging out by a side door or looking in a window. As you pull up the individual immediately departs. REPORT

10. While traveling overseas you are randomly approached in a bar by a very attractive model (male or female) who wants to buy you drinks. REPORT

11. While staying at a hotel you return to your room to find that items have been moved around or there are indicators that someone entered the room in your absence. REPORT