

Industrial Security Webinar Series

Learn @ Lunch



**Critical Elements of a Suspicious Contact Report (SCR)**

---

---

---

---

---

---

---

---

Learn @ Lunch

CDSE

**Agenda**

- What is Counterintelligence (CI)?
- NISPOM Reporting Requirements
- DSS Reporting Definitions (SCR, UCR, ANV)
- Identify what constitutes a Suspicious Contact covering multiple categories (email, foreign visits, foreign travel, etc.)
- Additional Useful Information

---

---

---

---

---

---

---

---

Learn @ Lunch

CDSE

**What is Counterintelligence?**

- Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against:
  - Espionage
  - Other Intelligence Activities
  - Sabotage
  - Assassinations
- Conducted by, for, or on behalf of:
  - Foreign powers
  - Foreign governmental and commercial organizations
  - Foreign persons or their agents
  - International terrorist organizations



---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

### Industry – First Line of Defense

- You possess or have access to classified information and/or information pertaining to technologies that are highly sought after by foreign entities



Friendly Information



Research, development, testing, and evaluation



Program milestones & specifications



System capabilities

- Foreign entities will also target information relating to your facility's personnel, security, and operations

YOU are the first line of defense in protecting classified information and defense technologies!

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

### NISPOM 1-302: Reports to be Submitted to the CSA

- 1-302 b. Suspicious Contacts  
Contractor shall report:
  - ...efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
  - ...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 shall be reported

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

### Poll 1

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

### DSS Reporting Definitions

- DSS sorts CI reports into three distinct categories:
  - **Suspicious Contact Report (SCR)** – a report of CI concern that likely represents efforts by an individual to obtain illegal or unauthorized access to classified information or technology
  - **Unsubstantiated Contact Report (UCR)** – a report where it is unlikely that an individual attempted to gain access to classified information or technology, yet still has some value
  - **Assessed No Value (ANV)** – a report that only remotely, if at all, represents a CI concern (SPAM, etc.)

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

### Identifying Suspicious Contacts

- Examples of reportable suspicious contacts:
  - Requests for protected information under the guise of a price quote or purchase request, market survey, or other pretense
  - Foreign entities targeting cleared employees traveling overseas
  - Attempts by foreign entities to acquire sensitive information during visits to cleared contractor facilities
  - Conferences, Conventions and Trade Shows (CC&T) targeting
  - Social Networking Services (SNS)
  - Attempts to place cleared personnel under obligation through special treatment, favors, gifts or money




---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

### (U) Attempted Acquisition of Technology (AAT)

From: Sally.Chen@yahoo.com  
 Sent: Friday, March 28, 2008 3:23 AM  
 To: Info@[U.S. Company]  
 Subject: SCS 3500

Dearest Friend,

Please let me know how you want to proceed on the sale of 30 units of the SCS 3500.

All export licenses in place and approved. The end-use of this item will not be for military or defense purposes.

Please get back to me ASAP regarding this urgent matter.

Sally Chen  
 CEO  
 Great Wall Innovators, Ltd.  
 Cell: 86 3522 9865  
 Office: 86 3522 9866  
 Fax: 86 3522 9877

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

**Poll 2**

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

**CI Awareness - Foreign Travel**

- Foreign travel increases the risk of foreign intelligence targeting
- Collection techniques
  - Bugged hotel rooms or airline cabins
  - Intercepts of fax and email transmissions
  - Tracking activity via ATM transactions, and internet usage at Internet kiosks or WIFI access points
  - Recording of telephone conversations
  - Unauthorized access to or theft of electronic devices – installation of malicious software
  - Intrusion into or searches of hotel rooms and hotel room safes
  - Enhanced interviews by customs officials
- Practical countermeasures (Foreign Travel Tri-Fold, Pre and Post Foreign Travel Briefings (with CISA support))

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

**CI Awareness- Foreign Visitors**

- Foreign delegation visits to cleared contractors are a common method of operation used to target U.S. technologies
- Foreign visitor collection techniques
  - Peppering escorts/personnel with questions
  - Wandering
  - Practicing "divide and conquer"
  - Switching visitors
  - Making last-minute additions to visit request
  - Switching topics
  - Purporting to be "distracted"
- Practical countermeasures (Preparing for Foreign Visitor Tri-Fold, \*\*Send CISA list of foreign attendees in advance of the visit\*\*)

---

---

---

---

---

---

---

---

Learn @ Lunch 

**CI Awareness- Conferences, Conventions, and Trade Shows**

- Conferences, conventions, and trade shows present collectors with a target-rich environment due to the abundance of technology, engineers, and technical personnel in attendance
- Collection techniques
  - Elicitation of classified or export-restricted information from subject matter experts
  - Theft of technology on display
  - Photography
  - Collection of business cards and other personal information
  - Gaining access to personal or business electronic devices left unattended
- Practical countermeasures (CCT Tri-Fold, Specific CCT Briefings provided by your CISA)

---

---

---

---

---

---

---

---

Learn @ Lunch 

**Poll 3**

---

---

---

---

---

---

---

---

Learn @ Lunch 

**CI Awareness- Social Media**

- Many people are using social media in this day and age, including cleared personnel.
- Some key indicators with social media friend/contact requests to report are as follows:
  - Unsolicited
  - Foreign
  - Foreign government/military/intel representative
  - Suspicious message/comment received with the request

---

---

---

---

---

---

---

---

Learn @ Lunch 

### Poll 4

---

---

---

---

---

---

---

---

Learn @ Lunch 

### What to Report

Email

- In addition to forwarding the original email to your respective ISR and CISA, please preface the email with as much detail as possible, i.e., Why you feel the contact is suspicious. (foreign nexus requesting a sensitive part, etc.)
- If the contact is directed at a specific employee, provide detail on the employee's background, i.e., Why he/she may have been targeted.



---

---

---

---

---

---

---

---

Learn @ Lunch 

### What to Report

Email

- Ensure you copy/paste the original email's "header" information. The header includes some critical data, such as the originating IP Address, which will be used during the analysis phase.
- Any other details you feel are relevant or might assist DSS with categorizing the report (SCR, UCR, ANV)



---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

**What to Report**

All other "non-email" contacts:

- Describe the actual event (foreign visitor/foreign travel/tradeshaw contact, etc.) in as much detail as possible (5W's)
- Provide as much detail as possible on the description of the suspicious individual (Height, Weight, Hair, Eyes, Distinguishing marks/tattoos, etc.)



---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

**What to Report**

All other "non-email" contacts

- If a business card was obtained, please include a scanned copy with your SCR submission
- For SNS contacts, capture a screen shot of the individual with as much identifying data as feasible (affiliations, education history, etc.)



---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

---

**First, Last, and Only (FLO)**

As your facility's FSO, you may be the first, last, and only opportunity for the U.S. Government to obtain the information being reported to you.

Each and every report you submit counts and has the real potential to make a significant impact to our national security.

---

---

---

---

---

---

---

---

Learn @ Lunch 

**Final Thought: Feedback on SCR**

- Our goal is to provide feedback on all SCRs that you submit
- Not always possible – Operational reasons
- Express your concerns when not received
- Considerations: Geographic concerns, office coverage, competing priorities, classification, etc.

---

---

---

---

---

---

---

Learn @ Lunch 

**Additional Support**

- Contact DSS CI for questions regarding:
  - This briefing
  - Foreign Visitors
  - Foreign Travel
  - Arranging Briefings
  - CI Support
- Visit DSS web page for additional educational material on the threat to you and Industry:

[WWW.DSS.MIL](http://WWW.DSS.MIL)

---

---

---

---

---

---

---

Learn @ Lunch 

**Contact Information**

For additional information, please contact your assigned IS Rep and CISA.

---

---

---

---

---

---

---

Learn @ Lunch CDSE

**Webinar Feedback**



25

---

---

---

---

---

---

---

---

Learn @ Lunch CDSE

**Contacts and Resources**

Contact CDSE at  
[counterintelligence.training@dss.mil](mailto:counterintelligence.training@dss.mil)

CI Training  
<http://www.cdse.edu/catalog/counterintelligence.html>

CI Products  
[http://www.dss.mil/isp/count\\_intell/index.html](http://www.dss.mil/isp/count_intell/index.html)

26

---

---

---

---

---

---

---

---