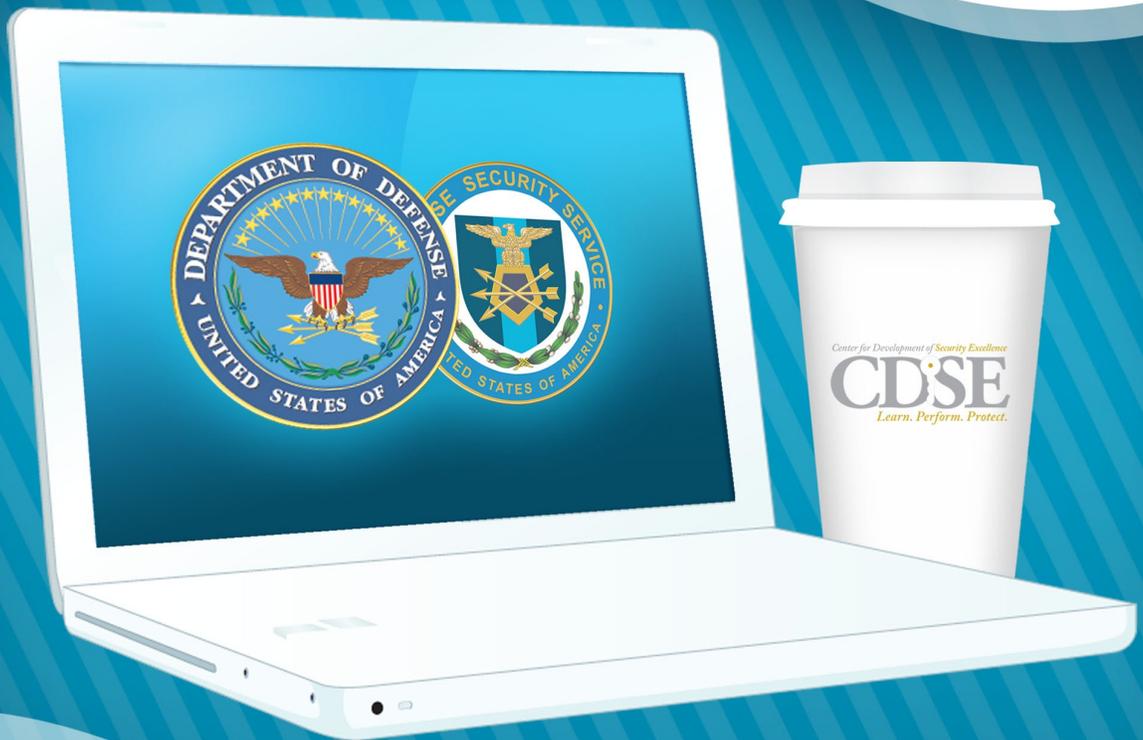


Industrial Security Webinar Series

Learn  Lunch



Lifecycle of a Suspicious Contact Report (SCR)

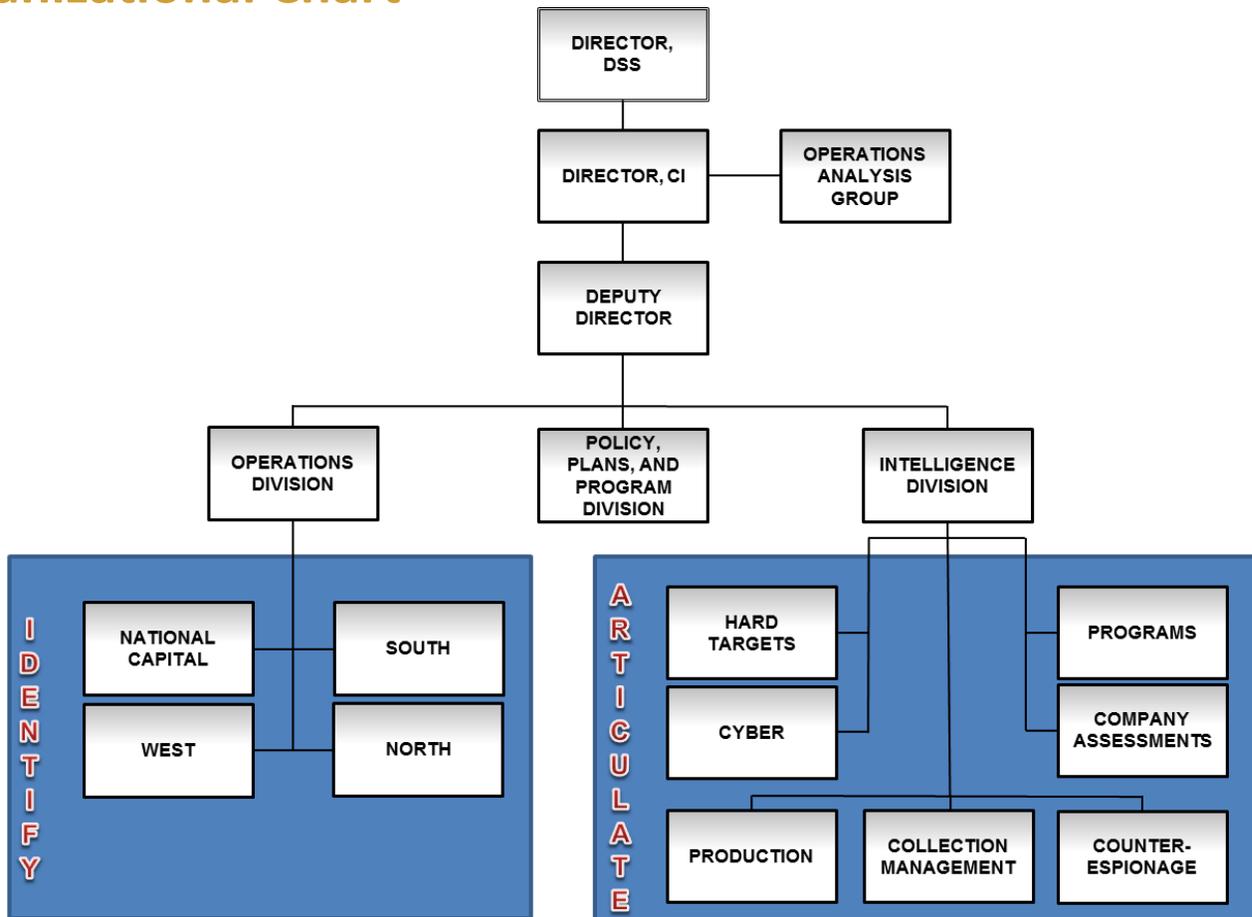


Lifecycle of an SCR

Agenda

1. Introduction
2. DSS CI Directorate
3. What is Counterintelligence (CI)?
4. Identifying Suspicious Contacts
5. DSS Reporting Definitions
6. DSS Reporting Process
7. Finished Intelligence Products
8. Additional Information

Organizational Chart



Lifecycle of an SCR

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

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!

Lifecycle of an SCR

1-302 Reports to be Submitted to the CSA

a. Adverse Information.

...concerning any of their cleared employees

...not based on rumor or innuendo

...subsequent termination of employment of an employee does not obviate the requirement to submit this report

b. Suspicious Contacts

...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

Identifying Suspicious Contacts

Examples of 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 via airport screening or hotel room incursions
- Attempts to entice cleared employees into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
- Attempts to place cleared personnel under obligation through special treatment, favors, gifts or money

Lifecycle of an SCR

DSS Reporting Definitions

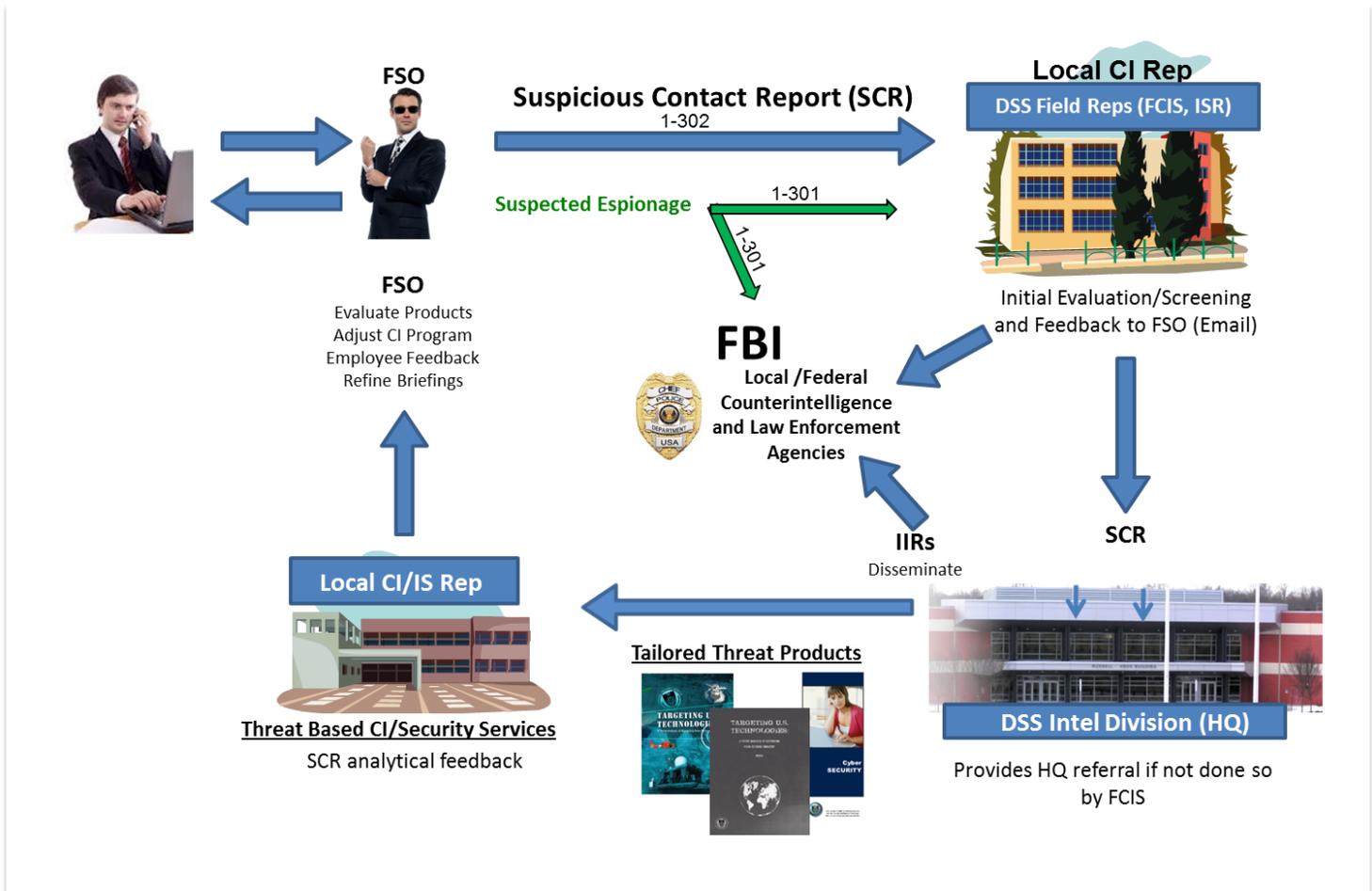
DSS sorts reports into three distinct categories:

Suspicious Contact Report (SCR) – a report of CI concern and 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

Assessed No Value (ANV) – a report that only remotely represents a CI concern

SCR Lifecycle



Lifecycle of an SCR

Roles – The Facility Security Officer

The Facility Security Officer (FSO) serves an integral role:

- Facilitates communication between DSS and cleared facility
- Promotes CI awareness at cleared facility

Pass suspicious contact information to DSS representative in a timely manner:

- Field CI Specialist (FCIS)
- Industrial Security Representative (ISR)
- Information Security System Professional (ISSP)

Receives SCR feedback and DSS finished analytic products

Roles – The Field CI Specialist

Receives suspicious contact from FSO/ISR/ISSP

Determines if contact is:

- SCR
- UCR
- ANV

If determined to be of CI value:

- Information is captured in a report and forwarded to CI headquarters for research and analysis

Has the option of generating an immediate local referral to respective U.S. Government agency or agencies based on applicability and time sensitivity

Lifecycle of an SCR

Roles – DSS CI Intelligence Division

Based on context of contact, SCR is sent to one of three branches:

- Hard Targets
- Cyber
- Counterespionage

Analysts conduct research and analysis

- Classified and unclassified resources

Generate an analytic response

Generate a referral at the national level if required

Forward findings to FCIS for dissemination to respective cleared facility

Roles – DSS CI Operations Division

- Conduct research on suspicious contacts received from industry
- Provide referrals to headquarters elements of other USG agencies
- Provide liaisons to FBI and ICE headquarters, and U.S. CYBERCOM and the National Cyber Investigative Joint Task Force
- Perform outreach to CI leads from 24 other federal agencies supported by DSS
- Contribute to National-Level policy discussions and de-confliction/synchronization efforts
- Develop monthly reporting metrics and provide final case disposition
- General administrative and logistics support to field offices

Lifecycle of an SCR

Roles – Operations Analysis Group

Established on June 15, 2010, as a forward-looking and innovative measure to drive collaboration and information sharing across the agency

Representatives from:

- CI, Industrial Security Field Operations (ISFO), Defense Industrial Security Clearance Office (DISCO), Foreign Ownership Control or Influence (FOCI), and Industrial Policy and Programs(IP) constitute membership under the OAG’s leadership

Meet daily to address high profile reports submitted based on reporting criteria and are addressed by the appropriate OAG representative(s)

- Each report examined to determine vulnerability-internal to DSS or external-and is addressed through resolution to include DSS process improvements

DSS CI Products

	C/U	Hard-Copy/ FCIS	DSS.smil. mil/ DSS.mil	DIBNet	SIPRnet email	HSIN	DIBNet- U
• Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry	C/U	X	X	X			
• The Crimson Shield	C	X	X	X	X		
• The Scarlet Sentinel	U					X	X
• Cyber Activity Bulletins	U					X	X
• Bronze Dragon – Program Assessments	C	X	X				
• Gray Torch – Company Assessments	C limited						



Lifecycle of an SCR

Additional Products

- Intelligence Information Reports (IIRs)
- DSS CI Web-Based Training
- DSS Threat Advisory
- Counterespionage Branch Analysis Report (CEBAR)
- CI Briefing
- CI Tri-folds

Additional Support

Contact DSS CI for questions regarding:

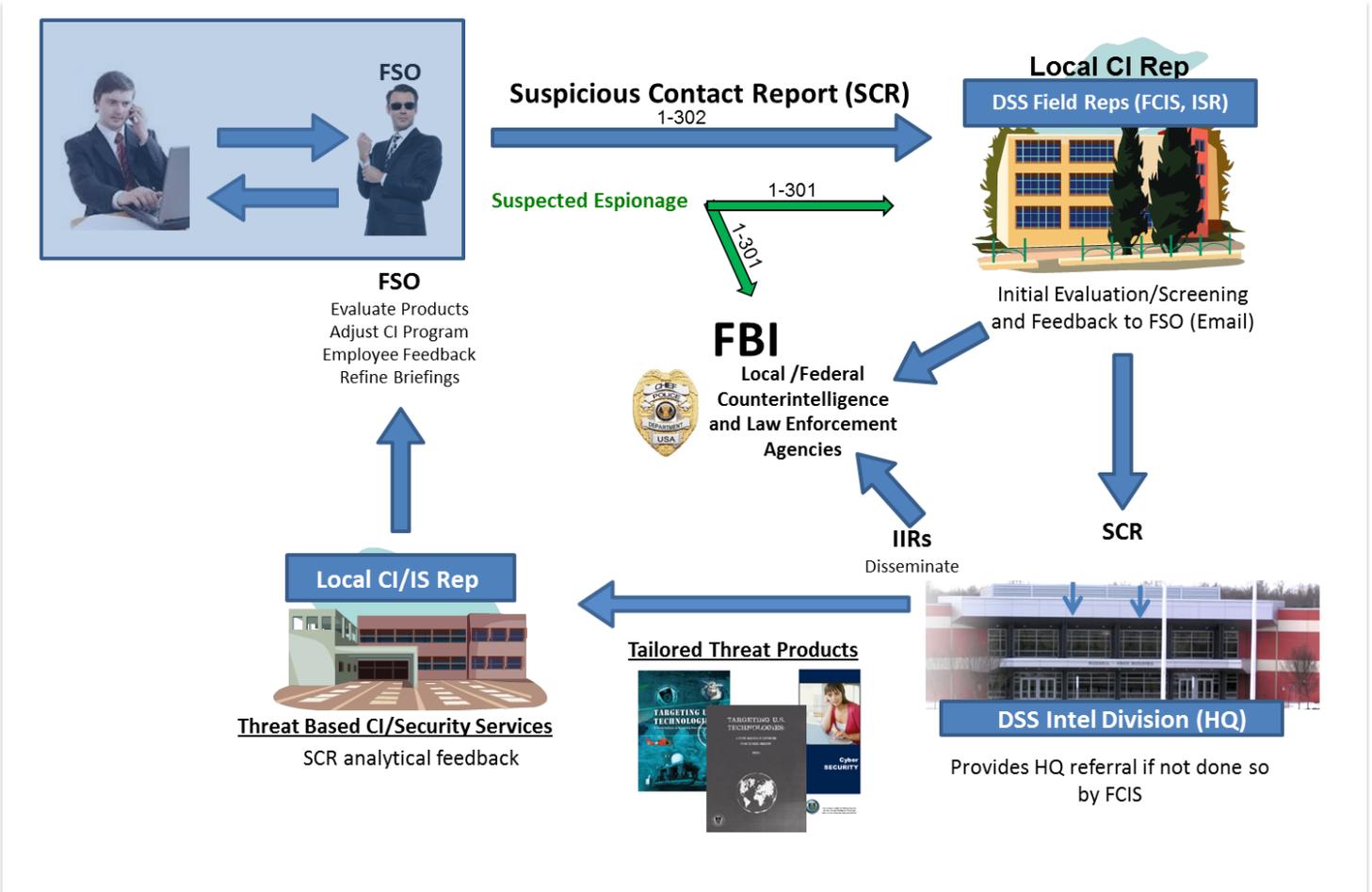
- This Briefing
- Foreign Visitors
- Foreign Travel
- Arranging Briefings
- CI Support

Visit DSS's web page for additional educational material on the threat to you and Industry:

WWW.DSS.MIL

Lifecycle of an SCR

SCR Lifecycle



First, Last, and Only (FLO)

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