DCSA/CDSE/ISOO Resources

CONTENTS OF THIS REFERENCE:

- DCSA website “Limited Access Authorizations for Non-U.S. Citizens”
- DCSA VRO Job Aid – Digital Signatures on the SF 312 (2/20/24)
- ISOO Notice 2017-04, Security Classification Guides
- DSCA Small Business Guide – Facility Clearance Process
- CDSE Industrial Security Job Aid – Reporting Requirements (no date)
- CDSE FSO Curricula Brochure (no date)
- DCSA CI Flyer – Cyber Threats
- DCSA CI Flyer – Elicitation
- DCSA CI Flyer – Personal Contact
- DCSA CI Flyer – Preparing for Foreign Visitors
- DCSA CI Flyer – Targeting during Conferences, Conventions, and Trade Shows

DCSA

DCSA website “Limited Access Authorizations for Non-U.S. Citizens”

RETURN TO PAGE 1

Limited Access Authorizations (LAA) for Non-U.S. Citizens

Non-U.S. citizens do not qualify for a security clearance. However, if a non-U.S. citizen requires access to U.S. classified information and meets the requirements of the 32 Code of Federal Regulations (CFR) 117.10(k), a Limited Access Authorization (LAA) no higher than the Secret level may be issued. An LAA enables a non-U.S. citizen to have limited access to classified information, but the LAA is not a national security eligibility. Access to classified will be limited to a specific program or project and will be cancelled upon the completion of the program or project for which it was approved. Access to classified information outside the scope of the approved LAA shall be considered a compromise of classified information. Access to classified information provided to the U.S. Government by another government or international organization will not be permitted under an LAA without the written consent of the government of the organization that provided the information.

If no U.S. classified access is needed but the subject requires area access, the request must be electronically submitted to the appropriate GCA.

Prior to submitting an application for an LAA, the contractor must obtain a written disclosure determination from a principal or a designated disclosure official or obtain a State Department approved export license. The LAA cannot serve as an export authorization.

All LAA applications must include a completed DD Form 3134 endorsed by the program executive officer or equivalent official responsible for the contract.

The **DD Form 3134** along with proof of foreign citizenship (i.e. passport), copy of disclosure determination or export license, and foreign security clearance certificate (if available) must be sent to DCSA via DoD Safe Access File Exchange, via fax to 571-305-6010, or email a scanned and secured pdf to **dcsa.iab@mail.mil**. A copy of the approved Technology Control Plan (TCP) must be submitted to our office prior to the LAA being granted.

Upon notification from DCSA that the application has been approved, the FSO will initiate an SF-86. The SF-86 should be electronically submitted as a Tier 5 investigation request for an LAA even though "Secret" is the highest level of access permitted. In addition, if the subject has lived outside the U.S. within the past ten years, separate security forms for applicable countries may need to be completed as well.

The FSO shall notify DCSA if there are any changes to the subject's personnel security records, such as change in contract number, citizenship status, or any adverse information.

If you have any additional questions regarding LAAs, please contact the DCSA at **dcsa.iab@mail.mil**.

Reference: DoDM 5200.02 Procedures for the DoD Personnel Security Program
Reference: 32 Code of Federal Regulations (CFR) 117.8(c3)
Reference: 32 Code of Federal Regulations (CFR) 117.11(h1)
Reference: 32 Code of Federal Regulations (CFR) 117.10(k)

Taken from the DCSA website under Industrial Security -> International Programs -> Security Assurances for Personnel and Facilities

https://www.dcsa.mil/Industrial-Security/International-Programs/Security-Assurances-for-Personnel-Facilities/

RETURN TO PAGE 1

DCSA
VRO

DCSA VRO Job Aid – Digital Signatures on the SF 312 (2/20/24)

RETURN TO PAGE 1

VRO Vetting Risk Operations

20 February 2024

Job Aid for Digital Signatures on the Standard Form 312

The purpose of this document is to provide a job aid to support the National Industrial Security Program (NISP) contractors on the 27 September 2023, Office of the Under Secretary of Defense for Intelligence and Security (OUSD I & S) memorandum, "Use of Digital Signatures on Standard Form 312".

There are four key points to highlight:

- Effective 20 February 2024, VRO will accept digitally signed SF-312s.
- The use of digital signatures on the SF-312 is **optional**. Manual or "wet" signatures will still be accepted by VRO.
- If the Subject digitally signs the SF-312, the witness block does not require a signature.
- VRO will accept an SF-312 with a combination of digital and manual signatures.

Public Lists of DoD Sponsored/Approved External Certificate Authority (ECA) Public Key Infrastructure (PKI)

- The public list of DoD sponsored External Certificate Authorities (ECA) Public Key Infrastructure (PKI) that are authorized to digitally sign the SF-312 can be located at https://public.cyber.mil/eca/.
- The public list of DoD approved external PKIs that are authorized to digitally sign the SF-312 can be located at https://public.cyber.mil/pki-pke/interoperability/.

Frequently Asked Questions

1. **Where can I find a copy of the SF-312 that allows for digital signature?**
   A copy of the SF-312 can be found here: https://www.gsa.gov/reference/forms/classified-information-nondisclosure-agreement-1

2. **Can a Subject use an Adobe Signature or DocuSign as a digital signature on the SF-312?**
   No, the Subject must use a DoD Common Access Card (CAC), DoD sponsored ECA PKI or DoD approved external PKI. The public facing websites with the list of those options are provided above.

3. **I have an Adobe signature created from my DoD sponsored/approved ECA PKI file. Does that qualify as an acceptable signature?**
   Yes, that qualifies as an acceptable signature. The website for the public list of DoD sponsored/approved ECA PKI is listed above.

4. **If the Subject uses a digital signature, is a Witness signature required?**
   No witness signature is required; however, a digital or manual signature is required in the Acceptance block.

5. **If the Subject uses a digital signature, is the Date, Social Security Number (SSN) and Organization still required?**
   Yes, please ensure the Subject fills out the Date, SSN and Organization information.

RETURN TO PAGE 1

6. **Can the Witness Signature (if required) be digital?**
   Yes, the Witness Signature on the SF-312 can be digital if it is on the list of DoD sponsored/approved ECA PKIs, listed above.

7. **Is the Acceptance Signature required if the Subject signs digitally? Can the Acceptance signature be digital?**
   The Acceptance signature is required on all SF-312s, regardless if the Subject signed digitally or manually. The Acceptance signature can either be digital or manual. If it is digital, please ensure the digital signature used is on the list of DoD sponsored/approved ECA PKIs.

8. **If the Subject signs the Debriefing Acknowledgement digitally, is there a requirement for a witness?**
   If the Subject signs digitally, there is no need for a witness because of the authentication, consent and integrity provided by the digital signature. Please ensure the digital signature is on the list of DoD sponsored/approved ECA PKIs.

9. **Do I need to submit a new SF-312 if my employee has previously signed an SF-312?**
   No, if the individual has signed an SF-312 previously, there is no need to sign a new one. To determine if an SF-312 was signed previously, login to DISS JVS and review the Subject Summary screen. A date will be listed on the NDA Signed Date if the individual has signed an SF-312.

Process Flow with Subject using Digital Signature

1. Subject signs the SF-312 digitally.
2. Witness Signature is NOT required.
3. Acceptance Signature is required (digitally or manually).
4. SF-312 is uploaded into DISS.

Process Flow with Subject using Manual Signature

1. Subject signs the SF-312 manually.
2. Witness Signature IS required (digital or manual).
3. Acceptance Signature is required (digital or manual).
4. SF-312 is uploaded into DISS.

RETURN TO PAGE 1

ISOO Notice 2017-04

Security Classification Guides

RETURN TO PAGE 1

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO Notice 2017-04: Security Classification Guides

September 14, 2017

1. The purpose of this notice is to reiterate the current requirements for security classification guides and to recommend a standard format for the guides to promote standardization and consistency for security classification guidance throughout the executive branch.

2. Executive Order (E.O.) 13526, Sec. 2.2, states that agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. In accordance with 32 CFR 2001.15, classification guides shall, at a minimum:

(1) Identify the subject matter of the classification guide;
(2) Identify the original classification authority by name and position, or personal identifier;
(3) Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;
(4) Provide the date of issuance or last review;
(5) State precisely the elements of information to be protected;
(6) State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;
(7) State, when applicable, special handling caveats;
(8) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.4 of the Order; and
(9) Prescribe a specific date or event for declassification, the marking ''50X1–HUM'' or ''50X2–WMD'' as appropriate, or one or more of the exemption codes listed in 2001.26(a)(2), provided that:
(i) The exemption has been approved by the Panel under section 3.3(j) of the Order;
(ii) The Panel is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and
(iii) The exemption code is accompanied with a declassification date or event that has been approved by the Panel.

3. To promote standardization and consistency for security classification guidance throughout the executive branch, ISOO is recommending a standard format for guides. ISOO also recommends the use of enhancement statements to indicate why the information must be protected, the damage impact of unauthorized disclosure, and how the information could be stated in an unclassified format. This is additional information that helps users manage risk and develop more useful security classification guidance. Enhancement statements can be applied to as many elements of information as necessary:

RETURN TO PAGE 1

Value: explains why the information is being protected.

Damage: describes the potential impact to national security should an unauthorized disclosure occur.

Unclassified statement: outlines how a user can address a classified item in an unclassified manner.

Example: (markings for training purposes only)

Line #	Element of Information	Classification Level	Reason (1.4)	Duration of Classification	Dissemination Controls	Remarks
2	Speed of aircraft	Secret	1.4(a)	25 years	N/A	
VALUE:						
DAMAGE:						
UNCLASSIFIED STATEMENT: [only used if the element of information itself is classified and you need to be able to describe it in an unclassified way]						

Note: Caveats (ex. REL TO, NOFORN, RD, etc.) may be annotated with the Classification Level, in the Remarks section, or as a Dissemination Control.

4. Security classification guides must be reviewed and updated as necessary, but at least every five years. To alleviate the burden of the review process, we recommend you spread out the review over the five year period, e.g. review approximately 20 percent of your guides each year.

Please direct any questions regarding this ISOO Notice to: isoo@nara.gov.

Mark A. Bradley

MARK A. BRADLEY
Director

RETURN TO PAGE 1

DCSA

Small Business Guide -

Facility Clearance Process

RETURN TO PAGE 1

What is a Facility Clearance (FCL)?

A FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the FCL granted to the facility.

Who Can Sponsor a Facility for a FCL?

A government contracting activity (GCA) or a currently Cleared Defense Contractor (CDC) may sponsor an uncleared company for an FCL.

The sponsorship package should include the following:

- Justification demonstrating bona fide procurement requirement to access classified information. Most common form is DD Form 254.
- Written GCA or Intelligence Community (IC) Authorization.
- Statement of Work (SOW)/Performance Work Statement (PWS): Highly recommended that a contract or subcontract specific SOW or PWS be included.

Considering Starting a Joint Venture (JV) ?

With new Mentor-Protégé Programs available to small businesses, more joint ventures are being considered. If you form a JV that is awarded a classified contract, the JV entity will require a FCL. This applies to all JVs, regardless if the separate entities of the JV currently hold a FCL.

There also can be confusion associated with populated and unpopulated JVs. The Facility Security Officer (FSO), the Insider Threat Program Senior Official (ITPSO), and the SMO Senior Management Official (SMO) must be employees of the organization holding the Facility Clearance. Therefore, the JV must have at least one employee who hold these positions. The SBA regulations, 13 CFR 121.103 (h) do allow a joint venture to have its own separate employees to perform administrative functions. Thus, a joint venture may be populated with employee(s) and still be considered an unpopulated joint venture so long as these employees are not performing the contracts awarded to the joint venture.

TIP: *When forming a JV, review the security requirements of the contracts you will be bidding on and ensure FCL sponsorship and timelines are considered.*

RETURN TO PAGE 1

Defense Security Service

Small Business Guide

Facility Clearance Process

www.dss.mil

The FCL Process

Submit Sponsorship Package

Submit a Sponsorship Package to DSS, via National Industrial Security System (NISS)

It must include:

1.Justification (ex. DD254)

2.Written GCA or IC Authorization

3. SOW/PWS

DAY 1

Sponsorship Package Accepted

- Package accepted by DSS and you receive a welcome email with your specific deadlines and instructions
- Within 5-10 days a telephonic survey is conducted to discuss your specific situation

DAY 20

Submit Business Documents via NISS

- Once the complete FCL package is submitted, your assigned Industrial Security Representative (IS Rep) from your local field office will review the package. If the package is complete, the IS Rep will forward the package for additional internal reviews and notify FCB to process any Key Management Personnel (KMP) personnel security clearances that are needed

DAY 45

Submit KMP Clearance Documents

- Completed Electronic Questionnaire for Investigations Processing (e-QIP)
- Electronic Fingerprints
- Verification of current clearance as applicable

Facility Clearance Issued

IMPORTANT: Waiting until the last day on these timelines could potentially lead to the process being discontinued if the timelines are not met or correct documents are not provided. In those instances, the company will have to be re-sponsored and the process begins all over again so timeliness and quality are paramount.

TIP: *Due to review and coordination timeframe, this may require a quick turnaround to complete e-QIPs. Search the Standard Form 86 PDF on any search engine to start collecting the information that you will need to upload into the e-QIP prior to it being released to you.*

How long will the whole process take?

- It depends on the individual situation. The two main hold points in the process that add time are processing of Personnel Clearances (PCL) for Key Management Personnel (KMP) and mitigations for businesses with Foreign Ownership or Controlling Interest (FOCI). Interims are granted, when possible, to allow contractors to begin performance.

- *Example:* If you are a business where the KMP currently holds an active personnel clearance at the level required by the contract and have no FOCI then the process will most likely go faster. The same is likely for two cleared businesses that form a Joint Venture (JV) and require the JV to be cleared.

TIP: *Please note that the biggest opportunity to expedite your Facility Clearance Process is in being prepared to provide the required information and documentation quickly at each stage of the process.*

RETURN TO PAGE 1

Tips for Small Businesses

- Cleared contractors can process individual consultants for a PCL and NOT a FCL when the consultant and immediate family members are the sole owners and only the consultant requires access to classified information. **Be aware of this when looking into subcontracting opportunities!**
- DSS Facility Clearance Branch (FCB) cannot adjust agency contract requirements that require a FCL at time of bid. If you have a concern, engage with the agency directly.
- The government funds the processing of PCLs and FCLs for access to classified information. The only cost to you to go through the process is to ensure the business is in compliance with the National Industrial Security Program Operating Manual (NISPOM).
- Leverage your business relationships and small business status to find subcontracting opportunities that will sponsor your business.
- See back flap for important information on joint ventures.

Resources Available to you:

- Visit www.DSS.mil to view a detailed and very helpful handbook on the FCL process, FCL checklist, FAQs, NISPOM.
- **Call the DSS Knowledge Center at 888-282-7682 and select option #3 for all FCL-related questions or status updates on your submission.**
- Visit www.CDSE.edu for FREE training, toolkits, job aids, security shorts and more such as FSO training, FSO Toolkit, and Merger/Acquisition/Reorganizations Job Aids.

CDSE

CDSE Industrial Security Job Aid –

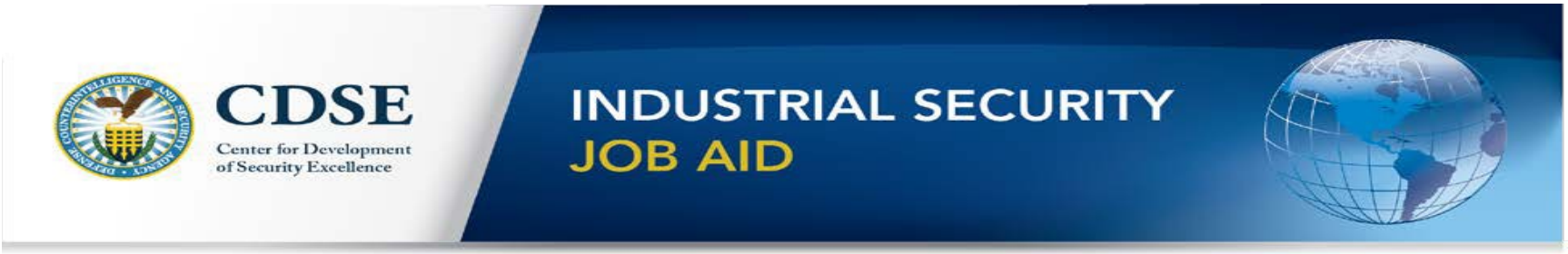
Reporting Requirements (no date)

RETURN TO PAGE 1

This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Espionage Sabotage Terrorism Subversive Activities	Any known information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of the contractor's sites	In writing. If the matter is urgent, the initial report may be made by phone and must be followed up in writing (i.e., email, formal correspondence). When a report is made to the Federal Bureau of Investigation (FBI), promptly notify your Industrial Security Representative (IS Rep) at the Defense Counterintelligence and Security Agency (DCSA) Field Office and provide a copy of the written report.	FBI Notify and provide copy of written report to IS Rep
Adverse Information	Any information that negatively reflects on the integrity or character of a cleared employee, that suggests his or her ability to safeguard classified information may be impaired, that his or her access to classified information may not be in the interest of national security, or that the individual constitutes an insider threat. Reporting should be based on references in SEAD 4, National Security Adjudicative Guidelines. Some examples include: • Allegiance to the United States • Foreign influence/preference • Personal conduct • Financial considerations • Drug involvement/substance misuse • Criminal conduct • Use of information technology *Do not report information based on rumor or innuendo.*	Appropriate function in the DOD Personnel Security System of Record (i.e., Incident Report in Defense Information System for Security (DISS))	Adjudication and Vetting Services (AVS)

RETURN TO PAGE 1



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Change in Status of Employee Determined Eligible for Access to Classified Information	The following changes in the personal status include: • Death • Change in name • Termination of employment • Change in citizenship	Enter changes as applicable in the DOD Personnel Security System of Record (i.e., DISS)	AVS
Citizenship by Naturalization	If a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization, the report will include: • City, county, and state where naturalized • Date naturalized • Court • Certificate number	Appropriate function in the DOD Personnel Security System of Record (i.e., Customer Service Request (CSR) in DISS)	AVS
Employees Desiring Not to Be Processed for a National Security Eligibility Determination or Not to Perform Classified Work	• Any employee who no longer wishes to be processed for a determination of eligibility for access to classified information • Any employee who no longer wishes to continue having access to classified information	Enter the reason in the appropriate function in the DOD Personnel Security System of Record (i.e., CSR in DISS)	AVS
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Refusal to sign Standard Form (SF) 312 Classified Information Nondisclosure Agreement (NDA)	An employee refuses to sign the SF 312, Classified Information NDA, or other approved NDA	Enter the reason in the appropriate function in the DOD Personnel Security System of Record (i.e., CSR in DISS)	AVS
Individual Culpability	The determination of an individual's responsibility for a security violation can be determined when one or more of the following factors are evident: • Deliberate disregard of security requirements	Appropriate function in the DOD Personnel Security System of Record (i.e., Incident Report in DISS)	AVS

RETURN TO PAGE 1

This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

	• Negligence in the handling of classified material • A pattern of questionable judgement, irresponsibility, negligence, or carelessness Report should include: • Statement of the administrative actions against the employee • Details of the incident(s)		
Suspicious Contacts	• Efforts by any individual, regardless of nationality, to gain illegal or unauthorized access to classified information • Efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact that suggests the employee may be the target of an attempted exploitation by an intelligence service of another country • All contacts by employees determined eligible for access to classified information with known or suspected intelligence officers from any country	In writing	IS Rep and Counterintelligence Special Agent (CISA)

Changed Conditions Affecting the Contractor's Eligibility for Access to Classified Information (e.g., Facility Clearance (FCL))	• Change of ownership or control
	• Change of operating name or address
	• Change to information previously submitted for Key Management Personnel (KMP)
	• Any action to terminate business or operations
	• Any material change concerning information previously reported as Foreign Ownership, Control, or Influence (FOCI)
	  ○ Submit a revised Certificate Pertaining to Foreign Interests (SF 328)
	  ○ Submit a copy of Schedule 13D, if received
		FCL System of Record (i.e., National Industrial Security System (NISS))	IS Rep (via NISS)

RETURN TO PAGE 1

This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

Changes in Storage Capability	Any change in the facility's storage requirement or capability to safeguard classified material	In writing	IS Rep
Inability to Safeguard Classified Material	Any emergency that renders the facility (or their location) incapable of safeguarding classified material	In writing	IS Rep
Unsatisfactory Conditions of a Prime or Subcontractors	Any information that indicates classified information cannot be adequately protected by a prime or subcontractor, or other circumstances that may impact the eligibility for access to classified information by any prime or subcontractors	In writing	IS Rep
Reporting by Subcontractor	Subcontractors will also notify their prime contractors if they make any reports to their Cognizant Security Agency (CSA).	In writing	IS Rep and Prime Contractor
Dispositioned Material Previously Terminated	When the location or disposition of classified material previously terminated from accountability is subsequently discovered and brought back into accountability	In writing	IS Rep
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Improper Receipt of Foreign Government Material	The receipt of classified information from foreign interests that is not received through U.S. Government channels. Report should identify: • Source (sender) • Originator (generated material) • Quantity (pages, volumes) • Subject or title • Date material was generated • Classification level (markings)	In writing	IS Rep
Employee Information in Compromise Cases	Report upon request of CSA only; information concerning an employee in connection with the loss, compromise, or suspected compromise of classified information	In writing	IS Rep
Foreign Classified Contracts	Any pre-contract negotiation or award not placed through the CSA or U.S. Government Contracting Activity (GCA) that involves or may involve:	In writing	IS Rep

RETURN TO PAGE 1

This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

	• The release or disclosure of U.S. classified information to a foreign interest • Access to classified information furnished by a foreign interest		
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Loss, Compromise, or Suspected Compromise	The loss, compromise, or suspected compromise of classified information, U.S. or foreign. If the preliminary inquiry finds no compromise, then the completed inquiry should be filed until it can be examined by your IS Rep on the next facility security review.	In writing (initial and final report)	IS Rep
Cyber Incident Reports	Any cyber incident on a classified, covered information system that has been approved by that CSA to process classified information	In writing	IS Rep
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Foreign Travel (UNOFFICIAL)	Prior approval of unofficial foreign travel is required to be reported. • The cleared employee notifies the cleared contractor (e.g., FSO or assigned designee) before foreign travel. If notification does not occur in advance, the covered individual must notify the cleared contractor as soon as possible after the travel occurs, not to exceed five business days • The cleared employee submits a complete travel itinerary to the cleared contractor, and the cleared contractor reports the travel prior to the unofficial foreign travel • The cleared contractor provides the covered individual with the National Counterintelligence and Security Center (NCSC) “Safe Travels” resource • The cleared contractor coordinates with a DCSA CISA	Appropriate function in the DOD Personnel Security System of Record (i.e., Foreign Travel in DISS) and, if applicable, in writing	AVS and, if applicable, CISA

RETURN TO PAGE 1

This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE Facility Security Officer (FSO) Toolkit).

	for appropriate pre-foreign travel briefings when the covered individual is traveling to a foreign country listed in the Director of National Intelligence's Worldwide Threat Assessment of the U.S. Intelligence Community		
Foreign Contacts (UNOFFICIAL)	Any contact with a foreign national involving the exchange of personal information A reportable instance involving an exchange of personal information with a foreign national would meet the following criteria: • The name and nationality of the foreign national are known by the cleared individual during or after the exchange of personal information • The nature of the personal information provided by the cleared individual to the foreign national is not reasonably expected to be accessible by the general public, nor to be willingly released to the general public by the cleared individual • Contact with the foreign national is re-occurring or expected to re-occur	Appropriate function in the DOD Personnel Security System of Record (i.e., CSR in DISS)	AVS

RETURN TO PAGE 1

CDSE

Facility Security Officer (FSO) Curricula

RETURN TO PAGE 1

HOW TO REGISTER

Registration is easy; simply register for the appropriate curriculum and you will automatically be registered for all courses and examinations within that curriculum.

When you complete all courses within the curriculum, you will be able to print a curriculum certificate of completion. You may also print certificates of completion for each individual course you successfully complete within the curriculum.

CREDIT RECOMMENDATIONS

The American Council on Education's College Credit Recommendation Service (ACE CREDIT) has evaluated and recommended three lower-level division baccalaureate/associate degree category semester hours in strategic security for both the **FSO Orientation for Non-Possessing Facilities Curriculum** *(IS020.CU)* and the **FSO Program Management for Possessing Facilities Curriculum** *(IS030.CU)*.

For decades, colleges and universities have trusted ACE CREDIT to provide reliable course equivalency information to facilitate their decisions to award academic credit.

For more information, visit the ACE CREDIT website at **www.acenet.edu/credit/**.

To see the Center for Development of Security Excellence displayed in the ACE National Guide, go to **www.acenet.edu/national-guide/.** Scroll down to "Browse Organizations" and select "C."

WHO SHOULD REGISTER?

Personnel that will serve as the FSO at a facility participating in the NISP.

The curriculum is also suitable for training other security professionals such as:

- Insider Threat Program Senior Officials (ITPSOs)
- Assistant FSOs
- Program Managers
- Contractor Executives
- Industrial Security Specialists
- Government Security Specialists
- Security Administrators
- Program Security Managers

PROGRAM CONTACT INFORMATION

If you have questions regarding this curriculum, please email **dcsa.cdsetraining@mail.mil.**

Revised September 2022

Center for Development of Security Excellence
938 Elkridge Landing Road | Linthicum, MD 21090
www.cdse.edu

RETURN TO PAGE 1

Facility Security Officer (FSO)

CURRICULA

FSO Orientation for Non-Possessing Facilities *(IS020.CU)* & FSO Program Management for Possessing Facilities *(IS030.CU)*

CDSE Center for Development of Security Excellence

PROGRAM DESCRIPTION

This program of study prepares individuals for the duties and responsibilities of an FSO in a contractor facility participating in the National Industrial Security Program (NISP).

Both the FSO Orientation for Non-Possessing Facilities (facilities without approved storage for classified material) and the FSO Program Management for Possessing Facilities (facilities with approval to store classified material) curricula comply with the FSO training requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

Successful completion of any of the previous versions of the required NISPOM FSO training satisfies the current NISPOM FSO training requirement unless advised otherwise by your Defense Counterintelligence and Security Agency (DCSA) Industrial Security Representative (IS Rep).

REQUIRED TRAINING FOR NEW FSOs

Possessing Facilities

To complete the FSO Program Management for **Possessing Facilities Curriculum** *(IS030.CU)*, students must complete the following courses and examinations:

IS011.16	Introduction to Industrial Security
IF011.16	Introduction to Information Security
IS140.16	Facility Clearances in the NISP
IS065.16	Understanding Foreign Ownership, Control or Influence (FOCI)
IS150.16	NISP Reporting Requirements
IS142.16	Personnel Clearances in the NISP
IS105.16	Visits and Meetings in the NISP
GS104.16	Developing a Security Education and Training Program
CI117.16	Protecting Assets in the NISP
IS130.16	NISP Self-Inspection
IS109.16	Safeguarding Classified Information in the NISP
IF103.16	Derivative Classification
IF105.16	Marking Special Categories of Classified Information
IS107.16	Transmission and Transportation for Industry

Non-Possessing Facilities

To complete the FSO Orientation for **Non-Possessing Facilities Curriculum** *(IS020.CU)*, students must complete the following courses and examinations:

IS011.16	Introduction to Industrial Security
IF011.16	Introduction to Information Security
IS140.16	Facility Clearances in the NISP
IS065.16	Understanding Foreign Ownership, Control or Influence
IS150.16	NISP Reporting Requirements
IS142.16	Personnel Clearances in the NISP
IS105.16	Visits and Meetings in the NISP
GS104.16	Developing a Security Education and Training Program
CI117.16	Protecting Assets in the NISP
IS130.16	NISP Self-Inspection

RETURN TO PAGE 1

DCSA

DCSA CI Flyer - Cyber Threats

RETURN TO PAGE 1

WHAT TO REPORT

- All cyberthreats
- Aggressive port scanning outside normal network noise
- Advanced techniques / evasion techniques
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained storage of encrypted data
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltration
- Malicious codes or blended threats
- Unauthorized email traffic to foreign destinations
- Use of Department of Defense (DoD) account credentials by unauthorized parties
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or CUI
- Any cyberactivity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

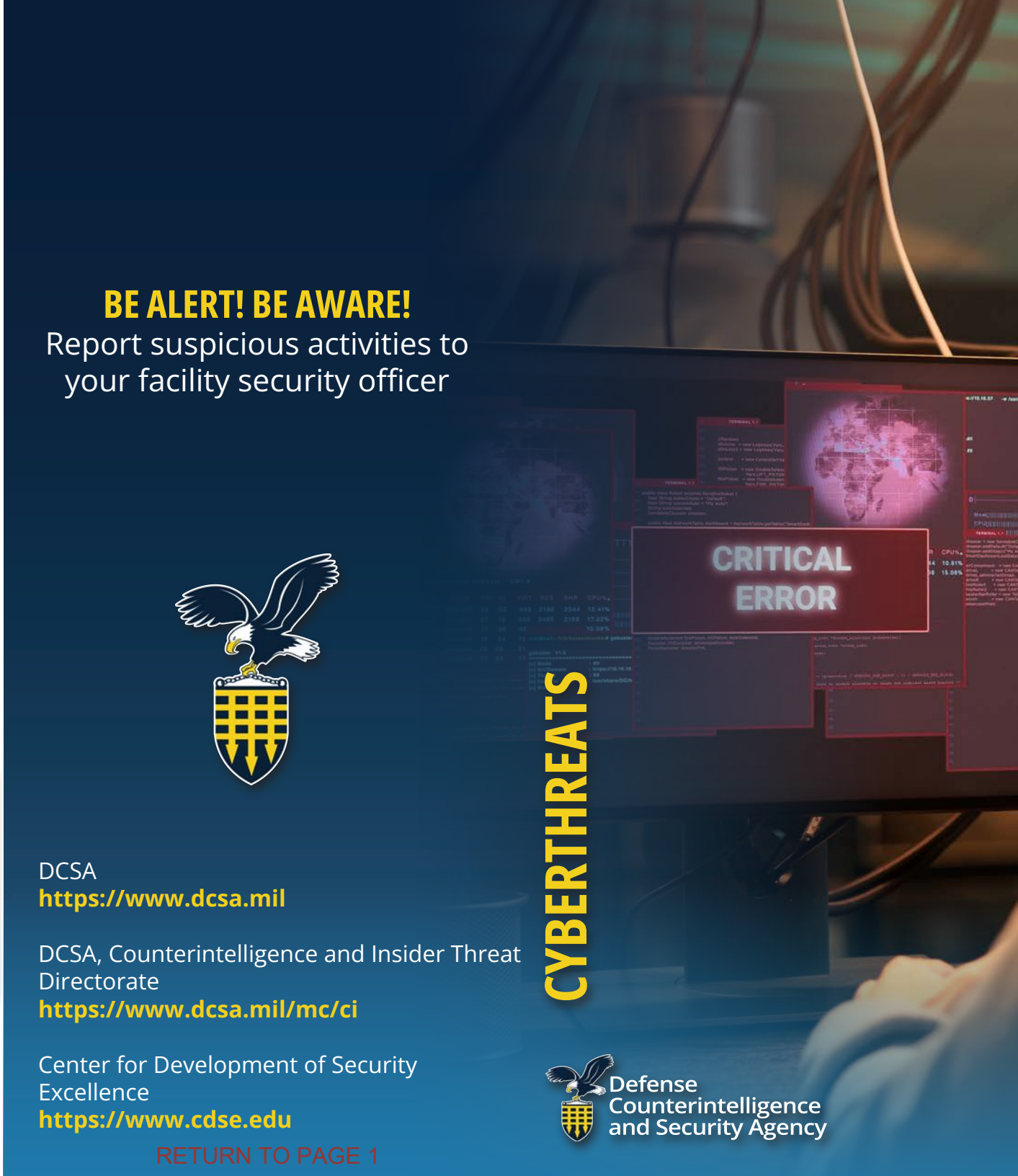
REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer



CYBERTHREATS

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence and Insider Threat Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

RETURN TO PAGE 1

Defense Counterintelligence and Security Agency

WHAT ARE CYBER THREATS?

Our nation's cyberthreats have tools and tricks from a multitude of resources, including publicly available information on the Internet. This makes it difficult to differentiate between criminal and intelligence entities, exacerbated by the ease with which adversaries can obtain information about potential targets. We live in a world where the Internet of Things includes computers, cell phones, Smart TVs, Alexa, Ring, watches, satellite radio, refrigerators, and window shades.

WHO IS BEING TARGETED?

You

Any individual, cleared or uncleared, regardless of job title or position, who can be used to gain access to an unsuspecting organization's network

Your company

Any organization or company, cleared or uncleared, with access to information coveted by our nation's adversaries

WHAT IS BEING TARGETED?

- International Traffic in Arms (ITAR), export-controlled and critical technology, and controlled unclassified information (CUI)
- Research and development
- Company unclassified networks (internal and external), partner and community portals, commonly accessed websites, and unclassified search history
- Proprietary information
- Administrative and user credentials
- Patch update sequences/patterns

Foreign intelligence entities seek aggregates of CUI or proprietary documents which paint a classified picture.

HOW ARE YOU BEING TARGETED?

- **Information Gathering:** Harvesting information
- **Targeting:** Coupling exploit with delivery methods
- **Delivery:** Infecting the target commonly using email, website hijacking, and removable media
- **Exploitation:** Exploiting a vulnerability on a system to execute code
- **Installation:** Malware providing persistence on targeted network
- **Command and Control:** Remote access computers, networks, or software/firmware
- **Actions on the Objective:** Access targeted information, data, and technology

HOW ARE YOU VULNERABLE?

- Publicly available information
- Contract information
- Company websites with technical/program data
- Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or uncleared companies
- Employee association with companies or technologies made public through scientific journals, academia, social networking sites such as Facebook and LinkedIn, etc.

PERSISTENT AND EMERGING CYBER THREATS

- Deepfakes: Creating fake images, sounds, and videos to fool the viewer
- Poisoning Attacks: Malicious injection into artificial intelligence program while it is learning
- Ransomware: New tactics, techniques, and procedures to exfiltrate data and release to the public
- Supply chain vulnerabilities
- Unsecure security products
- Malicious code injection
- Botnets
- Brute force
- Social network sites
- Credential harvesting

COUNTERMEASURES

- Training
- Using complex passwords
- Educating employees on social networking and email targeting; phishing email signs and reporting
- Defense in depth
- Technical defenses
- Patch management
- Monitoring suspicious network activity
- Open lines of communication among facility security, counterintelligence (CI), and network defense personnel
- Having a failsafe relating to system administrators. One person should not have all of the "Keys to the Kingdom"
- Proper configuration–audit and automate secure configuration

"The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million."

Cost of a Data Breach Report 2023, IBM Security

RETURN TO PAGE 1

DCSA

DCSA CI Flyer - Elicitation

RETURN TO PAGE 1

WHAT TO REPORT

Elicitation is a suspicious contact reportable by cleared companies to the Defense Counterintelligence and Security Agency (DCSA) under the National Industrial Security Program (NISPOM).

EXAMPLES OF REPORTABLE ACTIVITY

- Any individual's efforts, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
- All contacts with known or suspected intelligence officers from any country
- Any contact that suggests an employee may be targeted for exploitation attempts by another country's intelligence services

Because elicitation is subtle and difficult to recognize, report suspicious conversations to your FSO, DCSA Industrial Security Representative, and DCSA Counterintelligence (CI) Special Agent. These individuals can assess the information and determine if a potential CI concern exists

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence and Insider Threat Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

RETURN TO PAGE 1

ELICITATION

Defense Counterintelligence and Security Agency

WHAT IS ELICITATION?

Elicitation is a structured method of communication to extract predetermined information; the subject is unaware they are a target.

The elicitor will attempt to conduct collection activities away from the target's work to be less security conscious to ease the elicitation process.

Because elicitation can sound like a common conversation, it is difficult to tell if it is a friendly conversation or intelligence gathering. Foreign intelligence entities look for professional and personal information to use in future targeting efforts.

Elicitation requires patience and persistence. Pieces of information, collected over an extended period, gives the adversary desired information about technology, programs, and processes.

HOW ARE YOU BEING TARGETED?

- **Exploitation of Tendency to Complain:** Statements such as "I am so behind at work" can elicit a cleared employee's response, divulging schedule setbacks, staffing shortfalls, resource shortages, and other valuable information to a foreign government or competitor
- **Questionnaires and Surveys:** An elicitor states a benign purpose for the survey and surrounds questions they want answered with logical questions
- **Feigning Ignorance:** An elicitor portrays ignorance to have the target instruct them about a topic. This tactic is frequently employed in academia; it exploits the habit of teaching and puts the target in a familiar mindset to share information
- **False Statement:** An elicitor knowingly makes a false statement so the target can correct them. Another example is citing someone else's research or paper; this is particularly effective if the target is knowledgeable about the study/research area
- **Flattery:** Statements such as "That thing is really cool" can elicit numerous responses by leading the target to converse about topics of interest
- **Quid Pro Quo or Trading Confidences:** The elicitor provides the target with valuable information. Conversations begin, "I shouldn't tell you this but" or "This is off the record." This induces the target to return the favor and provide valuable information. Espionage may look more like a business transaction and less like gathering information
- **Paper Review:** Many cleared employees have ties to academia and research institutions. Cleared employees regularly receive requests to peer review research or theses. Many requests are straightforward, but some are attempts to leverage sensitive or classified research
- **Bracketing:** An elicitor asks a target about a sensitive value using high and low values, rather than asking for a specific number. The elicitor asking if the range is somewhere between 10 and 15 kilometers garners a response such as "Yes, in the high end." Bracketing allows the elicitor to adjust the bracket for the next target
- **Oblique Reference or Analogies:** An elicitor discusses a topic similar to the target's work so the target will use their work to make a point of reference. An example is the elicitor discussing a foreign or civilian system similar to the target's work. The target is likely knowledgeable and comfortable discussing this topic. The target may slip and use their own sensitive system as a point of reference to the foreign system
- **Criticism:** Criticism is accomplished by criticizing the target. An example is statements such as, "I saw on the news" or "I heard," followed by a statement that criticizes the cleared employee's work, company, or project. Many people will defend things they feel passionate about

WHY IS ELICITATION EFFECTIVE?

Elicitors will try to exploit natural human tendencies:

- Desire to seem polite and helpful
- Desire to seem knowledgeable or well-informed
- Desire to seem competent
- Desire to feel appreciated and contribute to something important
- Gossiping
- Correcting others
- Underestimating information's value
- Believing others are honest
- Complaining
- Showing empathy
- Being indiscrete, especially when emotionally charged

COUNTERMEASURES

In the event you are targeted, be prepared to respond. Know what information you cannot share and be suspicious of those seeking information. Do not share anything the elicitor is not authorized to know, including personal information. If you believe someone is attempting to elicit information from you:

- Change the topic
- Refer them to public websites
- Deflect the question with one of your own
- Provide a vague answer
- Explain that you don't know, and respond with "Why do you ask?"

Consider: If you have to say "No" let your facility security officer know.

RETURN TO PAGE 1

DCSA

DCSA CI Flyer - Personal Contact

RETURN TO PAGE 1

WHAT TO REPORT

Personal contact is the vector for many intelligence methods of operation that constitute suspicious contact. Report any suspected instance of actual or attempted elicitation.

EXAMPLES OF REPORTABLE SUSPICIOUS CONTACTS

- Any individual's efforts, regardless of nationality, to obtain illegal or unauthorized access to sensitive or classified information or to compromise a cleared employee
- All contacts with known or suspected foreign IOs
- Any contact that suggests foreign intelligence services may be targeting an employee for exploitation
- Business contact requesting information outside contract/agreement scope
- Business/personal contact seeking information about your coworkers or job duties
- Business/personal contact requesting you to violate company policy or security procedures

Because elicitation can be subtle or requests from personal contacts seem harmless, report any suspicious conversations to your facility security officer or DCSA Counterintelligence (CI) representative.

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting CI threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence and Insider Threat Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

RETURN TO PAGE 1

PERSONAL CONTACT

Defense Counterintelligence and Security Agency

WHAT IS PERSONAL CONTACT?

Personal contact occurs when a foreign actor, agent, or recruiter is in direct or indirect contact with a target.

Foreign intelligence entities (FIEs) commonly use elicitation to collect intelligence through contact that appears routine. A FIE method of operation attempts to confirm or expand knowledge of a sensitive program or gain clearer insight into a person's placement and access (P&A) prior to possible recruitment.

WHO IS BEING TARGETED?

Anyone with access to classified or sensitive intelligence. FIEs target anyone with P&A to desired information, knowledge of information systems, or awareness of security procedures.

This includes:

- **Developers:** Research and apply new materials or methods to Department of Defense (DoD) programs and technologies
- **Technicians:** Operate, test, maintain, or repair targeted technologies
- **Production Personnel:** P&A to targeted technologies' production lines or supply chains
- **IT Personnel:** Access to targeted facility networks and knowledge of network security protocols
- **Business Development Personnel:** Marketing and sales representatives, business travelers
- **Human Resources Personnel:** Access to personnel records and job applicants
- **Facility Employees:** P&A to a cleared or sensitive facility containing targeted information, including security, clerical, maintenance, and janitorial personnel

HOW ARE YOU BEING TARGETED?

PRIMARY METHODS OF OPERATION

- Exploitation of Business Activities
- Exploitation of Insider Access
- Search/Seizure
- Exploitation of Security Protocols
- Request for Information (RFI)/Solicitation
- Exploitation of Relationships

HOW CAN YOU RECOGNIZE IT?

This approach is usually subtle. Some indicators include:

- Business contact requesting information outside contract scope or through an increased or gradual progression of information initiated from legitimate discussions
- Request to move communications to platforms outside official business channels, such as commercial chat
- Hidden/obscured end use/end user data
- Offer of paid attendance at an overseas conference; keynote or guest speaker invitations
- Casual acquaintance appears to know more about your work or project than expected
- Casual contact shows unusual interest in your work, facility, personnel, or family details

WHY IS PERSONAL CONTACT EFFECTIVE?

Foreign intelligence officers (IOs) are trained in elicitation tactics and operate without borders. Non-traditional collectors, such as business and academic contacts, leverage existing relationships to obtain restricted information outside the relationship scope. Not all elicitation attempts are obvious. IOs and non-traditional collectors assess and leverage the target's personal goals and vulnerabilities to elicit information.

Elicitation should be reported even if there is no intent to reconnect.

Trained IO elicitors and non-traditional collectors will try to exploit natural human tendencies, including:

- Being polite and helpful
- Appearing well-informed, especially about your profession
- Expanding discussion on a topic, likely giving praise or encouragement
- Correcting others
- Underestimating the value of information being sought or given
- Believing others are honest

COUNTERMEASURES

In the event a personal contact requests restricted information or attempts to place you in an exploitable situation, be prepared to respond. Know what information you cannot share and be suspicious of those who seek such information. Do not share anything the elicitor is not authorized to know, including personal information about yourself or coworkers. Outreach may occur via social media. Plan tactful ways to deflect probing or intrusive questions. Never feel compelled to answer any question that makes you uncomfortable.

If someone is attempting to elicit information:

- Change the topic
- Refer them to public websites
- Deflect the question
- Provide a vague answer
- Have a prepared canned answer
- State that you do not know

Consider: If you have to say "No" let your Facility Security Officer know.

RETURN TO PAGE 1

DCSA

DCSA CI Flyer - Preparing for Foreign Visitors

RETURN TO PAGE 1

WHAT TO REPORT

View as suspicious any line of questioning concerning military or intelligence-based contracts or dual-use technology, unless topics were previously approved.

Even if an appropriate authority grants a foreign visitor access to classified U.S. information, that visitor is not entitled to classified information unless he/she has cleared need-to-know that has been communicated and verified in advance of the visit.

Inform your DCSA Industrial Security Representative or DCSA CI Special Agent of proposed foreign visitors. Given adequate time, they can assist with identifying risks to the cleared company, its technology, and its personnel.

View as suspicious any attendee's effort to contact you before, during, or after the visit by phone, email, or social media.

If any suspicious incidents occur during the visit, report them to your facility security officer immediately.

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

RETURN TO PAGE 1

PREPARING FOR FOREIGN VISITORS

Defense Counterintelligence and Security Agency

PREPARING FOR FOREIGN VISITORS

Foreign visitors are common in today's global economy. Cleared contractors should be aware of potential counterintelligence (CI) vulnerabilities and threats.

While most visitors are here for legitimate purposes, the sheer volume of visitors makes it difficult to detect those with ulterior motives.

Foreign delegation visits to cleared contractor facilities are one of the most frequently used methods to target and attempt to gain access to controlled unclassified information (CUI) from cleared industry.

WHY DO FOREIGN ENTITIES TARGET U.S. CLEARED INDUSTRY?

It is cheaper for foreign entities to illicitly obtain CUI or classified information and technology than to fund initial research and development (R&D) themselves. The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D prime targets for foreign collection of classified and unclassified commercial technology.

When a foreign visit occurs at your facility, preparation and awareness are essential to preventing loss of information. Stay alert and watch for indicators to help assess the potential for visitor targeting or collection.

HOW ARE YOU BEING TARGETED?

- **Peppering:** Visitors ask a variation of the same question or one visitor asks the same question to multiple employees
- **Wandering Visitor:** The visitor uses the distraction provided by a large delegation to slip away, out of the escort's control. Once away from the escort, the visitor may try to access a restricted area, sensitive, or classified documents or unattended and unlocked information systems
- **Divide and Conquer:** Visitors corner an escort away from the group and attempt to discuss unapproved topics to remove the escort's safety net of assistance in answering questions
- **Switch Visitors:** Delegations may add a new visitor to the group at the last minute, leaving little or no time for the company to vet the new visitor against known intelligence officers
- **Bait and Switch:** The visitors plan to discuss one business topic, but after arriving, they attempt to discuss the cleared contractor's other projects, often dealing with CUI or classified information
- **Distraught Visitor:** When the visitor's questions are not answered, he/she acts insulted or creates an uncomfortable scene to psychologically coerce information from the target
- **Use of Prohibited Electronics:** The visitors bring unauthorized electronic devices such as cell phones, cameras, or thumb drives into restricted space

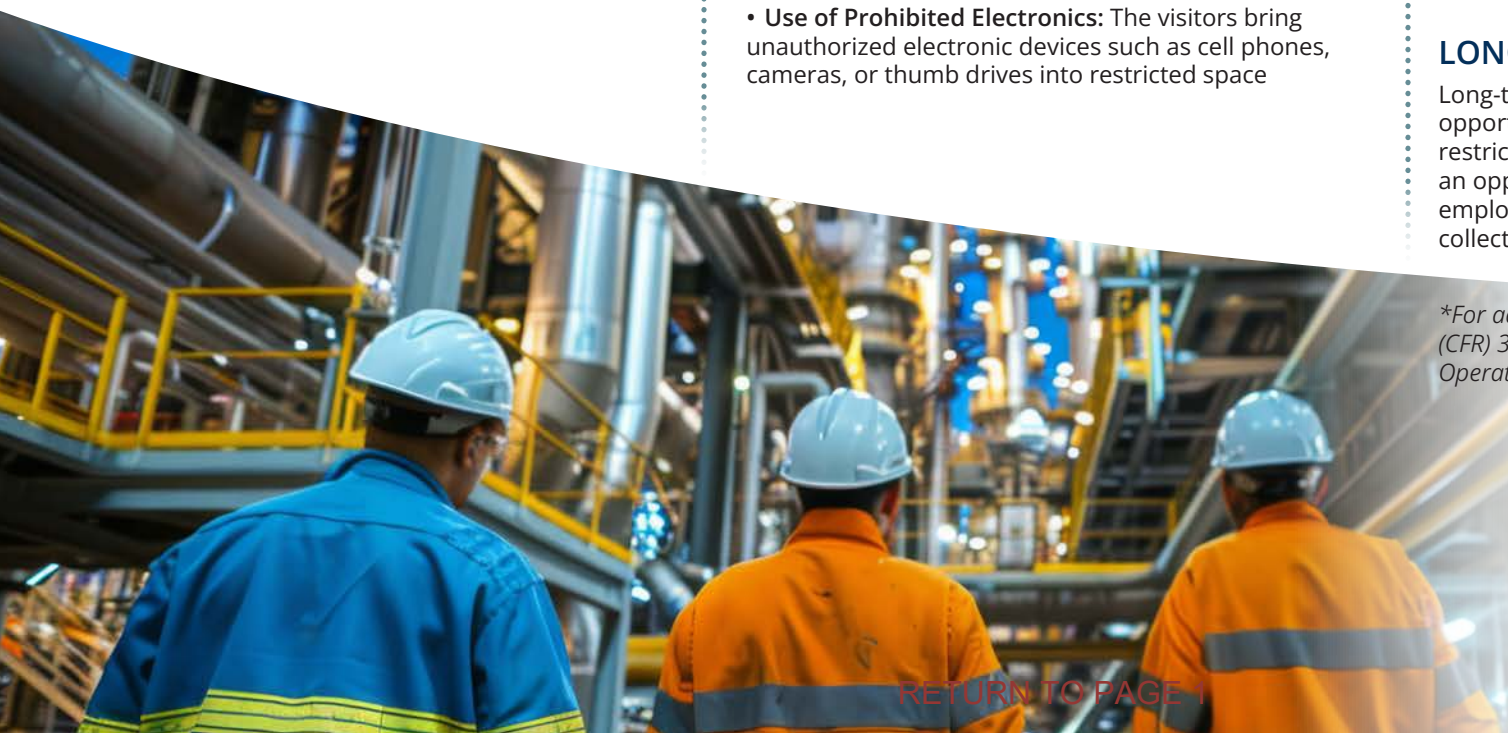
COUNTERMEASURES*

- Conduct a pre-visit facility walkthrough to ensure visitors cannot hear or see CUI, export-controlled information, or classified information during their visit
- Vet incoming foreign visitors with your supporting Defense Counterintelligence (DCSA) CI special agent
- Prior to the visit, brief all escorts and personnel working with the delegation on what they can and cannot discuss
- Develop standard, acceptable responses to questions that may arise, especially if projects are CUI or classified, are not applicable to the country visit, or include proprietary information
- Ensure there are enough escorts to properly support the number of visitors and escorts know where in the facility visitors can and cannot access
- Train escorts to detect suspicious behavior and questions, ensure they know to maintain visual contact with all visitors at all times, and develop contingency plans to handle visitors who leave the group
- If the delegation attempts to make additional contacts with escorts and speakers, ensure they limit discussions to the agreed-upon topics and information
- After the visit, debrief the host and all escorts to uncover if visitors exhibited any strange or suspicious activities or asked unusual and probing questions

LONG-TERM VISITS AND JOINT VENTURES

Long-term visits or joint ventures may provide an opportunity for a foreign long-term visitor to obtain restricted/proprietary information. They also provide an opportunity for visitors to spot, assess, and befriend employees that may assist, wittingly or unwittingly, in collecting restricted/proprietary information.

**For additional information, see Code of Federal Regulation (CFR) 32 Part 117 National Industrial Security Program Operating Manual (NISPOM).*



RETURN TO PAGE 1

DCSA

DCSA CI Flyer - Targeting During Conferences, Conventions, or Trade Shows

RETURN TO PAGE 1

WHAT TO REPORT

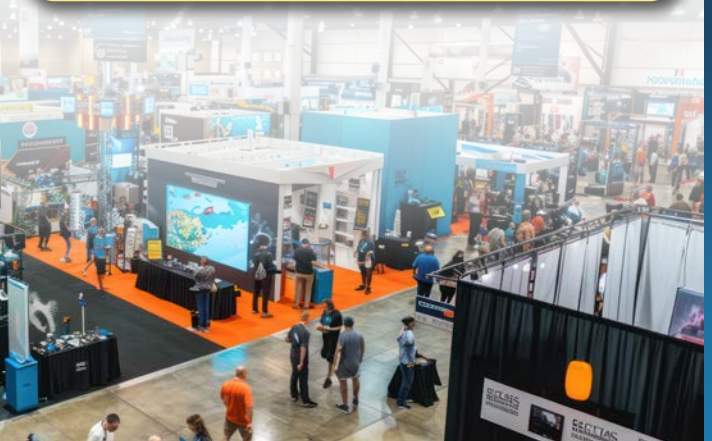
Immediately notify your facility security officer if you observe any of the following behaviors or believe you were targeted by an individual attempting to obtain information or technology they are not authorized to have:

- Offers to act as a foreign sales agent
- Attempts to steer conversations toward job duties or access to sensitive information or technology
- Insistent questioning outside the scope of what you are cleared to discuss
- Excessive photography/sketches, especially in areas that prohibit photography
- Individuals returning to the same booth multiple times to speak with different cleared employees
- Strangers trying to establish personal relationships outside work parameters
- Unusual or suspicious attempts at ongoing contact, including sending a follow-up email upon your return to the office
- Multiple individuals simultaneously asking questions, attempting to get you to reveal more than you should
- Theft of or missing items from your booth/display

REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.



BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADE SHOWS

DCSA
https://www.dcsa.mil

DCSA, Counterintelligence and Insider Threat Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

RETURN TO PAGE 1

Defense Counterintelligence and Security Agency

WHAT IS TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADESHOWS?

Conferences, conventions, or trade shows host a wide array of presenters, vendors, and attendees. This provides a permissive environment for foreign collectors, commercial rivals, start-up companies, intelligence officers, opportunists, and organized criminals to question vendors, develop business/social relationships, access actual or mockups of targeted technology, and interact with Subject Matter Experts (SMEs).

In 2019, nine percent of cleared industry reporting of suspicious contact-related activities occurred during attendance at conferences, conventions, or trade shows.

WHO IS BEING TARGETED?

Foreign collectors target anyone with access to targeted information and technology, or any SME in sought-after research or technology.

WHAT IS BEING TARGETED?

- Information, technical specifications, Department of Defense (DoD) plans, budgets/costs, system locations, and system pictures displayed at booths
- Information about cleared and uncleared employees to determine location to information, vulnerability to recruitment, and personnel interests to be used as pretext for future contact
- Physical or virtual access to company equipment
- Proprietary formulas and processes
- Blueprints and prototypes
- Research
- Vendor information
- Software information, i.e. source codes
- Company information – phone directories, corporate financial data, investment data, budgets, acquisitions, and sales

HOW ARE YOU BEING TARGETED?

Request for Information/ Solicitation

Exploitation of Experts

Search and Seizure

Surveillance

Foreign Intelligence Entities (FIEs) pose as potential customers, attendees, exhibitors, scientists, or as representatives of a nation other than their own.

Collectors attempt to elicit controlled unclassified information (CUI) and classified information through casual conversation during and after official events.

FIEs use these occasions to spot and assess individuals for potential recruitment. They use charm and/or potential business incentives to soften their targets.

During foreign travel, security personnel can subject attendees to search and seizure of documents and electronic devices, as well as surveillance at the venue, while socializing, and while in hotels.

HOW CAN YOU RECOGNIZE IT?

At conferences, conventions, or tradeshows you may witness:

- Attendees not wearing, or wearing incorrectly, IDs/badges
- Attempts to steal actual or mockups of technologies on display
- Photography of displays, especially when photography is explicitly prohibited
- Requests for information beyond the conference's scope
- Requests for the same information from different people during the conference
- Attempts to schedule post-event meetings or contact and attempts to develop personal friendships
- Attempts to contact you before, during, or after the meeting by phone, email, or social media

While traveling to and attending events, traditional intelligence officers will use the following techniques to obtain information about you, your work, and your colleagues:

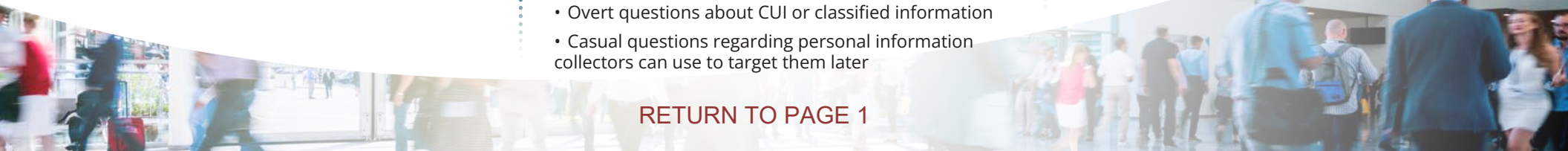
- Detailed and probing questions about specific technology
- Overt questions about CUI or classified information
- Casual questions regarding personal information collectors can use to target them later
- Prompting employees to discuss duties, access, or clearance level
- Attempts to access your electronic devices, i.e., laptop, smartphones

COUNTERMEASURES

- Display signage requesting no touching or photography of items on display
- Complete annual counterintelligence awareness training
- Attend security briefings and de-briefings
- Remain cognizant of your surroundings and anyone displaying increased interest in you or your exhibit
- At events, display mockups, not actual working versions of your product
- Do not leave technology, mockups, sensitive documents, or electronics unattended
- Create controlled access areas for sensitive displays that should not be touched or photographed
- Prepare responses for questions involving CUI or classified aspects of your product
- If your company provides WiFi for employees, create a strong password, and change it before and after each show
- Do not accept electronic gifts

WHEN ATTENDING EVENTS OVERSEAS

- Request a threat assessment from the program office and your local DCSA representative prior to traveling to an event overseas
- Use designated travel laptops that contain no CUI or exploitable information
- Do not use foreign computers or fax machines and limit sensitive discussions
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Do not post pictures or mention you are on travel on social media



RETURN TO PAGE 1