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.

PERSONAL CONTACT

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

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.