WHAT TO REPORT

Personal contact is the vector for many intelligence methods of operation that constitutes "suspicious contact." Report any instance where you suspect you may be the target 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 the 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, you should report any suspicious conversations to your facility security officer or Defense Counterintelligence and Security Agency (DCSA) Counterintelligence (CI) representative.

REPORTING REQUIREMENT

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

If you suspect you or your company are targeted, report it immediately, which is critical to disrupting CI threats and mitigating risks. Reporting allows us to share and address risks together. Report securely to your servicing DCSA CI Special Agent using encryption or DOD Safe.

DCSA
https://www.dcsa.mil

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

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

PERSONAL CONTACT

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DEFINING PERSONAL CONTACT

Person-to-person contact occurs by any means where the foreign actor, agent, or recruiter is in direct or indirect contact with the target.

Foreign intelligence entities (FIE) commonly use a method and technique called elicitation to collect intelligence through what appears as normal, even mundane, social or professional contact. An FIE method of operation attempts to confirm or expand their knowledge of a sensitive program or gain clearer insight into a person's placement and access (P&A) prior to possible recruitment.

PRIMARY METHODS OF OPERATION AND EXPLOITATION

This method of contact is associated with all methods of operation FIE apply when targeting cleared industry.

Those with the highest risk include:

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

WHO ARE THEY TARGETING?

YOU are at risk simply because YOU have access to classified or sensitive intelligence. FIE aggressive collectors will target anyone with P&A to desired information, knowledge of information systems, or awareness of security procedures.

This includes but is not limited to:

- **Developers:** Scientists, researchers, and engineers researching and applying new materials or methods to Department of Defense (DOD) programs and other leading-edge technologies
- **Technicians:** Engineers or specialists that operate, test, maintain, or repair targeted technologies
- **Production Personnel:** Personnel with P&A to targeted technologies' production lines or supply chains

- **IT Personnel:** Systems administrators or others with access to targeted facility networks and knowledge of network security protocols
- **Business Development Personnel:** Marketing and sales representatives, business travelers
- **Human Resources Personnel:** HR representatives with access to personnel records and job applicants
- **Facility Employees:** Anyone with P&A to a cleared or sensitive facility containing targeted information, including security, clerical, maintenance, and janitorial personnel

HOW CAN YOU RECOGNIZE IT?

This approach, by trained professional intelligence officers (IO) and non-traditional collectors, will usually be subtle.

Some likely indicators of this method include:

- Business contact requesting information outside the contract scope, or through an increased or gradual progression of information initiated from legitimately authorized business discussions
- 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 IOs are professionally trained in elicitation tactics and operate without borders. IOs focus on collecting protected and valuable information. Non-traditional collectors, such as business and academic contacts, leverage existing relationships to obtain restricted information outside the relationship scope. Because of this, not all elicitation attempts are obvious. They operate along a spectrum of least intrusive to most intrusive means.

The trained IO elicitor and non-traditional collectors will try to exploit natural human tendencies, including the desire or tendency to:

- Be polite and helpful, even to strangers or new acquaintances
- Appear well-informed, especially about your profession
- Expand discussion on a topic, likely giving praise or encouragement, to show off
- Correct others' comments
- Underestimate the value of the information being sought or given, especially if we are unfamiliar with how that information could be used
- Believe others are honest, a reluctance to be suspicious of others

COUNTERMEASURES

In the event you believe a personal contact has requested 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, your family, or your 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 feel uncomfortable.

If you believe someone is attempting to elicit information from you, you can:

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

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