INDICATORS

The following may indicate an attempt by a foreign entity to acquire U.S. export-controlled technology and systems or classified information:

- Cold calls
- End user is a warehouse or company that organizes shipments for others
- No end-user certificate
- Vagueness of order — quantity, delivery destination, or identity of customer
- Multiple sales representatives
- Unusual quantity
- Requested modifications of technology
- Rushed delivery date
- No return address
- Destination of end user is a third country
- Obscure PO Box or residence
- Multiple businesses using the same address
- Individual requests all products be shipped directly to him/her

INDICATORS

- The request is directed at an employee who does not know the sender and is not in the sales or marketing office
- Solicitor acting as a procurement agent for a foreign government
- Military-specific technology requested for a civilian purpose
- Company request for technology outside the requestor's scope of business
- Last-minute substitutions of visiting personnel
- Visitors request last-minute change of agenda to include export-controlled technology
- Requestor offers to pick up products rather than having them shipped
- Broken English/poor grammar
- Individual has no knowledge of technical specifications of requested technology

Reporting THE THREAT

Bottom Line:

Be Assertive. Be Alert. Be Aware.

Report Suspicious Activity!

Report suspicious activity to your local security contact.
Your DSS point of contact is:

This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

Defense Security Service (DSS)

The DSS Counterintelligence Directorate works to protect Department of Defense (DoD) classified information resident in the cleared industrial base and to enhance security awareness among internal and external customers.

Prompt reporting of foreign collection attempts is critical to an effective industrial security program. Immediately notify the nearest DSS office should you have any reason to believe that your company or one of its employees has been a target of a foreign collection attempt.

Reporting Requirements

The National Industrial Security Program Operating Manual (NISPOM) 1-302b states, "Contractors shall report efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee."

NISPOM 1-301 requires that cleared contractors report actual, probable or possible espionage, sabotage, terrorism, or subversion promptly to the FBI and DSS.

THREAT

DSS has consistently found that the greatest number of suspicious contacts originate from the East Asia and Pacific regions.

- The nature and extent of these contacts suggest a concerted effort to exploit contacts for competitive, economic, and military advantage

Within the past year, DSS found that the majority of suspicious contacts originated from commercial entities.

- These likely represent an attempt to make the contacts seem more innocuous by using non-governmental entities as surrogate collectors

Exploitation of cyberspace for surreptitious access to cleared contractor data systems is a growing concern.

METHODS

Foreign entities often use the following methods to target cleared industry and attempt to gain access to classified/sensitive information and technologies:

- Attempted acquisition of and requests for information about controlled technology
  - Most popular collection techniques
  - Represents a low-risk/high gain method of operation
  - Usually involves emailing, mailing, faxing or telephoning individual U.S. cleared contractor employees; web-card submissions; or use of a website's "contact us" page
- Foreign individuals will often solicit employment on classified cleared contractor projects, while foreign companies and research facilities will offer their technical and business services.
- Attempted intrusions are the most common suspicious network activity
  - Socially engineered emails with malicious attachments to exploit commercial software programs
  - Spoofing emails that imitate valid domains (i.e., .mil or .gov addresses)
  - Attempted intrusions initiated from removable media (USB drives)