Reportable Suspicious Contacts Include

- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
- Contact by cleared employees with known or suspected intelligence officers from any foreign country
- Any contact that suggests the employee concerned may be the target of an attempted exploitation by a foreign intelligence entity
- Attempts to entice cleared employees into compromising 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
- Requests for protected information in the guise a of price quote or purchase request, market survey, or other pretense

Suspicious Purchase Requests

The following may indicate an attempt by a foreign entity to illegally acquire classified or export-controlled technology or information:

- 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
- End user address is in a third country
- Address is an obscure PO Box or residence
- Multiple businesses using the same address
- Buyer requests all products be shipped directly to him/her
- The request is directed at an employee who does not know the sender and is not in the sales or marketing office
- Solicitor is acting as a procurement agent for a foreign government
- Military-specific technology is requested for a civilian purpose
- Company requests technology outside the requestor's scope of business
- Visitors request last-minute change of agenda to include export-controlled technology
- Requestor offers to pick up products rather than having them shipped
- Requestor uses broken English or poor grammar
- Individual has a lack of/no knowledge of the technical specifications of the requested type of technology

Be Alert! Be Aware!

Report suspicious activity to your local security official.

Counterintelligence Awareness

Defense Security Service
Counterintelligence Directorate
www.dss.mil

SPOTTING THE SUSPICIOUS

Threat

United States cleared industry is a prime target of many foreign intelligence collectors and foreign government economic competitors. Cleared employees working on America's most sensitive programs are of special interest to other nations.

The number of reported collection attempts rises every year, indicating an increased risk for industry. While any geographic region can target sensitive or classified U.S. technology, the Defense Security Service (DSS) has consistently found that the majority of suspicious contacts reported by cleared industry originate from East Asia and the Pacific regions.

Every region has active collectors. Cleared contractors should remain vigilant regardless of the collector's assumed country of origin.

The nature and extent of industry reported suspicious contacts suggest a concerted effort to exploit cleared contractors for economic and military advantage. These contacts range from outright attempts to steal technology to seemingly innocuous business ventures.

One of the fastest growing areas of concern is the exploitation of cyberspace for surreptitious access to cleared contractor data systems and cleared individuals. The potential for blended operations where cyberspace contributes to traditional tradecraft presents the greatest risk to cleared industry. An increase in unsolicited contacts made with cleared industry employees from compromised accounts amplifies the potential for compromise of cleared individuals, classified programs, or classified systems occurring in the unclassified cyber domain.

Through analysis of industry reporting, DSS has found that foreign intelligence services utilize both commercial and government-affiliated entities.

- The large number of commercial contacts likely represents an attempt by foreign governments to make the contacts seem more innocuous by using non-governmental entities as surrogate collectors
- The number of government-affiliated contact reports is likely due to foreign governments' increased reliance on government-affiliated research facilities that contact cleared U.S. contractors under the guise of information-sharing

Collection Methods

Recent industry reporting indicates that while foreign entities continue to use direct and overt means in their attempts to gain access to classified/sensitive information and technologies or to compromise cleared individuals, foreign entities are also returning to indirect collection methods.

Cyber Exploitation

- Spear phishing was the most common malware delivery technique; this technique allows the malicious actors to send targeted emails with low risk and potentially high payoff
- Watering Hole attacks (compromised third-party websites) may provide a means for malicious actors to gain unauthorized access to your network or device.
- Removable media (USB devices) can provide a means to quickly spread malicious software from a trusted position
- Use of removable media (USB drives) can initiate attempted intrusions

Attempted acquisition of and requests for information about controlled technology

- Represent a low-risk/high gain method of operation
- Usually involve emailing, mailing, faxing, or cold calling U.S. cleared contractor employees; web-card submissions; or use of a website's "contact us" page
- Collectors ask for everything from price quotes and technical specifications to the outright sale of the technology

■ With **academic solicitation**, foreign students seek post-graduate positions, thesis assistance, or reviews of drafts of scientific publications

■ Representatives of foreign companies often **solicit or market their services** to cleared U.S. companies and offer to market the cleared company's products overseas, provide technical and business services, or seek employment on classified cleared contractor projects

■ During **foreign delegation visits** to cleared facilities, visitors may show up unannounced, attempt to gain access to restricted areas, or add unvetted visitors to their party last minute