U.S. 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. The Defense Counterintelligence and Security Agency has consistently found that the majority of suspicious contacts reported by cleared industry originate from East Asia and the Pacific region. However, every region has active collectors. Cleared contractors should remain vigilant regardless of the collector's assumed country of origin.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)
COUNTERINTELLIGENCE AWARENESS

WHAT IS THE THREAT?

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.

The exploitation of cyberspace continues to be a key area of concern. 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, DCSA 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 contacts 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.

WHO IS BEING TARGETED?

Foreign collectors may target anyone with access to the targeted information, knowledge of information systems, or security procedures. Potential targets often include, but are not limited to:

- **Developers**: Scientists, researchers and engineers researching and applying new materials or methods to defense and other leading edge technologies
- **Technicians**: Engineers or specialists that operate, test, maintain, or repair targeted technologies
- **Production personnel**: Personnel with access to production lines or supply chain of targeted technologies
- **IT personnel**: Systems administrators or others with access to cleared facility networks and knowledge of network security protocols
- **Business development personnel**: Marketing and sales representatives
- **Human resources personnel**: HR representatives with access to personnel records
- **Facility personnel**: Anyone with access to a cleared or sensitive facility containing targeted information including security, clerical, maintenance, and janitorial personnel

WHAT ARE THE MOST COMMON COLLECTION METHODS?

Attempted Acquisition of Technology: Includes attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans, spec sheets or the like. These often involve email, mail, cold-calling cleared employees, web card submissions, or use of a website's "contact us" application.

>> Indicators of Suspicious Purchase Requests:

- 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 P.O. 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

Exploitation of Business Activities: Attempts to exploit an existing commercial relationship or establish a commercial relationship in order to obtain access to protected information, technology, or persons. These include joint ventures, partnerships, mergers and acquisitions, foreign military sales, or attempted development of service provider relationships.

Exploitation of Cyber Operations: Attempts to conduct actions to place at risk the confidentiality, integrity or availability of targeted networks, applications, credentials, or data to gain access to, manipulate or exfiltrate protected information, technology, or personnel information.

>> Common Cyber Operation Methods:

- Phishing operations use emails with embedded malicious content or attachments
- Watering Hole attacks (compromised third-party websites) may provide a means for malicious actors to gain unauthorized access to a network or device
- Removable media (USB devices) can provide a means to quickly spread malicious software from a trusted position

Request for Information (RFI)/Solicitation: Direct or indirect attempts to collect protected information by directly or indirectly asking, requesting, or eliciting protected information, technology, or persons.

>> Common Methods of Contact for RFI/Solicitation:

- Conferences, conventions, or tradeshows – contacts initiated during an event
- Email, mail, telephone, web form
- Foreign visits – Activities or contact occurring before, during, or after a visit to a contractor's facility

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 between cleared employees and 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, coercion 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 of a price quote or purchase

Immediately notify your facility security officer and/or a DCSA representative if you observe any of the above behaviors or believe you were targeted by an individual attempting to obtain illegal or unauthorized access to classified information.