COMMON CYBER OPERATION METHODS

- **Phishing Operations:**
  Emails with embedded malicious content or attachments for the purpose of compromising a network to include, but not limited to, spear phishing, cloning, and whaling
- **Watering Hole:**
  Use of a compromised website to target visitors. These could be third-party websites or your company website to access your customers or persons with common interests
- **Patch Management:**
  Attacks that exploit outdated networking equipment and unpatched software/ hardware vulnerabilities
- **Exploitation of Mobile Devices:**
  Tampering with mobile devices that have trusted access to a protected network
- **Introduction of Backdoor Access Panels**

TRAINING REQUIREMENTS

Cleared contractors are required to receive training on Threat Awareness, Counterintelligence (CI) Awareness, and reporting requirements as per the National Industrial Security Program Operation Manual (NISPOM).

REPORTING REQUIREMENTS

The NISPOM requires the reporting of suspicious contacts, behaviors, and activities.

If you suspect you may have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting CI threats and mitigating risks. Reporting allows us to share and address risks together.

DCSA
https://www.dcsa.mil

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

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

COUNTERINTELLIGENCE AWARENESS & REPORTING

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

WHAT IS THE THREAT?

Our Nation's secrets and technological advantages are in jeopardy–the same secrets that make your company profitable. U.S. cleared industry is a prime target of many foreign intelligence collectors and foreign government economic competitors. The nature and extent of industry threat reporting suggests 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 and/or academic ventures. Through analysis of industry reporting, DCSA has found that foreign intelligence services use both commercial and government-affiliated entities. The large number of commercial contacts likely represents foreign governments' attempts to make contacts seem more innocuous by using non-threatening approaches.

WHO ARE THEY TARGETING?

Foreign collectors may target anyone with access to the targeted information, knowledge of information systems, or security procedures, including:

Developers: Scientists, researchers, engineers, and program managers who research and develop leading technologies

Technicians: Engineers/ specialists who operate, test, maintain, or repair targeted technologies

Supply Chain Personnel: Personnel involved in sourcing and purchasing components integrated with a deliverable defense product or technology, including stockroom control specialists

Information Systems Personnel: Systems administrators or others with access to cleared facility networks and knowledge of network security protocols

Business Development Personnel: Marketing/sales representatives for both domestic and foreign markets

Human Resources (HR) Personnel: HR representatives with access to sensitive information serving as public company contacts and initial screeners of prospective and current employees

Foreign Access Points: Foreign travelers, foreign visitor hosts/escorts, and personnel with foreign contacts

Senior Managers: Company owners and managers listed on open source web content and business records

Subject Matter Experts (SMEs): Scientists and engineers involved with targeted technology publishing in technical journals, participating in professional associations and/or academia, and patent owners

Administrative Staff: Secretaries, administrative/ executive assistants with access to leadership calendars, contact lists, and company proprietary information

Anyone with access to national defense information

MOST COMMON COLLECTION METHODS

Attempted Acquisition of Technology:

Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, product specification sheets, or the like. Contact methods often involve email, mail, cold-calling employees, web card submissions, contacts at trade shows, foreign sales representatives, or use of a website's "contact us" application.

Indicators of Suspicious Purchase Requests:

- The customer or address is similar to one listed on the Commerce Department's Denied Persons List, the Entity List, or other government suspicious entities lists
- Suspicious delivery addresses such as an obscure P.O. Box, residence, or multiple businesses using the same address
- Customer is reluctant to offer information about the end-use of the item
- Customer's line of business does not fit product's applications
- The customer wants to pay cash for a very expensive item when the sale terms would normally call for financing
- The customer has little to no business background available
- The customer declines routine installation, training, or maintenance/warranty services
- The customer is unfamiliar with the product's performance characteristics but still wants the product
- The customer uses third-party broker or address is listed in a third country
- Solicitor acts as a procurement agent for a foreign government
- The customer requests commercial technology modified for military use

Exploitation of Business Activities:

Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; and leveraging an existing commercial relationship in order to obtain access to controlled unclassified information (CUI) in the form of personnel or protected information and technology.

Exploitation of Supply Chain:

Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communications. Contact methods often involve solicitations and marketing offers with below-average pricing and lead times; attempts to purchase a product line supplier; cyber operations; and exploitation of third-party technical service providers.

Requests for Information (RFI):

Collecting protected information by directly or indirectly asking or eliciting personnel for protected information and technology.

Common Methods of Contact for RFI:

- Conferences, conventions, and tradeshows
- Email, surveys, telephone, web forms
- Foreign contacts, visits, and travel

Exploitation of Insiders:

Trusted insiders exploiting their authorized placement and access within cleared industry or causing other harm to compromise personnel or protected information and technology.

Exploitation of Experts:

Gaining access in order to obtain access to CUI in the form of personnel or protected information and technology. Contact methods may include soliciting SME participation in foreign conferences, such as paper submissions, invited speaker, or technical board positions; or offering SMEs foreign academic faculty positions and paid offers to collaborate with foreign academic institutions.

Exploitation of Cyber Operation Methods:

Foreign intelligence entities or other adversaries compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials, or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology. Cyberspace exploitation continues to be a key concern. The potential for blended operations where cyber activity contributes to traditional tradecraft presents a great risk to cleared industry.