WHO IS BEING TARGETED?

Anyone with access to targeted information, knowledge of information systems, or security procedures:

- **Developers:** Research and develop leading technologies
- **Technicians:** Operate, test, maintain, or repair targeted technologies
- **Supply Chain Personnel:** Source and purchase components integrated with deliverable defense products or technology
- **Information Systems Personnel:** 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:** 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):** Involved with targeted technology publishing in technical journals, participating in professional associations and/or academia, and patent owners
- **Administrative Staff:** Access to leadership calendars, contact lists, and company proprietary information
- **Janitorial, Maintenance, and Support Staff:** Access to personnel, information, and technology
- **Anyone with access to national defense information**

REPORTING REQUIREMENTS

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

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks.

Cleared contractors are required to receive training on threat awareness, CI awareness, and reporting requirements per NISPOM.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

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

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

COUNTERINTELLIGENCE AWARENESS AND REPORTING

Defense Counterintelligence and Security Agency

WHAT IS THE THREAT?

U.S. cleared industry is a target of many foreign intelligence collectors and economic competitors. Industry threat reporting suggests a concerted effort to exploit cleared contractors by overt attempts to steal technology, as well as covert business and academic ventures. DCSA's industry reporting analysis found foreign adversaries and competitors use traditional and nontraditional collectors and commercial and government-affiliated entities. The amount of commercial contacts reported likely represents foreign governments' attempts to make contacts innocuous by using non-threatening approaches.

HOW ARE YOU BEING TARGETED?

MOST COMMON METHODS OF OPERATION

Exploitation of Business Activities

Exploitation of Insider Access

Attempted Acquisition of Technology

Exploitation of Supply Chain

Request for Information/ Solicitation

Exploitation of Experts

Exploitation of Cyber Operations

EXPLOITATION OF BUSINESS ACTIVITIES:

Establishing or leveraging a commercial relationship via joint ventures, partnerships, mergers and acquisitions, or foreign military sales to obtain controlled unclassified information (CUI).

EXPLOITATION OF INSIDER ACCESS:

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

ATTEMPTED ACQUISITION OF TECHNOLOGY:

Acquiring controlled technologies, via direct contact or through the use of front companies or intermediaries, including equipment, diagrams, schematics, plans, or product specification sheets.

METHODS OF CONTACT

- Email
- Cold-calling
- Mail
- Trade shows
- Web cards and "contact us" forms
- Foreign contact (sales)

INDICATORS OF SUSPICIOUS PURCHASE REQUESTS

- Similar name or address to those on government suspicious entities lists
- Suspicious delivery addresses: obscure addresses or multiple businesses using the same address
- Customer is reluctant to discuss item's end-use
- Customer line of business does not fit product's applications
- Solicitor acting as procurement agent for foreign government
- Requesting commercial technology modified for military use
- Customer wants to pay cash for an expensive item when sale terms would normally call for financing
- Customer has little to no business background available
- Customer declines routine installation, training, or maintenance/warranty services
- Customer is unfamiliar with product performance characteristics but still wants the product
- Customer uses third-party broker or address is listed in a third country

EXPLOITATION OF SUPPLY CHAIN:

Compromising supply chain by introducing counterfeit or malicious products or materials into the supply chain to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communications.

Contact methods 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 eliciting personnel for protected information and technology.

METHODS OF CONTACT

- Email
- Telephone
- Web form or survey
- Foreign contact, visit, or travel
- Conferences, conventions, or tradeshows

EXPLOITATION OF EXPERTS:

Gaining access to obtain CUI.

Contact methods include soliciting subject matter expert (SME) participation in foreign conferences or paying SMEs to collaborate with foreign academic institutions.

EXPLOITATION OF CYBER OPERATIONS:

Foreign intelligence entities/adversaries compromising confidentiality, integrity, or availability of targeted networks, applications, credentials, or data to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.

COMMON CYBER OPERATION METHODS:

- **Phishing Operations:** Emails with embedded malicious content or attachments for the purpose of compromising a network, including spear phishing, cloning, and whaling
- **Exploitation of Mobile Devices:** Tampering with mobile devices that have trusted access to a protected network
- **Patch Management:** Attacks that exploit outdated networking equipment and unpatched software/ hardware vulnerabilities
- **Watering Hole:** Use of a compromised website to target visitors, including third-party or company websites to access your customers or persons with common interests
- Introduction of Backdoor Access Panels