REPORTING REQUIREMENTS

National Industrial Security Program Operating Manual (NISPOM) requires the reporting of suspicious contacts, behaviors, and activities.

If you suspect you or your company has been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence threats and mitigating risks. Reporting allows us to share and address risks together.

"China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes, to require or pressure technology transfer from U.S. companies."

Annual Intellectual Property Report to Congress, February 2019

DCSA
https://www.dcsa.mil

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

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

EXPLOITATION OF BUSINESS ACTIVITY

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

WHAT IS EXPLOITATION OF BUSINESS ACTIVITY?

Establishing a commercial relationship via joint ventures, partnerships, direct commercial sales, or service providers; leveraging an existing commercial relationship to obtain access to personnel or protected information and technology.

WHO ARE THEY TARGETING?

- Any cleared employee or cleared company that supports cleared facilities, or that works with controlled unclassified information (CUI) or classified information relating to the Department of Defense (DOD) or other U.S. Government programs or systems
- Foreign collectors or their agents often target employees involved in business development, sales, marketing, information sharing, or other "professional collaborative efforts" to develop a relationship
- Once such an entity establishes a business relationship, they seek to leverage that relationship to contact other cleared employees working with targeted information and technology

WHY IS IT EFFECTIVE?

Foreign entities exploit legitimate activities with defense-oriented companies to obtain access to otherwise denied information, programs, technology, or associated U.S. personnel. This method of operation relies on the appearance of legitimacy provided by the established commercial or business activity. Conversely, U.S. company personnel, cleared or uncleared, seeking to build positive relationships and gain future business with foreign partners may unwittingly provide information beyond the scope of the business activity for which the relationship exists.

Examples of this exploitation include:

- Foreign ownership of, or financial interest in, a U.S. company may provide access to intellectual property rights held by the U.S. company
- Business activity may allow the foreign company access to information on the U.S. company's network

- Foreign-produced hardware and software sold to a cleared company may include design vulnerabilities and malware that could provide foreign actors access to a company's networks and information
- Foreign collectors prey upon cleared employees' eagerness to develop or expand a commercial relationship to increase sales or revenues
- A joint venture with a foreign company using the U.S. company's name allows foreign employees to use the U.S. company's name on business cards
- Cleared employees who are uninformed and uneducated on the commercial agreement's security limits or the technology's export control restrictions may commit a security violation by unwittingly providing information that should not be shared, based on the established relationship

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

- Personal contact
- Cultural commonality
- Foreign visits
- Direct military sales
- Direct commercial sales
- Conferences, conventions, and tradeshows
- Cyber operations
- Email requests
- Business propositions and solicitations
- Academic solicitations
- Web form submissions
- Joint ventures
- Social networking sites
- Claiming to have been referenced by (XYZ), i.e., friend, another company/ vendor/customer, etc

HOW CAN YOU RECOGNIZE IT?

A business relationship with a foreign company or person may be entirely legitimate. However, in many cases, foreign entities with nefarious motives and intent build relationships or abuse existing relationships with U.S. industry to establish pathways to restricted information and technology. Building on apparent legitimate business activity, foreign collectors abuse the relationship as a vector to gain access to restricted or prohibited information. These commercial and business relationships include:

- Misrepresenting themselves as a foreign representative for a U.S. company
- Selling and installing hardware or software in cleared contractors' or sensitive facilities' networks
- Buying a substantial or majority interest in U.S. companies to gain intellectual property rights for technology, as well as to share data or appoint key management personnel in the acquired company

Potentially Suspicious Exploitation Scenarios:

- Foreign company has a nebulous business background
- Foreign company attempts to obscure ties to a foreign government
- Foreign company attempts to acquire interest in companies or facilities inconsistent with their current business lines
- Foreign partner/client requests to visit cleared facility not related to the business relationship
- Foreign visitors violate security protocols during visits to cleared facilities, or change the members of a visiting delegation at the last minute
- Foreign company seeks to establish joint ventures with cleared companies to act as U.S. company's representative in foreign markets
- Foreign company attempts to use a subsidiary in a third country to establish business relationships or buy interests in a cleared U.S. company
- Foreign company targets U.S. cleared employees, or those working in support of cleared companies, for information beyond the scope of the current relationship, or offers partnership with the cleared company