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.

EXPLOITATION OF BUSINESS ACTIVITIES

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

Defense Counterintelligence and Security Agency

WHAT IS EXPLOITATION OF BUSINESS ACTIVITY?

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

WHO IS BEING TARGETED?

- Any cleared employee or cleared company that supports cleared facilities, works with controlled unclassified information (CUI), or classified information related to the Department of Defense (DoD) or other U.S. Government programs
- Employees involved in business development, sales, marketing, information sharing, or professional collaborative efforts to develop a relationship
- Entities seek to leverage business relationships to contact other cleared employees working with targeted information and technology

HOW ARE YOU BEING TARGETED?

METHODS OF OPERATION:

- Cultural commonality
- Acquisition of technology via a cleared company's foreign sales representative or distributor
- Business propositions and solicitations
- Direct military or commercial sales
- Joint ventures
- Claiming to have been referred

METHODS OF CONTACT:

- Email
- Foreign Visit
- Cyber Operations
- Web Form
- Personal Contact
- Conferences, Conventions, or Trade Shows
- Rèsumè—Academic
- Social Networking Service

WHY IS EXPLOITATION OF BUSINESS ACTIVITY EFFECTIVE?

Foreign entities exploit legitimate activities with defense-oriented companies to obtain access to otherwise denied information, programs, technology, or personnel. This method of operation relies on the legitimacy provided by the established commercial or business activity. Conversely, U.S. personnel seeking to gain future business with foreign partners may unwittingly provide information beyond the scope of the original business activity.

EXAMPLES OF THIS EXPLOITATION MAY 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 U.S. networks
- Foreign-produced hardware and software may include design vulnerabilities and malware that could provide foreign actors access to a company's network
- Foreign collectors prey upon cleared employees' eagerness to develop commercial relationships 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 unaware of commercial agreement security limits or export control restrictions may commit a security violation by unwittingly providing information that should not be shared

"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

HOW CAN YOU RECOGNIZE IT?

A business relationship with a foreign company or person may be entirely legitimate; however, foreign entities with nefarious intent may abuse relationships with U.S. industry to establish pathways to restricted information and technology. Building on 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, sharing data, or appointing key management personnel in the acquired company

VIGNETTES

- Foreign company has a nebulous business background
- Foreign company attempts to obscure ties to foreign government
- Foreign company attempts to acquire interest in companies or facilities inconsistent with 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 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