WHAT IS EXPLOITATION OF BUSINESS ACTIVITIES?

Attempts to establish a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service providers.

Attempts to leverage an existing commercial relationship in order to obtain access to protected information, technology, or persons.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

EXPLOITATION OF BUSINESS ACTIVITIES

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

- Personal contact
- Cultural commonality
- Foreign visits
- Foreign military sales
- Direct commercial sales
- Conferences, conventions, or tradeshows
- Cyber operations
- Email requests
- Business propositions and solicitations
- Academic solicitations
- Web form submissions
- Joint ventures
- Social networking services

WHO IS BEING TARGETED?

- Any company with cleared personnel, that works in support of cleared facilities, or that works with sensitive, restricted, or classified information relating to the Department of Defense (DoD) or other U.S. Government agencies' programs or systems.
- Foreign collectors, or their agents, often target employees involved in business development, sales, marketing, information sharing, or other "professional collaborative efforts" in order to develop a relationship.
- Once such an entity establishes a business relationship, they seek to take advantage of 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 not, 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 how this exploitation can be effective are illustrated below:

- 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 that could provide foreign actors access to a company's networks and information;
- Foreign collectors prey upon cleared employees' eagerness to develop or expand commercial relationships to increase sales or revenues;
- A joint venture with a foreign company formed using the U.S. company's name, allowing foreign employees to use the U.S. company's name on business cards;

- Cleared employees not informed and educated on the business and security limits of the commercial agreement or the export control restriction of technology may commit a security violation by unwittingly providing information that should not be shared, based on the established relationship.

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 the 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 contractor or sensitive facilities or 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.
- The following are eight examples of potentially suspicious exploitation scenarios:

1. Foreign company has a nebulous business background;
2. Foreign company attempts to obscure ties to a foreign government;
3. Foreign company attempts to acquire interest in companies or facilities inconsistent with their current business lines;
4. Foreign partner/client requests to visit cleared facility not related to the business relationship;
5. Foreign visitors violate security protocols during visits to cleared facilities, or change the members of a visiting delegation at the last minute;
6. Foreign company seeks to establish joint ventures with cleared companies to act as U.S. company's representative in foreign markets;
7. Foreign company (including companies from countries subject to sanctions) attempts to use a subsidiary in a third country to establish business relationships or buy interests in a cleared U.S. company;
8. 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 or sensitive company during conferences, conventions, exhibits, or tradeshows.

COUNTERMEASURES

To mitigate foreign partners' or clients' ability to gain access to restricted information or technology, U.S. cleared companies have many options available to them. The following are just six examples of such options:

1. Ensure all employees interacting with foreign partners know the specifics of the relationship and what information, equipment, and technology they can and cannot share, and understand the requirements to report "suspicious activity;"
2. Ensure security protocols are in place and adhered to for access to the facility, assembly/production line, and networks, and are all periodically reviewed and updated;
3. Prior to receiving foreign visitors, ensure the facility and the personnel are prepared for the visit, including appropriate briefings, and submit names of the visitors to DCSA prior to the visit;
4. Ensure employees attending conferences, conventions, exhibits, or tradeshows know what information they can share with potential partners and clients, and are aware of their reporting requirements regarding any suspicious contacts;
5. Cleared companies owned by foreign companies should develop and implement appropriate foreign ownership, control or influence (FOCI) mitigation procedures in consultation with DCSA to insulate sensitive information from unauthorized foreign entities;
6. Proactively engage with your designated DCSA representative on a regular basis and remain familiar with foreign collection trends and reporting requirements.