WHAT TO REPORT

Immediately notify your facility security officer if you observe any of the following behaviors or believe you were targeted by an individual attempting to obtain information or technology they are not authorized to have:

- Offers to act as a foreign sales agent
- Attempts to steer conversations toward job duties or access to sensitive information or technology
- Insistent questioning outside the scope of what you are cleared to discuss
- Excessive photography/sketches, especially in areas that prohibit photography
- Individuals returning to the same booth multiple times to speak with different cleared employees
- Strangers trying to establish personal relationships outside work parameters
- Unusual or suspicious attempts at ongoing contact, including sending a follow-up email upon your return to the office
- Multiple individuals simultaneously asking questions, attempting to get you to reveal more than you should
- Theft of or missing items from your booth/display

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.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADE SHOWS

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 TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADESHOWS?

Conferences, conventions, or trade shows host a wide array of presenters, vendors, and attendees. This provides a permissive environment for foreign collectors, commercial rivals, start-up companies, intelligence officers, opportunists, and organized criminals to question vendors, develop business/social relationships, access actual or mockups of targeted technology, and interact with Subject Matter Experts (SMEs).

In 2019, nine percent of cleared industry reporting of suspicious contact-related activities occurred during attendance at conferences, conventions, or trade shows.

WHO IS BEING TARGETED?

Foreign collectors target anyone with access to targeted information and technology, or any SME in sought-after research or technology.

WHAT IS BEING TARGETED?

- Information, technical specifications, Department of Defense (DoD) plans, budgets/costs, system locations, and system pictures displayed at booths
- Information about cleared and uncleared employees to determine location to information, vulnerability to recruitment, and personnel interests to be used as pretext for future contact
- Physical or virtual access to company equipment
- Proprietary formulas and processes
- Blueprints and prototypes
- Research
- Vendor information
- Software information, i.e. source codes
- Company information – phone directories, corporate financial data, investment data, budgets, acquisitions, and sales

HOW ARE YOU BEING TARGETED?

Request for Information/ Solicitation

Exploitation of Experts

Search and Seizure

Surveillance

Foreign Intelligence Entities (FIEs) pose as potential customers, attendees, exhibitors, scientists, or as representatives of a nation other than their own.

Collectors attempt to elicit controlled unclassified information (CUI) and classified information through casual conversation during and after official events.

FIEs use these occasions to spot and assess individuals for potential recruitment. They use charm and/or potential business incentives to soften their targets.

During foreign travel, security personnel can subject attendees to search and seizure of documents and electronic devices, as well as surveillance at the venue, while socializing, and while in hotels.

HOW CAN YOU RECOGNIZE IT?

At conferences, conventions, or tradeshows you may witness:

- Attendees not wearing, or wearing incorrectly, IDs/badges
- Attempts to steal actual or mockups of technologies on display
- Photography of displays, especially when photography is explicitly prohibited
- Requests for information beyond the conference's scope
- Requests for the same information from different people during the conference
- Attempts to schedule post-event meetings or contact and attempts to develop personal friendships
- Attempts to contact you before, during, or after the meeting by phone, email, or social media

While traveling to and attending events, traditional intelligence officers will use the following techniques to obtain information about you, your work, and your colleagues:

- Detailed and probing questions about specific technology
- Overt questions about CUI or classified information
- Casual questions regarding personal information collectors can use to target them later
- Prompting employees to discuss duties, access, or clearance level
- Attempts to access your electronic devices, i.e., laptop, smartphones

COUNTERMEASURES

- Display signage requesting no touching or photography of items on display
- Complete annual counterintelligence awareness training
- Attend security briefings and de-briefings
- Remain cognizant of your surroundings and anyone displaying increased interest in you or your exhibit
- At events, display mockups, not actual working versions of your product
- Do not leave technology, mockups, sensitive documents, or electronics unattended
- Create controlled access areas for sensitive displays that should not be touched or photographed
- Prepare responses for questions involving CUI or classified aspects of your product
- If your company provides WiFi for employees, create a strong password, and change it before and after each show
- Do not accept electronic gifts

WHEN ATTENDING EVENTS OVERSEAS

- Request a threat assessment from the program office and your local DCSA representative prior to traveling to an event overseas
- Use designated travel laptops that contain no CUI or exploitable information
- Do not use foreign computers or fax machines and limit sensitive discussions
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Do not post pictures or mention you are on travel on social media