WHAT IS THE CCTS METHOD OF CONTACT?

Contact initiated by a foreign intelligence entity, or on behalf of one, during an event such as a conference, convention, exhibition or tradeshow.

Foreign intelligence officers or non-traditional collectors may use this contact method for exploitation of commercial/business activities, RFI/ solicitation, exploitation of experts or persons with access, attempted acquisition of technology, and theft to obtain targeted information or technologies.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

CONFERENCES, CONVENTIONS, OR TRADESHOWS

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

Foreign collectors use many methods to gather information on current and emerging U.S. technology. They may pose as potential customers, attendees, exhibitors, or scientists, and even as a representative of a nation other than their own. Collectors may attempt to directly ask about sensitive or classified information or try to elicit information during casual conversation during and after official events.

- Exploitation of Commercial/Business Activities
- Exploitation of Insider Access
- Exploitation of Security Protocols
- RFI/Solicitation
- Exploitation of Experts
- Theft
- Exploitation of Relationships
- Surveillance

WHO IS BEING TARGETED?

Foreign collectors will target personnel with access to the targeted information and technology, or who are subject matter experts in sought after research/technology.

WHAT DO THEY WANT?

- Information, technical specifications, and pictures of the systems displayed at booths
- Exploitable information about both cleared and uncleared employees
- Information about which cleared and uncleared employees have access to technologies of interest
- Personal information about cleared and uncleared individuals, including hobbies, family information, and interests. This information can be used to either exploit or build a relationship with the individual at a later date
- Personal or professional information that can be used as a pretext for ongoing or future contact

WHY IS IT EFFECTIVE?

Conferences, conventions, or tradeshows host a wide array of presenters, vendors, and attendees, which provide a permissive environment for traditional and non-traditional collectors to question vendors, develop business/social relationships, access actual or mockups of targeted technology, and interact with subject matter experts. Foreign intelligence officers use these occasions to spot and assess individuals for potential recruitment. They frequently use charm and/or potential business incentives to attempt to soften their target.

One aspect of this method of contact is foreign travel related to the event. During travel, attendees are subject to search and seizure of documents and electronic devices by host or transit nation security personnel, as well as surveillance at the venue, while socializing, and while resident in their hotels.

HOW CAN YOU RECOGNIZE IT?

- At the conferences, conventions, or tradeshows you may witness:
- Attempts to steal actual or mockups of technologies on display
- Attempts to access your electronic devices – laptop, smartphones, etc.
- Photography of displays, especially when photography is explicitly prohibited

- Requesting information from you beyond the scope of the conference
- Individual requesting same information from different personnel at your booth
- Traditional intelligence officers will apply elicitation techniques to subtly extract information about you, your work, or your colleagues.
  - ♦ You may experience the following elicitation techniques while attending conferences, conventions, or tradeshows:
    - ◊ Detailed and probing questions about specific technology
    - ◊ Overt questions about sensitive or classified information
    - ◊ Casual questions directed at individual employees regarding personal information that collectors can use to target them later
    - ◊ Prompting employees to discuss their duties, access, or clearance level

COUNTERMEASURES

- Attend annual CI awareness training
- Attend security briefings and de-briefings
- Create a plan to protect any classified or controlled sensitive technology or information brought overseas and consider whether equipment or software can be adequately protected
- Request a threat assessment from the program office and your local DSS representative prior to traveling to a conference, convention, or tradeshow
- Do not publicize travel plans; limit sharing of this information to people who need to know
- Maintain control of classified or sensitive information and equipment
- Immediately report suspicious activity to the appropriate authorities at the event and your facility security officer
- Do not post pictures or mention you are on travel on social media
- Retain unwanted sensitive material pending proper disposal
- Do not use foreign computers or fax machines, and limit sensitive discussions

WHAT TO REPORT

- Offers to you to act as a foreign sales agent
- Attempts to steer conversations toward your job duties or access to sensitive information or technology
- Insistent questioning outside the scope of what you're cleared to discuss in an unclassified environment
- Taking excessive photographs, especially in areas that prohibit photography
- Individuals returning to the same booth multiple times in an attempt to speak with different cleared employees working the booth
- 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
- Immediately notify your facility security officer if you observe any of the above behaviors or believe you were targeted by an individual attempting to obtain illegal or unauthorized access to classified information.