PRACTICAL COUNTERMEASURES

- Ensure every employee receives annual counterintelligence (CI) awareness training
- Develop a plan to protect any classified and export-controlled technology or information brought overseas and consider whether equipment or software can be adequately protected
- Request a threat assessment from the program office prior to traveling to a conference, convention, or trade show outside the U.S.
- Ensure employees immediately report suspicious activity at conferences, conventions, and trade shows to their facility security officer
- Employees traveling abroad should not publicize their travel plans
- Recommend all employees receive a pre-travel security briefing
- While traveling, employees should maintain control of classified or sensitive information and equipment. Employees should retain unwanted sensitive material pending proper disposal.
- Employees should not use foreign computers or faxes and should limit sensitive discussions

BOTTOM LINE:

BE ALERT. BE AWARE.

REPORT SUSPICIOUS ACTIVITY!

This pamphlet is intended to:

- Assist you in recognizing and responding to unauthorized attempts to solicit sensitive or classified information at conferences, conventions, and trade shows
- Advise you to immediately report suspicious contacts or the potential loss or compromise of sensitive or classified information

Report suspicious activity to your facility security officer.
Your DSS point of contact is:

Counterintelligence Awareness Tips when Attending:

CONFERENCES, CONVENTIONS, AND TRADE SHOWS

This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

BE PREPARED

- You can be targeted at any conference, convention, or trade show, foreign or domestic
- Attend a security pre-briefing before going to any event where you may encounter foreign nationals to ensure you are sensitized to current collection techniques and requirements
- Be informed on general security guidelines and the handling of classified information, and know which parts of your business you are allowed to discuss
- Do not underestimate the value of the information you're sharing. Unsuspecting personnel are often targeted because they don't realize the value of the information to collectors
- Collectors may pose as attendees, exhibitors, or scientists

Be Careful

Collectors use many methods to gather information on current and emerging U.S. technology. Collectors may attempt to directly ask about sensitive or classified information, or may try to elicit information from you during casual conversation both during and after any official events.

REPORTABLE BEHAVIORS

- Offers to act as foreign sales agent
- Attempts to steer conversations towards your job duties or access to sensitive 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 asking questions simultaneously, attempting to get you to reveal more than you should
- Any suspicious contact that occurs while at events

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.

ELICITATION TECHNIQUES

Elicitation is the process by which someone tries to extract information from another individual using direct and indirect questioning, including:

- Asking detailed and probing questions about specific technology
- Overtly questioning about sensitive or classified information
- Casually questioning individual employees about personal information that collectors can use to target them later
- Prompting employees to discuss their duties, access, or clearance level

Note: A skilled elicitor can guide a conversation to areas of interest without directly asking questions that make his or her intent obvious.

What They're After

- Information, technical specifications, and pictures of the systems displayed at booths
- Exploitable information about cleared employees
- Information about which cleared employees have access to technologies of interest
- Personal information about cleared 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