International visitors are common in today's global economy and often results in increased business. Although most visitors are there on legitimate business, cleared contractors need to be aware that there are potential vulnerabilities related to these visits.

Foreign delegation visits to cleared contractor facilities are one of the most frequently used approaches to target and attempt to gain access to sensitive and classified information resident in cleared industry.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

FOREIGN VISITS

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

The most common methods of operation associated with foreign visits include:

- **Violation of Security Protocols**: Attempts by visitors/ unauthorized individuals to circumvent or disregard security procedures that may indicate a risk to protected information, technology or persons
- **Exploitation of Relationships**: Attempts to leverage existing personal or authorized relationships to gain access to protected information
- **Request for Information (RFI)/Solicitation**: Direct or indirect attempts to collect protected information by asking, petitioning or requesting of the host
- **Exploitation of Commercial/Business Activities**: Attempts to establish a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales or service provider or leverage an existing commercial relationship in order to obtain access to protected information, technology or persons

HOW CAN YOU RECOGNIZE IT?

- **Peppering**: Visitors ask a variation of the same question or one visitor asks the same question to multiple U.S. contractor employees
- **Wandering Visitor**: The visitor uses the distraction provided by a large delegation to slip away, out of the control of the escort. Once away from the escort, the visitor may attempt to gain access to a restricted area, sensitive or classified documents, or unattended and unlocked information systems
- **Divide and Conquer**: Visitors corner an escort away from the group and attempt to discuss unapproved topics in order to deprive the escort of his safety net of assistance in answering questions
- **Switch Visitors**: Delegations may add a new visitor to the group at the last minute, leaving little or no time for the company to vet the new visitor against community lists of known intelligence officers
- **Bait and Switch**: The visitors say they are coming to discuss one business topic, but after they arrive they attempt to discuss the cleared contractor's other projects, often dealing with sensitive or classified information
- **Distraught Visitor**: When the visitor's questions are not answered, he/she acts insulted or creates an uncomfortable scene to psychologically coerce information from the target
- **Use of Prohibited Electronics:** The visitors bring unauthorized electronic devices such as cell phones, cameras, or thumb drives into restricted space

COUNTERMEASURES*

**For additional information, see National Industrial Security Program Operating Manual, Chapter 10, Section 5*

- Prior to the visit, brief all escorts and personnel working with the delegation on what they can and cannot discuss, and limit the scope of all discussions to the legitimate business at hand
- Develop standard, acceptable responses to questions that may arise, especially if the projects are sensitive or classified, are not applicable to the visit, or include proprietary information
- Submit the names of the visitors to DCSA prior to the visit as far in advance as feasible; provide updates as necessary
- Conduct a pre-visit walkthrough of the facility to

ensure visitors will not be able to hear or see sensitive or classified information during all areas of their visit; mitigate areas of concern

- Train escorts on detecting suspicious behavior and questions; maintain visual contact with visitors at all times
- After the visit, debrief the hosting representatives and all escorts to identify any strange and/or suspicious activities exhibited by their visitors or unusual or probing questions
- Provide employees with training on how to detect elicitation attempts
- Share the minimum amount of information appropriate to the joint venture
- Periodically interview employees who have frequent contact with visiting personnel to check on indicators of economic espionage or recruitment attempts
- Conduct regular computer audits
- Do not allow visitors to use networked computers; provide stand-alone computers
- Change passwords and access controls to rooms, buildings and computers that long-term visitors used
- Train employees on how to handle contact with prior visitors
- Do not hesitate to end the tour and escort visitors out of the facility for non-compliance

EXPLOITING THE FOREIGN VISITS SYSTEM

The U.S. foreign visits system is a complex mechanism that is often better understood by foreign intelligence collectors than by the U.S. companies that participate in the system.

One way to exploit the system is to make multiple requests to different U.S. agencies. Another is to take advantage of different procedures depending upon whether the visit can be described as government sponsored, non-sponsored, or commercial in nature. For example, if a classified visit is disapproved, the foreign group may seek to arrange a commercial visit through a different U.S. Government agency.

LONG-TERM VISITS AND JOINT VENTURES

Long-term visits or joint ventures may provide an opportunity for a competing company to obtain restricted/proprietary information.

They also provide an opportunity for visitors to spot, assess, and befriend employees that may assist in willing or unwillingly collect restricted/proprietary information

THE TAKE-AWAY

Any line of questioning concerning military or intelligence-based contracts or dual-use technology, unless previously approved, should be viewed as suspicious behavior.

Even if an appropriate authority grants a foreign visitor access to classified U.S. information, that visitor is not entitled to classified information unless he/she has cleared need to know that has been communicated and verified in advance of the visit.

Inform your DCSA representative of proposed foreign visitors. Given adequate time, they can assist with identifying risks to the cleared company, its technology, and its personnel.

If any suspicious incidents occur during the visit, immediately report them to your facility security officer or DCSA representative.