

WHAT TO REPORT

View as suspicious any line of questioning concerning military or intelligence-based contracts or dual-use technology, unless topics were previously approved.

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 Industrial Security Representative or DCSA CI Special Agent of proposed foreign visitors. Given adequate time, they can assist with identifying risks to the cleared company, its technology, and its personnel.

View as suspicious any attendee's effort to contact you before, during, or after the visit by phone, email, or social media.

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

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



DCSA
<https://www.dcsa.mil>

DCSA, Counterintelligence Directorate
<https://www.dcsa.mil/mc/ci>

Center for Development of Security
Excellence
<https://www.cdse.edu>

PREPARING FOR FOREIGN VISITORS



PREPARING FOR FOREIGN VISITORS

Foreign visitors are common in today's global economy. Cleared contractors should be aware of potential counterintelligence (CI) vulnerabilities and threats.

While most visitors are here for legitimate purposes, the sheer volume of visitors makes it difficult to detect those with ulterior motives.

Foreign delegation visits to cleared contractor facilities are one of the most frequently used methods to target and attempt to gain access to controlled unclassified information (CUI) from cleared industry.

WHY DO FOREIGN ENTITIES TARGET U.S. CLEARED INDUSTRY?

It is cheaper for foreign entities to illicitly obtain CUI or classified information and technology than to fund initial research and development (R&D) themselves. The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D prime targets for foreign collection of classified and unclassified commercial technology.

When a foreign visit occurs at your facility, preparation and awareness are essential to preventing loss of information. Stay alert and watch for indicators to help assess the potential for visitor targeting or collection.

HOW ARE YOU BEING TARGETED?

- **Peppering:** Visitors ask a variation of the same question or one visitor asks the same question to multiple employees
- **Wandering Visitor:** The visitor uses the distraction provided by a large delegation to slip away, out of the escort's control. Once away from the escort, the visitor may try to access 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 to remove the escort's 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 known intelligence officers
- **Bait and Switch:** The visitors plan to discuss one business topic, but after arriving, they attempt to discuss the cleared contractor's other projects, often dealing with CUI 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*

- Conduct a pre-visit facility walkthrough to ensure visitors cannot hear or see CUI, export-controlled information, or classified information during their visit
- Vet incoming foreign visitors with your supporting Defense Counterintelligence (DCSA) CI special agent
- Prior to the visit, brief all escorts and personnel working with the delegation on what they can and cannot discuss
- Develop standard, acceptable responses to questions that may arise, especially if projects are CUI or classified, are not applicable to the country visit, or include proprietary information
- Ensure there are enough escorts to properly support the number of visitors and escorts know where in the facility visitors can and cannot access
- Train escorts to detect suspicious behavior and questions, ensure they know to maintain visual contact with all visitors at all times, and develop contingency plans to handle visitors who leave the group
- If the delegation attempts to make additional contacts with escorts and speakers, ensure they limit discussions to the agreed-upon topics and information
- After the visit, debrief the host and all escorts to uncover if visitors exhibited any strange or suspicious activities or asked unusual and probing questions

LONG-TERM VISITS AND JOINT VENTURES

Long-term visits or joint ventures may provide an opportunity for a foreign long-term visitor to obtain restricted/proprietary information. They also provide an opportunity for visitors to spot, assess, and befriend employees that may assist, wittingly or unwittingly, in collecting restricted/proprietary information.

**For additional information, see Code of Federal Regulation (CFR) 32 Part 117 National Industrial Security Program Operating Manual (NISPOM).*

