

# Foreign Collection Methods: Indicators and Countermeasures

Most Commonly Used Collection Methods .....	2
Unsolicited and Direct Requests.....	3
Technique.....	3
Indicators.....	3
Countermeasures .....	3
Suspicious Network Activity.....	3
Technique.....	4
Indicators.....	4
Countermeasures .....	4
Targeting at Seminars, Conventions, and Trade Shows .....	4
Technique.....	5
Indicators.....	5
Countermeasures .....	5
Insider Threat .....	5
Technique.....	6
Indicators.....	6
Countermeasures .....	6
Foreign Visits .....	7
Technique.....	7
Indicators.....	7
Countermeasures .....	7
Solicitation and Seeking Employment.....	7
Technique.....	8
Indicators.....	8
Countermeasures .....	8

## ***Most Commonly Used Collection Methods***

*If you suspect you may have been a target of any of the methods included here, or have been targeted by any other method, report it to your FSO immediately.*

The most common foreign collection methods, used in over 80% of targeting cases, are:

- Unsolicited and direct requests
- Suspicious internet activity
- Targeting at conferences, conventions, and trade shows
- Insider threat
- Solicitation and employment
- Foreign visits

## ***Unsolicited and Direct Requests***

### **Technique**

This method utilizes an information request from an unknown source that was not sought or encouraged.

Requests may originate from:

- Foreign companies
- Individuals
- Foreign government officials
- Organizations

### **Indicators**

There are several possible indicators of unsolicited and direct requests, including, but not limited to, those listed below.

The requestor:

- Sends a request using a foreign address
- Has never met recipient
- Identifies self as a student or consultant
- Identifies employer as a foreign government
- States that work is being done for a foreign government or program
- Asks about a technology related to a defense program, project, or contract
- Asks questions about defense-related programs using acronyms specific to the program
- Insinuates the third party he/she works for is "classified" or otherwise sensitive
- Admits he/she could not get the information elsewhere because it was classified or controlled
- Advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- Advises the recipient not to worry about security concerns
- Assures the recipient that export licenses are not required or not a problem

### **Countermeasures**

The following countermeasures can protect against unsolicited and direct requests:

- View unsolicited and direct requests with suspicion, especially those received via the Internet
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified:
  - Do not respond in any way
  - Report the incident to security personnel

*If you suspect you may have been targeted using this method, contact your FSO.  
For further information, refer to the Counterintelligence section of the DSS website at  
[www.dss.mil](http://www.dss.mil).*

## ***Suspicious Network Activity***

Suspicious internet activity is the fastest growing method operation for foreign entities seeking to gain information about U.S. interests. It may also be referred to as *cyber terror*, *cyber threats*, *cyber warfare*, etc.

### **Technique**

An adversary may target anyone or any system at any facility, using a number of methods:

- Input of falsified, corrupted data
- Malware, malicious code, viruses
- Hacking
- Chat rooms-elicitation
- Email solicitation

### **Indicators**

The following is a list of suspicious indicators related to suspicious Internet activity and cyber threats:

- Unauthorized system access attempts
- Unauthorized system access to or disclosure of information
- Any acts that interrupt or result in a denial of service
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- Emails received from unknown senders with foreign addresses

### **Countermeasures**

The following countermeasures can be taken by cleared defense contractors to guard against this collection method:

- Develop and implement a Technology Control Plan (TCP)
- Conduct frequent computer audits
  - Ideally: Daily
  - At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Direct personnel to avoid responding to any unknown request and to report these requests
- Disconnect computer system temporarily in the event of a severe attack

*If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at [www.dss.mil](http://www.dss.mil).*

## ***Targeting at Seminars, Conventions, and Trade Shows***

This method directly links targeted programs and technologies with knowledgeable personnel.

### **Technique:**

- Technical experts may receive invitations to share their knowledge
- Experts may be asked about restricted, proprietary, and classified information

### **Indicators**

The following are suspicious indicators related to seminars, conventions, and trade shows.

Prior to event:

- Personnel receive an all-expenses-paid invitation to lecture in a foreign nation
- Entities want a summary of the requested presentation or brief 6-12 months prior to the lecture date
- Host unsuccessfully attempted to visit facilities in the past
- Travel to event may pose targeting opportunities

During event:

- Telephone monitoring and hotel room intrusions
- Conversations involving classified, sensitive, or export-controlled technologies or products
- Excessive or suspicious photography and filming of technology and products
- Casual conversations during and after the event hinting at future contacts or relations
- Foreign attendees' business cards do not match stated affiliations
- Attendees wear false name tags

### **Countermeasures**

The following countermeasures can be taken by cleared defense contractors to guard against this collection method:

- Consider what information is being exposed, where, when, and to whom
- Provide employees with detailed travel briefings concerning:
  - The threat
  - Precautions to take
  - How to react to elicitation
- Take mock-up displays instead of real equipment
- Request a threat assessment from the program office
- Restrict information provided to only what is necessary for travel and hotel accommodations
- Carefully consider whether equipment or software can be adequately protected

*If you suspect you may have been targeted using this method, contact your FSO.  
For further information, refer to the Counterintelligence section of the DSS website at  
[www.dss.mil](http://www.dss.mil).*

## ***Insider Threat***

The insider threat has the potential to inflict the greatest damage of any collection method.

### **Technique**

Targets of the insider threat include:

- Employees
- Contractors
- Anyone with legitimate access to an organization

### **Indicators**

The following are potential espionage indicators:

- Alcohol or other substance abuse or dependence
- Mental health issues
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Financial difficulties
- Unexplained or sudden affluence
- Unreported foreign contact and travel
- Inappropriate, unusual, or excessive interest in classified information
- Misuse of information systems
- Divided loyalty or allegiance to the United States
- Works hours inconsistent with job assignment
- Repeated security violations
- Reluctance to take polygraph

### **Countermeasures**

The following countermeasures can be taken by cleared defense contractors to guard against the insider threat:

- Provide training on the insider threat
- Brief employees on elicitation methods
- Brief employees to be alert to actions of other employees
- Monitor the activities of foreign visitors for indications that they are targeting company personnel
- Require personnel to sign a legally enforceable non-disclosure agreement
- Limit the dissemination of sensitive information based on need-to-know
- Monitor classified systems for reportable anomalies

*If you suspect your facility may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at [www.dss.mil](http://www.dss.mil).*

## ***Foreign Visits***

### **Technique**

Suspicious contact during a foreign visit can occur at any time and may come from:

- One-time visitors
- Long-term visitors
  - Exchange employees
  - Official government representatives
  - Students
- Frequent visitors
  - Sales representatives
  - Business associates

### **Indicators**

Suspicious or inappropriate conduct during foreign visits can include:

- Requests for information outside the scope of what was approved for discussion
- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information and becoming irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed

***If you suspect you may have been a target of this method, report it to your FSO.***

### **Countermeasures**

The following countermeasures can protect cleared defense contractors against unauthorized access by foreign visitors:

- Contractors may coordinate with DSS prior to visit
- Prior to visit, brief hosts and escorts on approved procedures
- Walk visitor route and identify vulnerabilities
- Prior to the visit, notify all employees about the visit, restrictions on the visitors, and the nature of the threat
- Debrief personnel in contact with visitors
- Ensure visitors do not bring recording devices, including cell phones, into the facility

***If you suspect your facility may have been targeted using this method, contact your FSO.***

***For further information, refer to the Counterintelligence section of the DSS website at [www.dss.mil](http://www.dss.mil).***

## ***Solicitation and Seeking Employment***

The solicitation and seeking employment collection method may take many forms including, but not limited to, joint ventures or research partnerships, offering of services, or internship programs for foreign students.

### **Technique**

- Places foreign personnel in close proximity to cleared personnel
- Provides opportunity to build relationships that may be exploited
- Places adversary inside facility to collect information on desired technology

### **Indicators**

Indicators include:

- Foreign visitors transmit documents written in a foreign language to a foreign embassy or foreign country
- Foreign visitors request:
  - Access to the LAN
  - Unrestricted facility access
  - Company personnel information

***If you suspect you may have been a target of this method, report it to your FSO.***

### **Countermeasures**

The following countermeasures may guard against this collection method:

- Review all documents being transmitted; use a translator, when necessary
- Provide foreign representatives with stand-alone computers
- Share the minimum amount of information appropriate to the scope of the joint venture/research
- Educate employees extensively
  - Project scope
  - Handling and reporting elicitation
  - Sustainment training
- Refuse to accept unnecessary foreign representatives into the facility
- Develop a Technology Control Plan (TCP)

***If you suspect your facility may have been targeted using this method, contact your FSO.***

***For further information, refer to the Counterintelligence section of the DSS website at [www.dss.mil](http://www.dss.mil).***