
Reporting the Threat
INSIDER THREAT
Counterintelligence Awareness Tips for Attending
Conferences, Conventions, and Trade Shows
Counterintelligence Integration
Counterintelligence
ELICITATION & RECRUITMENT
CI
COUNTERINTELLIGENCE
Best Practices for Cleared Industry
threat
CI INTEGRATION
CONVENTIONS,
& TRADE SHOWS
preparing for
foreign visitors
preparing
for
foreign
visitors
COUNTERINTELLIGENCE
foreign travel vulnerability
elicitation & recruitment
REPORTING
THE THREAT
insider
threat
CI AWARENESS
insider threat
CYBERSECURITY
counterintelligence
INTEGRATION
counterintelligence awareness
vulnerability
Preparing for FOREIGN VISITORS
cyber

COUNTERINTELLIGENCE AWARENESS

What is the Threat?

United States' cleared industry is a prime target of many foreign intelligence collectors and foreign government economic competitors. Cleared employees working on America's most sensitive programs are of special interest to other nations.

The number of reported collection attempts rises every year, indicating an increased risk for industry. While any geographic region can target sensitive or classified U.S. technology, the Defense Security Service (DSS) has consistently found that the majority of suspicious contacts reported by cleared industry originate from East Asia and the Pacific region.

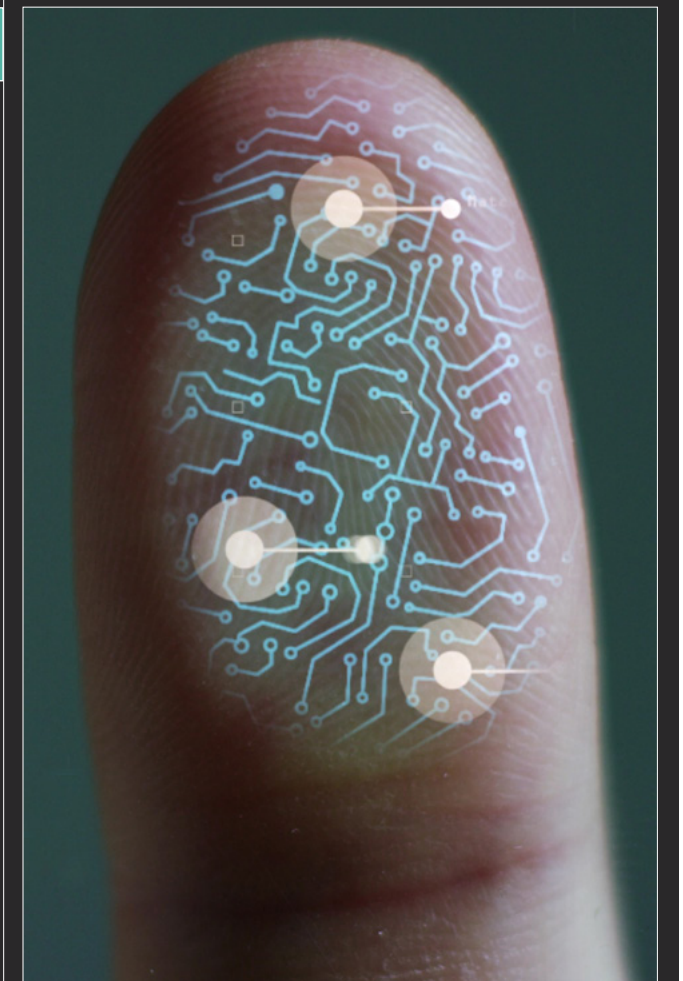
However, every region has active collectors. Cleared contractors should remain vigilant regardless of the collector's assumed country of origin.

The nature and extent of industry reported suspicious contacts suggest a concerted effort to exploit cleared contractors for economic and military advantage. These contacts range from outright attempts to steal technology to seemingly innocuous business ventures.

The exploitation of cyberspace continues to be a key area of concern. The potential for blended operations where cyberspace contributes to traditional tradecraft presents the greatest risk to cleared industry. An increase in unsolicited contacts made with cleared industry employees from compromised accounts amplifies the potential for compromise of cleared individuals, classified programs, or classified systems occurring in the unclassified cyber domain.

Through analysis of industry reporting, DSS has found that foreign intelligence services utilize both commercial and government-affiliated entities.

- The large number of commercial contacts likely represents an attempt by foreign governments to make the contacts seem more innocuous by using non-governmental entities as surrogate collectors
- The number of government-affiliated contacts is likely due to foreign governments' increased reliance on government-affiliated research facilities that contact cleared U.S. contractors under the guise of information-sharing



Who is Being Targeted?

Foreign collectors may target anyone with access to the targeted information, knowledge of information systems, or security procedures. Potential targets are not limited to but often include:

- **Developers**: Scientists, researchers and engineers researching and applying new materials or methods to defense and other leading edge technologies
- **Technicians**: Engineers or specialists that operate, test, maintain, or repair targeted technologies
- **Production personnel**: Personnel with access to production lines or supply chain of targeted technologies
- **IT personnel**: Systems administrators or others with access to cleared facility networks and knowledge of network security protocols
- **Business development personnel**: Marketing and sales representatives
- **Human resources personnel**: HR representatives with access to personnel records
- **Facility personnel**: Anyone with access to a cleared or sensitive facility containing targeted information including security, clerical, maintenance, and janitorial personnel

What Are the Most Common Collection Methods?

Attempted Acquisition of Technology: Includes attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans spec sheets or the like. These often involve email, mail, cold-calling cleared employees, web card submissions, or use of a website's "contact us" application.

>> Indicators of Suspicious Purchase Requests:

- End user is a warehouse or company that organizes shipments for others
- No end-user certificate
- Vagueness of order – quantity, delivery, destination, or identity of customer
- Multiple sales representatives
- Unusual quantity
- Requested modifications of technology
- Rushed delivery date
- No return address
- End user address is in a third country
- Address is an obscure PO Box or residence
- Multiple businesses using the same address
- Buyer requests all products be shipped directly to him/her

Be Alert! Be Aware! Report suspicious activity to your local security official.

COUNTERINTELLIGENCE AWARENESS

- The request is directed at an employee who does not know the sender and is not in the sales or marketing office
- Solicitor is acting as a procurement agent for a foreign government
- Military-specific technology is requested for a civilian purpose
- Company requests technology outside the requestor's scope of business
- Visitors request last-minute change of agenda to include export-controlled technology
- Requestor offers to pick up products rather than having them shipped
- Requestor uses broken English or poor grammar
- Individual has a lack of/no knowledge of the technical specifications of the requested type of technology

Exploitation of Business Activities: Attempts to exploit an existing commercial relationship or establish a commercial relationship in order to obtain access to protected information, technology, or persons. These include joint ventures, partnerships, mergers and acquisitions, foreign military sales, or attempted development of service provider relationships.

Exploitation of Cyber Operations: Attempts to conduct actions to place at risk the confidentiality, integrity or availability of targeted networks, applications, credentials, or data to gain access to, manipulate or exfiltrate protected information, technology, or personnel information.

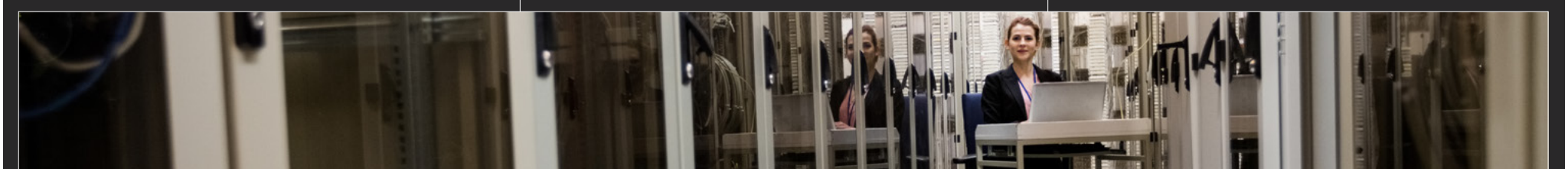
>> **Common Cyber Operation Methods:**

- Phishing operations use emails with embedded malicious content or attachments
- Watering Hole attacks (compromised third party websites) may provide a means for malicious actors to gain unauthorized access to a network or device
- Removable media (USB devices) can provide a means to quickly spread malicious software from a trusted position

Request for Information (RFI)/Solicitation: Direct or indirect attempts to collect protected information by directly indirectly asking, requesting, or eliciting protected information, technology, or persons

>> **Common Methods of Contact for RFI/ Solicitation:**

- Conferences, conventions, or tradeshows – contacts initiated during an event
- Email, mail, telephone, web form
- Foreign visits – Activities or contact occurring before, during, or after a visit to a contractor's facility



Reportable Suspicious Contacts Include:

- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
- Contact between cleared employees and known or suspected intelligence officers from any foreign country
- Any contact that suggests the employee concerned may be the target of an attempted exploitation by a foreign intelligence entity
- Attempts to entice cleared employees into compromising situations that could lead to blackmail, coercion or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
- Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money
- Requests for protected information in the guise of a price quote or purchase

Immediately notify your facility security officer and/or a DSS representative 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.

Be Alert! Be Aware! Report suspicious activity to your local security official.

REPORTING THE THREAT

Reporting Requirements for Cleared Companies

National Industrial Security Program Operating Manual (NISPOM) paragraph 1-302b states, "Contractors shall report efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee."

Cleared contractors must also report actual, probable, or possible espionage, sabotage, terrorism, or subversion promptly to the Federal Bureau of Investigation (FBI) and DSS (NISPOM 1-301).

Although this requirement is not directed to unclassified information or systems, contractors must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on its unclassified information systems. (See Industrial Security Letter 2013-05)

What to Report*

***Note:** Report any of the following incidents if they meet the thresholds of NISPOM paragraphs 1-301, or 1-302a. or b. These lists are not all inclusive. Some of the examples are also considered security violations or personnel security issues, which should be handled in accordance with applicable procedures.*

>> Mishandling of Classified Information

- Removing or sending classified material out of secured areas without proper authorization
- Unauthorized copying, printing, faxing, emailing, or transmitting classified material
- Transmitting or transporting classified information by unsecured or unauthorized means
- Unauthorized storage of classified material, including storage at home
- Reading or discussing classified information in an unauthorized area or over a non-secure communication device
- Improperly removing or changing classification markings
- Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities

>> Misuse of Computer Systems

- Unauthorized network access
- Unauthorized email traffic to foreign destinations
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Use of DoD account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or controlled unclassified information
- Data exfiltrated to unauthorized domains affecting classified information, systems or cleared individuals
- Actual or attempted unauthorized access into U.S. automated information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges

>> Suspicious Cyber Incidents

- Advanced techniques and/or advanced evasion techniques, which imply a sophisticated adversary
- Pre-intrusion aggressive port scanning

- Denial-of-service attacks or suspicious network communication failures
- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning, such as through social networking sites
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage
- Any cyber activity linked to the law enforcement or counterintelligence suspicious indicators provided by the FBI, DSS, Defense Intelligence Agency or by any other cyber centers

>> Foreign Influence

- Undisclosed visits to foreign diplomatic facilities
- Trips to foreign countries inconsistent with an individual's financial ability
- Foreign entities targeting employees traveling overseas via airport screening or hotel room incursions
- Unreported close and continuing contact with a foreign national, including intimate contacts, shared living quarters, or marriage

>> Suspicious Contacts

- Requests for information that make an individual suspicious, including questionable contacts or interaction

>> Suspicious Financial Activity

- Unexplained expensive purchases not reasonably supported by the individual's income
- Sudden unexplained reversal of a negative financial situation or repayment of large debts

>> Recording Devices

- Unauthorized possession of cameras or recording or communication devices in classified areas
- Discovery of suspected surveillance devices in classified areas

Cleared Industry's Role

The technology and information resident in U.S. cleared industry is under constant and pervasive threat from foreign intelligence entities seeking to gain the technological edge.

Increased awareness of the targeted information and methods of operation used by foreign entities is critical to improving our ability to identify and thwart collection attempts.

Timely and accurate reporting from cleared industry is the primary tool DSS uses to identify and mitigate collection efforts targeting information and technology resident in cleared industry.

Immediately report suspicious activities, behaviors, and contacts to your facility security officer.

Be Alert! Be Aware! Report suspicious activity to your local security official.

EXPLOITATION OF BUSINESS ACTIVITIES

What is Exploitation of Business Activities?

Attempts to establish a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service providers.

Attempts to leverage an existing commercial relationship in order to obtain access to protected information, technology, or persons.

What are the Primary Methods of Exploitation?

- Personal contact
- Cultural commonality
- Foreign visits
- Foreign military sales
- Direct commercial sales
- Conferences, conventions, or tradeshows
- Cyber operations
- Email requests
- Business propositions and solicitations
- Academic solicitations
- Web form submissions
- Joint ventures
- Official agreements
- Social networking services

Who is Being Targeted?

Any company with cleared, that works in support of cleared facilities, or that works with sensitive, restricted, or classified information relating to the Department of Defense (DoD) or other U.S. Government agencies' programs or systems.

Foreign collectors, or their agents, often target **employees involved in business development, sales, marketing, information sharing, or other "professional collaborative efforts"** in order to develop a relationship.

Once such an entity establishes a business relationship, they seek to take advantage of that relationship to contact other cleared employees working with targeted information and technology.

Why is it Effective?

Foreign entities exploit legitimate activities with defense-oriented companies to obtain access to otherwise denied information, programs, technology, or associated U.S. personnel. This method of operation relies on the appearance of legitimacy provided by the established commercial or business activity.

Conversely, U.S. company personnel, cleared or not, seeking to build positive relationships and gain future business with foreign partners, may unwittingly provide information beyond the scope of the business activity for which the relationship exists.

>> Five examples of how this exploitation can be effective are illustrated below:

- Foreign ownership of, or financial interest in, a U.S. company may provide access to intellectual property rights held by the U.S. company;
- Business activity may allow the foreign company access to information on the U.S. company's network;
- Foreign-produced hardware and software sold to a cleared company may include design vulnerabilities that could provide foreign actors access to a company's networks and information;
- Foreign collectors prey upon cleared employees' eagerness to develop or expand commercial relationship to increase sales or revenues;

- A joint venture with a foreign company formed using the U.S. company's name, allowing foreign employees to use the U.S. company's name on business cards;
- Cleared employees not informed and educated on the business and security limits of the commercial agreement or the export control restriction of technology may commit a security violation by unwittingly providing information that should not be shared, based on the established relationship.

How Can You Recognize It?

A business relationship with a foreign company or person may be entirely legitimate. However, in many cases, foreign entities with nefarious motives and intent build relationships or abuse existing relationships with U.S. industry to establish pathways to restricted information and technology. Building on apparent legitimate business activity, foreign collectors abuse the relationship as a vector to the restricted or prohibited information.

>> These commercial and business relationships include:

- Misrepresenting themselves as a foreign representative for a U.S. company;
- Selling and installing hardware or software in cleared contractor or sensitive facilities or networks;
- Buying a substantial or majority interest in U.S. companies to gain intellectual property rights for technology, as well as to share data or appoint key management personnel in the acquired company.

>> Eight examples of potentially suspicious exploitation scenarios are presented below:

- Foreign company has a nebulous business background;
- Foreign company attempts to obscure ties to a foreign government;
- Foreign company attempts to acquire interest in companies or facilities inconsistent with their current business lines;
- Foreign partner/client requests to visit cleared facility not related to the business relationship;

Be Alert! Be Aware! Report suspicious activity to your local security official.

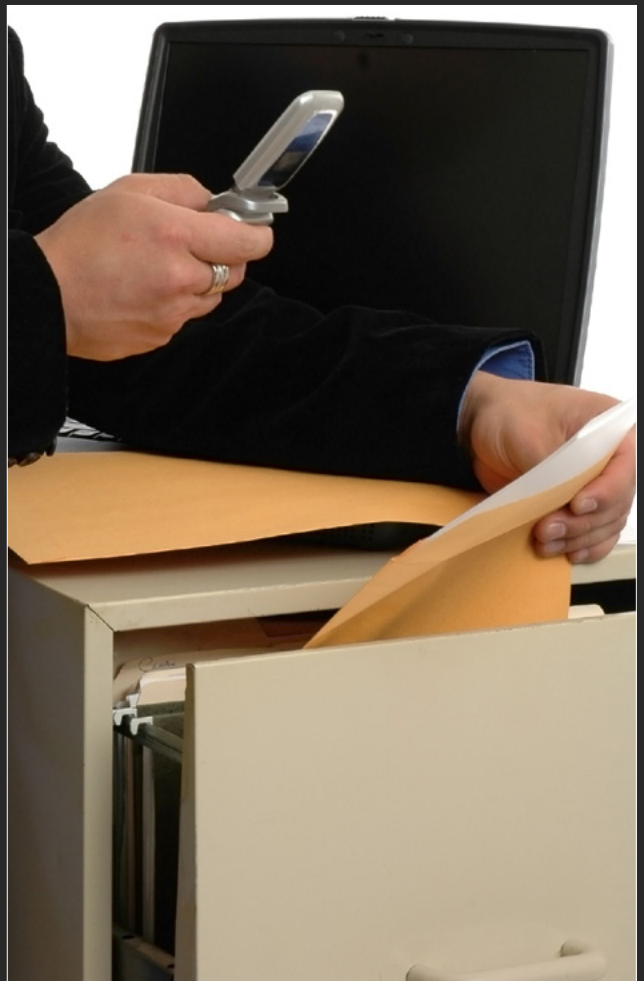
EXPLOITATION OF BUSINESS ACTIVITIES

- Foreign visitors violate security protocols during visits to cleared facilities, or change the members of a visiting delegation at the last minute;
- Foreign company seeks to establish joint ventures with cleared companies to act as U.S. company's representative in foreign markets;
- Foreign company (including companies from countries subject to sanctions) attempts to use a subsidiary in a third country to establish business relationships or buy interests in a cleared U.S. company;
- Foreign company targets U.S. cleared employees, or those working in support of cleared companies, for information beyond the scope of the current relationship or offers partnership with the cleared or sensitive company during conferences, conventions, exhibits, or tradeshows.

Countermeasures

To mitigate foreign partners' or clients' ability to gain access to restricted information or technology, U.S. cleared companies have many options available to them. Below are just six examples of such options:

- Ensure all employees interacting with foreign partners know the specifics of the relationship and what information, equipment, and technology they can share and cannot share, and understand the requirements to report "suspicious activity;"
- Ensure security protocols are in place and adhered to for access to the facility, assembly/ production line, and networks, and are all periodically reviewed and updated;
- Prior to receiving foreign visitors, ensure the facility and the personnel are prepared for the visit, including appropriate briefings, and submit names of the visitors to DSS prior to the visit;
- Ensure employees attending conferences, conventions, exhibits, or tradeshows know what information they can share with potential partners and clients, and are aware of their reporting requirements regarding any suspicious contacts;



- Cleared companies owned by foreign companies should develop and implement appropriate foreign ownership, control or influence (FOCI) mitigation procedures in consultation with DSS to insulate sensitive information from unauthorized foreign entities;
- Proactively engage with your designated DSS representative on a regular basis and remain familiar with foreign collection trends and reporting requirements.

Reporting

A foreign partner (current or prospective), client, or owner attempting to leverage a business activity to obtain unauthorized access to classified information to compromise a cleared employee constitutes a suspicious contact, and is reportable by cleared companies to DSS under the terms of the NISPOM 1-302b.

DSS annually produces an informative publication, Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting. This document includes many examples of reporting trends and technological issues of interest from foreign perspectives, which lead to suspicious contacts.

>> Common examples of reportable activity are provided below, but many more exist:

- Foreign partners or clients improperly requesting protected information under the auspices of an existing business relationship
- Suspicious activity by foreign partner representatives during visits to cleared facilities
- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee

Successful exploitation of business activity can have a catastrophic impact on national security and have adverse business ramifications for the targeted company and its subsidiaries.

It is vital that suspicious incidents are promptly and appropriately reported, including those involving foreign corporate partners or clients, to the company's facility security officer and, when warranted, the DSS representative.

Be Alert! Be Aware! Report suspicious activity to your local security official.

EXPLOITATION OF GLOBAL SUPPLY CHAIN

What is Exploitation of Global Supply Chain?

Activities of foreign intelligence entities or other adversarial attempts aimed at compromising and or sabotaging the supply chain. Some examples of supply chain exploitation may include, but are not limited to, the introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to protected data, to alter data, to disrupt operations, to interrupt communication, reverse engineer, or otherwise cause disruption to the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of an equity.

A supply chain consists of a network of suppliers, manufacturers, developers, warehouses, distribution centers, transportation vehicles, and wholesale or retail outlets. The supply chain may be global and also includes the designers, producers, shippers, and resellers that create, distribute or in any other way have the ability to influence the product.

Organizations should protect against supply chain threats to the affected information system, system component, or information system service by employing a standardized process to address supply chain risk as part of a comprehensive, defense-in-breadth information security strategy.

What are the Primary Methods of Exploitation?

- Cyber operations
- Personal contact
- Phishing operations
- Academic and professional résumé submissions

Who is Being Targeted?

Any cleared contractor supplying or installing complete systems or components for DoD or other government agency's systems, equipment, facilities, or procurement programs.

- **Acquisition and procurement**: Personnel purchasing components to include microelectronics for use in the production or maintenance of U.S. Government systems, programs, or technology
- **Design, Manufacturing, and Assembly**: Personnel with access to manufacturing lines or supply chain of U.S. Government programs, projects, and systems

- **Technicians**: Personnel accessing U.S. Government equipment or systems conducting routine maintenance or incorporating new components in existing systems/equipment

Why is it Effective?

Successful exploitation of supply chain would allow foreign agents, or personnel acting on their behalf, to manipulate components intended for DoD systems, degrading DoD capabilities and effectiveness during potential conflicts, or to gain access to sensitive information.

Nonconforming components will not perform to specification and can include malicious logic intended to degrade or destroy DoD systems and could cause events ranging from injury, to loss of life, to compromise of national security.

- Nonconforming parts are often difficult to identify compared to authentic components
- An actor with insider access could introduce malicious changes or substitutions with a nonconforming part during any phase, increasing the difficulty in identifying potential malfeasance
- During the design and manufacturing phases, an actor could perform a series of malicious changes, to include: Gate level changes, protocol changes, parameter modifications, wiring modifications, etc
- During the sustainment phase, limited sources for obsolescent components may lead to manufacturers receiving nonconforming parts via gray market suppliers

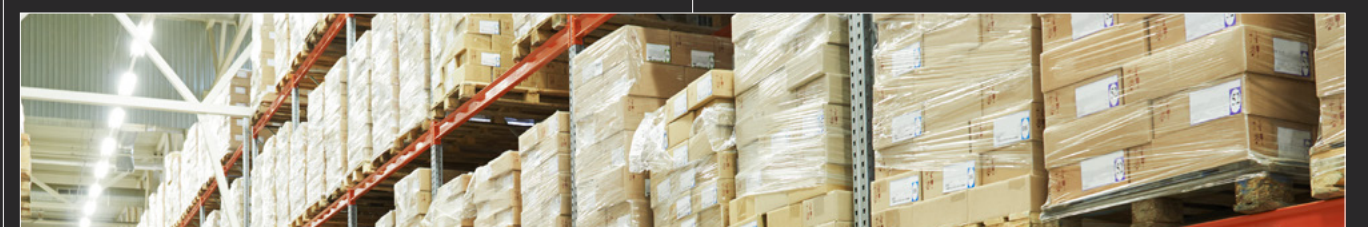
How can you Recognize it?

Exploitation of the global supply chain can occur at any phase during the process.

- During design and manufacturing, personnel should use trusted and controlled distribution, delivery, and warehousing options.
- During sustainment, personnel should also be aware of signs of tampering with shipping containers, and establish protocols to include the lindependent verification and validation of microelectronics, and in particular microelectronics obtained outside of authorized vendors (e.g., obsolete microelectronics).

>> Signs of a compromised supply chain may include any of the following:

- Exhibits functionality that was outside the original design
- A device, or multiple devices, from a lot, that exhibits a unique error or failure
- Employees violating security protocols for handling of components, or introducing non-compliant components
- Dealers offering rare or out of production components at low prices



Be Alert! Be Aware! Report suspicious activity to your local security official.

EXPLOITATION OF GLOBAL SUPPLY CHAIN

- Dealers offering short lead times for large orders of components
- Shipping containers show signs of tampering

Countermeasures

>> To mitigate tampering with components at the cleared facility during assembly and production:

- Ensure security protocols are in place and adhered to for access to the facility, assembly and production lines, and networks
- Establish and maintain an effective insider threat program
- Train workforce to identify and promptly report suspicious activities

>> To mitigate the threat of counterfeit components:

- Use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods
- Integrate acquisition offices with other offices including the information assurance and security offices
- Ensure sub-contractor or off-site production facilities conduct effective supply chain risk management
- Create incentives for suppliers who: implement required security safeguards, promote transparency into their organizational process and security practices, provide additional vetting of the processes and security practices of sub-suppliers, restrict purchases from specific suppliers, and provide contract language regarding the prohibition of uncompromised or counterfeit components
- Always use independent verification and validation for obsolete microelectronics and vet external testing houses;
- Consider lifetime buys for components to avoid purchasing grey market nonconforming parts.

Reporting

The introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to classified information, to alter data, disrupt operations, or to interrupt communications related to classified contracts or cleared constitutes a "suspicious contact," and is reportable by cleared companies to DSS (NISPOM 1-302b).

>> Examples of reportable activity include:

- Devices that exhibit functionality that was outside the original design
- A device, or multiple devices from a lot, that exhibits a unique error or failure
- Inadvertent or deliberate attempts to break a trusted chain of custody
- Introduction of counterfeit components into a U.S. Government system during production
- Unauthorized personnel of any nationality accessing restricted areas of a cleared facility involved in the production of components for DoD systems
- Efforts by any individual, regardless of nationality, to compromise a cleared employee involved in manufacturing, assembling, or maintaining DoD systems

Successful exploitation of supply chain can have a catastrophic impact. It is vital that personnel promptly report suspected incidents to their facility security officer or DSS representative.

Be Alert! Be Aware! Report suspicious activity to your local security official.

EXPLOITATION OF INSIDER ACCESS

What is an Insider Threat?

Insiders: Any person with authorized access to any government or contract resource to include personnel, facilities, information, equipment, networks or systems. This can include employees, former employees, consultants, and anyone with access.

Insider Threat: The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities.

Why is it Effective?

Insiders have arguably caused more damage to the security of the United States than foreign intelligence officers, and with today's technological advances, they have the ability to cause more harm than ever before. What used to take years to collect now takes minutes because of the increased use of removable media.

Insiders are often aware of your company's vulnerabilities and can exploit that knowledge to their benefit. Not every suspicious circumstance or behavior represents an insider threat, but every situation needs to be examined to determine potential risk.

An insider can have a negative impact on national security and industry resulting in:

- Loss or compromise of classified or controlled sensitive information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Physical harm or loss of life

How can you Recognize it?

Detecting potentially malicious behavior among employees with access to classified or controlled sensitive information involves gathering information from many sources and analyzing that information for clues or behaviors of concern. In most cases, co-workers admit they noticed questionable activities but failed to report incidents because they did not recognize the pattern and did not want to get involved or cause problems for their co-workers.

A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be evident.

Ignoring questionable behaviors can only increase the potential damage the insider can have on national security or employee safety. While each insider threat may have different motivation, the indicators are generally consistent.

Potential Espionage Indicators

- Repeated security violations and a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required to do so
- Seeking to gain higher clearance or expand access outside the job scope without bona fide need for the access

- Engaging in classified conversations without a need to know
- Attempting to enter areas not granted access to
- Working hours inconsistent with job assignment or unusual insistence on working in private
- Accessing information not needed for job

Behavioral Indicators*

- Depression
- Stress in personal life
- Exploitable behavior traits:
  - Use of alcohol or drugs
  - Gambling
- Financial trouble
- Prior disciplinary issues

*These behaviors may also be indicative of potential workplace violence.

Examples of Reportable Behaviors:

>> Information Collection

- Keeping classified materials in an unauthorized location (e.g., at home)
- Attempting to access classified information without authorization
- Obtaining access to sensitive information inconsistent with present duty requirements
- Questionable downloads
- Unauthorized use of removable media

>> Information Transmittal

- Using an unclassified medium to transmit classified materials
- Discussing classified materials on a non-secure telephone or in nonsecure emails or text messages
- Removing the classification markings from documents
- Unnecessary copying of classified material

>> Foreign Influence

- Expressing loyalty to another country
- Concealing reportable foreign travel or contact

Reporting

You are the first line of defense against insider threats. Help protect our national security by reporting any suspicious behavior that may be related to an insider threat.

Each employee has a responsibility to ensure the protection of classified and controlled sensitive information entrusted to them.

Be aware of potential issues and the actions of those around you and report suspicious behaviors and activities to your local security official.

Be Alert! Be Aware! Report suspicious activity to your local security official.

PERSONAL CONTACT

What is a Personal Contact?

Person-to-person contact via any means where the target is in direct or indirect contact with an agent or co-optee of the targeting entity.

What are the Primary Methods of Exploitation?

This method of contact is associated with all methods of operation applied by foreign entities targeting cleared industry. Those with the highest risk include:

- Exploitation of Commercial/Business Activities
- Exploitation of Insider Access
- Exploitation of Security Protocols
- RFI/Solicitation
- Exploitation of Relationships
- Search/Seizure

Who is Being Targeted?

Foreign collectors will target anyone with access to the desired information, knowledge of information systems, or security procedures. This includes but is not limited to:

- **Developers**: Scientists, researchers, engineers researching and applying new materials or methods to defense and other leading edge technologies
- **Technicians**: Engineers or specialists that operate, test, maintain, or repair targeted technologies
- **Production personnel**: Personnel with access to production lines or supply chain of targeted technologies
- **IT personnel**: Systems administrators or others with access to targeted facility networks and knowledge of network security protocols
- **Business development personnel**: Marketing and sales representatives
- **Human resources personnel**: HR representatives with access to personnel records
- **Facility personnel**: Anyone with access to a cleared or sensitive facility containing targeted information including security, clerical, maintenance, and janitorial personnel

Why is it Effective?

Foreign intelligence officers are trained in elicitation tactics; their job is to obtain protected information. Non-traditional collectors, such as business and academic contacts, will leverage existing relationships to obtain restricted information outside the scope of the relationship. Because of this, not all elicitation attempts are obvious to the target.

The trained elicitor and the non-traditional collectors will try to exploit natural human tendencies, including:

- The desire to be polite and helpful, even to strangers or new acquaintances
- The desire to appear well informed, especially about our profession
- The tendency to expand on a topic when given praise or encouragement; to show off
- The tendency to correct others
- The tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used
- The tendency to believe others are honest; a disinclination to be suspicious of others

How can you Recognize it?

The approach, both by trained intelligence professionals and non-traditional collectors, will usually be subtle. Some likely indicators of this method of contact include:

- Business contact requesting information outside of the scope of contract, or through an increased or gradual progression of information initiated from legitimately authorized business discussions
- Hidden or obscured end use or end user information
- Offer of paid attendance at an overseas conference
- Casual acquaintance appears to know more about your work or project than expected
- A casual contact shows unusual interest in your work, facility, personnel, or family details

Countermeasures

In the event you believe a personal contact has requested restricted information or attempts to place you into an exploitable situation, be prepared and know how to respond. Know what information you cannot share and be suspicious of those who seek such information.

Do not share anything the elicitor is not authorized to know, including personal information about yourself, your family, or your co-workers.

If you believe someone is attempting to elicit information from you, you can:

- Change the topic
- Refer them to public websites
- Deflect the question
- Provide a vague answer
- Explain that you don't know

What to Report

Personal contact is the vector for many intelligence methods of operation which constitute "suspicious contact," and are reportable by cleared companies to DSS (NISPOM 1-302b), and should be promptly reported.

Examples of reportable activity include:

- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized
- access to sensitive or classified information or to compromise a cleared employee
- All contacts with known or suspected intelligence officers from any country
- Any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country
- Business contact requesting information outside the scope of established contracts/agreements
- Business or personal contact asking for information about your co-workers
- Business or personal contact requesting you to violate a company policy or security procedures

Because elicitation can be subtle or requests from personal contacts may seem innocuous, you should report any suspicious conversations to your facility security officer or DSS representative.

Be Alert! Be Aware! Report suspicious activity to your local security official.

FOREIGN VISITS

What is the Foreign Visit Method of Contact?

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.

What are the Primary Methods of Exploitation?

>> Foreign collectors' 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 NISPOM, 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 DSS 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

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 DSS 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 DSS representative.

Be Alert! Be Aware! Report suspicious activity to your local security official.

ACADEMIC SOLICITATION

What is Academic Solicitation?

Academic solicitation is one of the fastest growing methods of operation reported by cleared contractors. The number of foreign academics requesting to work with classified programs continues to rise, and the academic community will likely remain a top target for the foreseeable future.

DSS defines academic solicitation as the use of students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information. These attempts can include requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; requests for and access to software and dual-use technology; or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees.

Foreign intelligence entities exploit unsuspecting professors and researchers to gain access to sensitive or classified information and technology.

Placing academics at, and requesting to collaborate with, U.S. research institutions under the guise of legitimate research offers access to developing technologies and cutting-edge research. Any such placement and information learned would not only satisfy the collectors' immediate technological requirements, but also result in better educated scientists and researchers for indigenous technology development.

Most of these contacts are likely legitimate. However, some foreign academics may ultimately take advantage of their placement and access to further national research and development goals. In such cases, foreign nationals studying under or regularly interacting with cleared employees engaged in classified research and development pose a threat to U.S. government sponsored basic and applied research.

It is imperative for academics to be familiar with, and comply with, the laws, regulations and procedures governing the restrictions on sharing classified, or export-controlled, technologies and information with foreign students or academics.

Who is Being Targeted?

- Subject matter experts teaching technical courses

- Researchers and scientists conducting classified research on behalf of a U.S. Government customer
- Researchers, scientists, and subject matter experts employed at cleared components of academic institutions
- Researchers, scientists, and subject matter experts with unclassified work published in scientific or technical journals or presented at science conferences

What are they After?

- Classified, sensitive, or export-restricted basic and applied research
- Developing defense or dual-use technologies

- Information about the students, professors, and researchers working on the technologies

Why is it Effective?

Academic solicitation is an effective way of collecting information due to the collaborative nature of the academic community.

- U.S. universities and research institutions regularly host foreign students to help cultivate their technical abilities without realizing that this free-flowing exchange of information can place the U.S. technological infrastructure at risk. Home countries can exploit their student's access to supplement intelligence collection efforts against emerging U.S. DoD and civilian technical research.
- U.S. researchers that receive unsolicited requests to review scientific publications readily provide feedback with the hopes of reviewing the resulting findings. However, any feedback provided may confirm or refute scientific hypotheses.
- Foreign intelligence entities use foreign students who are already knowledgeable about targeted academic fields to collect
- Foreign students and professors target U.S. students and researchers who are knowledgeable in the desired field
- It is often difficult to discern the legitimate contacts from those that represent nefarious attempts to gain access to sensitive or classified information or technology

Common Scenarios

- Foreign students accepted to a U.S. university or at postgraduate research programs are recruited by their home country to collect information, and may be offered state-sponsored scholarships as an incentive for their collection efforts
- U.S. researchers receive requests to provide dual-use components under the guise of academic research
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research
- U.S. professors or researchers are invited to attend or submit a paper for an international conference
- Overqualified candidates seeking to work in cleared laboratories as interns
- Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual's field of research
- Intelligence entities will send subject matter expert requests to review research papers, in hopes the expert will correct any mistakes

What to Report

Any contact (i.e., emails, telephone, personal contact) that is suspicious because of the manner or subject matter of the request. This may include requests from U.S. persons, or from foreign nationals located in the United States or abroad, and may consist of:

- Unsolicited applications or requests for undergraduate, graduate, postgraduate or other research positions
- Unsolicited requests for access to research papers or other research-related publications or documents
- Unsolicited requests for assistance with or review of thesis papers, draft publications or other research-related documents
- Unsolicited invitations to attend and/or present at international conferences

Be Alert! Be Aware! Report suspicious activity to your local security official.

FOREIGN TRAVEL VULNERABILITY

Foreign Travel

You can be the target of a foreign intelligence or security service at any time and in any place; however, the risk is greater when you travel overseas. When overseas, foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders.

While traveling overseas, any information electronically transmitted over wires or airwaves is vulnerable to foreign intelligence services' interception and exploitation. Suspicious entities can easily intercept voice, fax, cellular, data, and video signals.

Many countries have sophisticated eavesdropping/intercept technology and are capable of collecting information we want to protect, especially overseas. Numerous foreign intelligence services target telephone and fax transmissions.

Your diligence determines whether or not our sensitive information is protected from unauthorized disclosure.

What are the primary methods of exploitation?

Overseas travelers are most vulnerable during transit. Travelers should be wary of extensive questioning from airport security, luggage searches, and downloading of information from computers and personal electronic devices.

Travelers should maintain heightened awareness once they reach their destination. Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside their hotel room) may be monitored and recorded.

Entities can analyze their recorded observations for collecting information or exploiting personal vulnerabilities. This information is useful for future targeting and recruitment approaches.

Another favored tactic for industrial spies is to attend tradeshows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment.

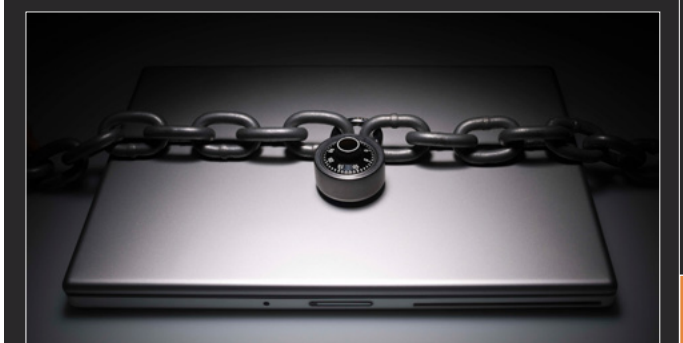
>> Collection Techniques Travelers Should Be Wary of:

- Bugged hotel rooms or airline cabins (including video surveillance)
- Intercepts of fax and email transmissions
- Recording of telephone calls or conversations
- Unauthorized access and downloading, including outright theft of hardware and software

- Installation of malicious software on computers or personal electronic devices
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment or substitution of flight attendants
- Individuals appearing to try and eaves-drop on your conversations
- Individuals attempting to read your computer screen or documents over your shoulder

Countermeasures

- Leave unneeded electronic devices at home
- Use designated travel laptops that contain no sensitive or exploitable information



- Use temporary email addresses not associated with your company
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Encrypt data, hard drives, and storage devices whenever possible
- Use complex passwords
- Enable login credentials on laptops and devices
- Do not publicize travel plans and limit sharing of this information to people who need to know
- Do not post pictures or mention you are on travel on social media until your return
- Attend pre-travel security briefings
- Maintain control of sensitive information, media, and equipment. Pack them in your carry-on luggage and maintain control of them at all times. Do not leave them unattended in hotel rooms or stored in hotel safes
- Keep hotel room doors locked. Note how the room looks when you leave compared to when you return

- Limit sensitive discussions; public areas are rarely suitable for discussion of sensitive information
- Do not use computer or fax equipment at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspicious inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely
- Attend post-travel debriefing and report any and all suspicious activity

Be Alert! Be Aware! Report suspicious activity to your local security official.

CONFERENCES, CONVENTIONS & TRADESHOWS

What is the Conference, Conventions, or Tradeshows 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.

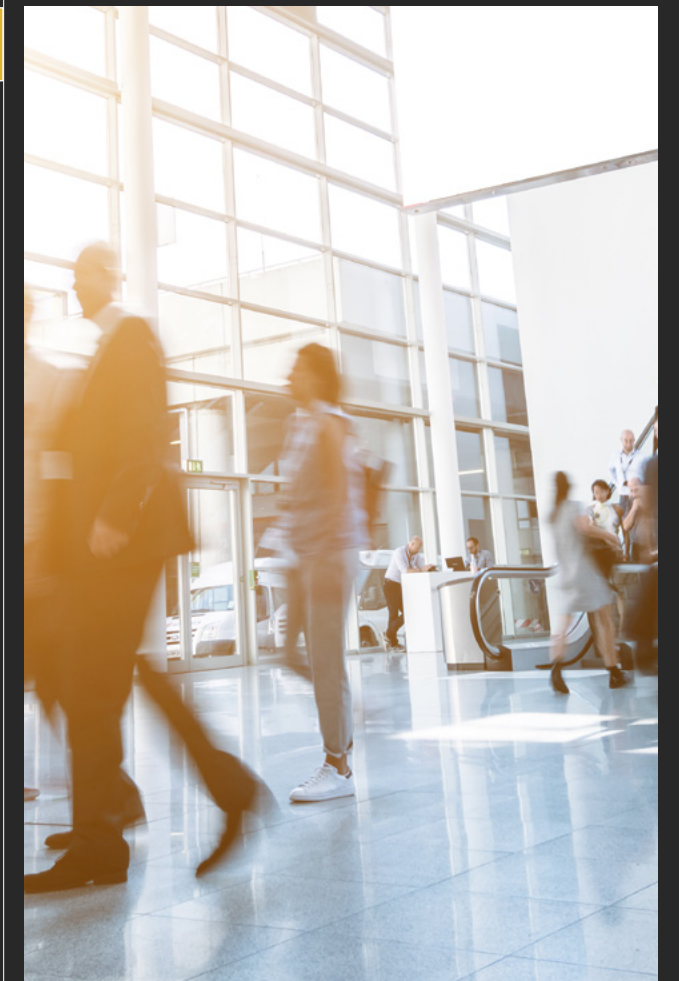
Foreign collectors use many methods to gather information on current and emerging U.S. technology. They may pose as potential customers, attendees, exhibitors, or scientists, and even as a representative of a nation other than their own. Collectors may attempt to directly ask about sensitive or classified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

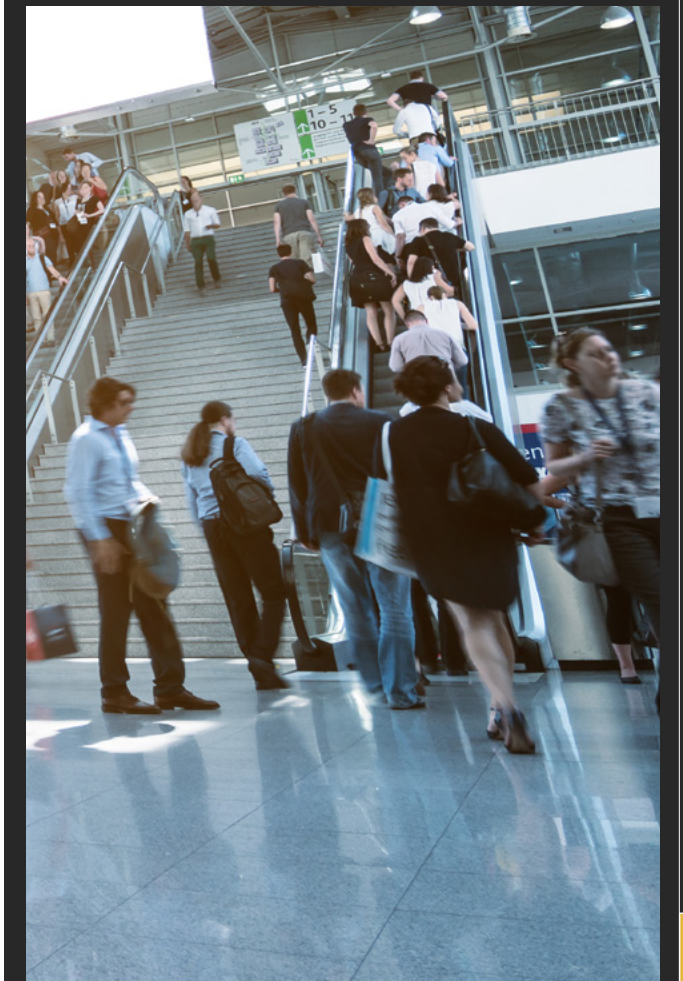
What are the Primary Methods of Exploitation?

- 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 anyone with access to the targeted information and technology, or 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, 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.

Be Alert! Be Aware! Report suspicious activity to your local security official.

CONFERENCES, CONVENTIONS & TRADESHOWS

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 intheir 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, and 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.

Be Alert! Be Aware! Report suspicious activity to your local security official.

CYBER THREATS

Why Are You a Target?

- Publicly available information helps foreign intelligence entities identify people with placement and access.
  - Contract information (bid, proposal, award or strategies)
  - Company website with technical and program information
  - Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or non-cleared companies
- Employee association with companies or technologies made public through scientific journals, academia, public speaking engagements, social networking sites, etc.

What Do They Target?

- Company unclassified networks (internal and extranets), partner and community portals, and commonly accessed websites
- Proprietary information (business strategy, financial, human resource, email, and product data)
- Export-controlled technology
- Administrative and user credentials (usernames, passwords, tokens, etc.)
- Foreign intelligence entities seek the aggregate of unclassified or proprietary documents which could paint a classified picture

How Do They Compromise Networks, Systems, and Technical Data?

Reconnaissance: Research phase used to identify and select targets by browsing websites to obtain names, emails, business and social relationships, and technical information.

Weaponization: The foreign intelligence entities assemble the payload and wrapper, such as coupling a remote access exploit with a prepared spear-phishing email.

Delivery: The foreign intelligence entity infects the target, most commonly using email, website hijacking, or removable media (through insiders).

Exploitation: Successful compromise of targeted vulnerability to allow malicious code to be run.

Installation: Executed malicious code inserts malware, such as a Remote Access Trojan or opens a backdoor connection to the target system – may allow for persistence.

Command and Control: The malware will communicate to a controller server to send or receive instructions from the foreign intelligence entity.

Actions on the Objective: After completing the above actions, the foreign intelligence entity can fulfill their requirements. Intelligence requirements can range from exfiltration, using the system as a strategic position to compromise additional systems within the targeted network (hop-point), or sabotaging the system and network.

Countermeasures

>> Employees

- Remember that everyone is a potential target
- Use complex passwords, change them regularly, and don't reuse
- Be wary when connecting with unknown individuals on social networking sites
- Spear-phishing can happen on any account, including personal email accounts
  - Do not open emails, attachments, or click links from unfamiliar sources, even if they look official

>> IT Department & Management

- Train all personnel on:
  - Spotting a spear phishing, phishing, or whaling email attempt
  - Social networking site connections
  - Proper cyber security procedures and concerns
- Implement defense-in-depth: a layered defense strategy that includes technical, organizational, and operational controls
- Implement technical defenses: firewalls, intrusion detection systems, internet content filtering, and a DNS proxy
- Update your anti-virus software daily and download vendor security patches for all software
- Do not use manufacturers' default passwords on software or hardware
- Monitor, log, analyze and report attempted and successful intrusions to your systems and networks – even unsuccessful intrusions present a counterintelligence value!
- Maintain open communication between company counterintelligence and network defense personnel. Defense only is not a comprehensive strategy

What to Report

- Advanced techniques and/or advance evasion techniques, which imply a sophisticated adversary
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Pre-intrusion aggressive port scanning
- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning, such as through social networking sites
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. automated information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltrated to unauthorized domains affecting classified information, systems or cleared individuals
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Unauthorized email traffic to foreign destinations
- Use of DoD account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or controlled unclassified information
- Any cyber activity linked to suspicious indicators provided by DSS, or by any other cyber centers and government agencies

Reportable activities are not just limited to those activities that occur on classified information systems. Industrial Security Letter 2013-05 (which NISPOM paragraph 1-301) instructs cleared U.S. companies that they must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on unclassified information systems.

NISPOM paragraph 1-302b reminds cleared U.S. companies that they "shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.

Be Alert! Be Aware! Report suspicious activity to your local security official.

COUNTERINTELLIGENCE

Defense Security Service
www.dss.mil

National Counterintelligence and Security Center
https://www.dni.gov/index.php/ncsc-home