COUNTERINTELLIGENCE

Best Practices for Cleared Industry

About the DEFENSE SECURITY SERVICE

Defense Security Service Mission

The Defense Security Service (DSS) supports national security and the warfighter through our security oversight and education missions. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program and serves as the functional manager for the Department of Defense (DoD) security professional development program.

>> Five Primary Tasks:

- Clear industrial facilities, accredit associated information systems, and administer aspects of the industrial portion of the DoD Personnel Security Program
- Collect, analyze, and provide threat information to cleared industry and government partners
- Provide advice, assistance, and oversight to cleared industry
- Manage foreign ownership, control, or influence in cleared industry
- Deliver security education and training

Role of DSS Counterintelligence

The DSS Counterintelligence (CI) Directorate seeks to identify and counter unlawful penetrators of cleared U.S. industry to stop foreign attempts to obtain illegal or unauthorized access to classified information and technology resident in the U.S. cleared industrial base.

DSS CI articulates the foreign intelligence threat to U.S. government cleared industry leaders.

DSS CI special agents are deployed across the country to support facility security officers (FSOs) and other cleared industry representatives in recognizing and appropriately reporting unlawful foreign attempts to acquire classified and controlled sensitive technology.

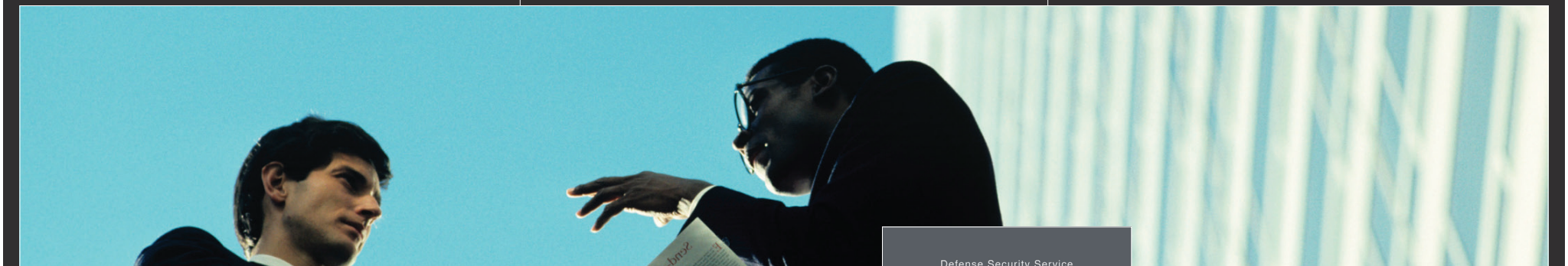
DSS CI's risk-based approach incorporates a realistic assessment of threats to critical DoD research, technology, and classified information, and tailors

CI services through objective criteria and threat categorization to mitigate the risk.

DSS Counterintelligence Mission Areas

>> Threat Awareness

- Provide analysis of foreign threats to help U.S.



cleared industry develop remedial actions to decrease individual and collective risk

- Build awareness and understanding of the threats

>> Referral and Liaison

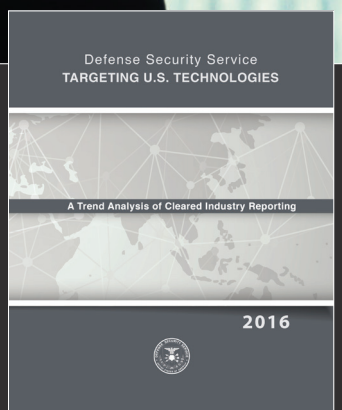
- Evaluate reports of suspicious contacts or activities submitted by cleared industry that present potential threat cases
- Receive, evaluate and when appropriate refer threat reporting from cleared industry to those Department of Defense CI and law enforcement organizations with authority to act against foreign adversaries
- Refer developments to DoD CI and federal law enforcement agencies for further investigation

>> CI Integration

- Provide security awareness and educate cleared industry concerning effective threat identification and reporting

Products

DSS publishes a myriad of analytical threat products:



- **"Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting,"** provides a statistical and trend analysis analyzing the most prolific foreign collectors targeting the cleared contractor community
- Periodic current and anticipatory threat products regarding various programs, companies, and emerging threats
- Cyber alert products concerning the latest threats and the tools used by the adversary in cyberspace

For specific threat information, please contact your facility security officer who will work in conjunction with the local DSS CI special agent.

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

COUNTERINTELLIGENCE AWARENESS: Spotting the Suspicious

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, DSS has consistently found that the majority of suspicious contacts reported by cleared industry originate from East Asia and the Pacific regions.

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.

One of the fastest growing areas of concern is the exploitation of cyberspace for surreptitious access to cleared contractor data systems and cleared individuals. 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 contact reports 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

Collection Methods

Recent industry reporting indicates that while foreign entities continue to use direct and overt means in their attempts to gain access to classified/sensitive information and technologies or to compromise cleared individuals, foreign entities are also returning to indirect collection methods.

>> Cyber Exploitation

- Spear phishing was the most common malware delivery technique; this technique allows the malicious actors to send targeted emails with low risk and potentially high payoff
- Watering Hole attacks (compromised third-party websites) may provide a means for malicious actors to gain unauthorized access to your network or device.
- Removable media (USB devices) can provide a means to quickly spread malicious software from a trusted position
- Use of removable media (USB drives) can initiate attempted intrusions

>> **Attempted acquisition** of and **requests for information** about controlled technology

- Represent a low-risk/high gain method of operation
- Usually involve emailing, mailing, faxing, or cold calling U.S. cleared contractor employees; web-card submissions; or use of a website's "contact us" page

- Collectors ask for everything from price quotes and technical specifications to the outright sale of the technology

>> With **academic solicitation**, foreign students seek post-graduate positions, thesis assistance, or reviews of drafts of scientific publications

>> Representatives of foreign companies often **solicit or market their services** to cleared U.S. companies and offer to market the cleared company's products overseas, provide technical and business services, or seek employment on classified cleared contractor projects

>> During **foreign delegation visits** to cleared facilities, visitors may show up unannounced, attempt to gain access to restricted areas, or add unvetted visitors to their party at the last minute

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 by cleared employees with 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 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 a of price quote or purchase request, market survey, or other pretense

Suspicious Purchase Requests

The following may indicate an attempt by a foreign entity to illegally acquire classified or export-controlled technology or information:

- End user is a warehouse or company that organizes shipments for others
- No end-user certificate
- 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
- Vagueness of order — quantity, delivery destination, or identity of customer
- Buyer requests all products be shipped directly to him/her
- 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

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 FSO.

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

INSIDER THREAT: Combating the Enemy Within Your Organization

What is an Insider Threat?

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 the potential risk.

Definitions

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 the Insider Threat Significant?

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 an Insider Threat?

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 or 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

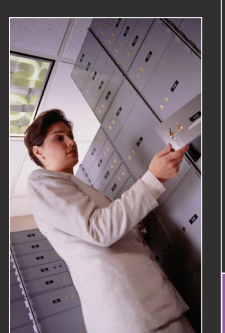
>> Behavioral Indicators *

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

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

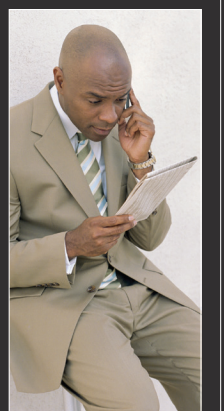
Examples of Reportable Behaviors

>> Information Collection



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

>> Additional Suspicious Behaviors

- Sudden reversal of financial situation or a sudden repayment of large debts or loans

- Being disgruntled to the point of wanting to retaliate
- Repeated or unrequired work outside of normal duty hours
- Bringing an unauthorized electronic device into a controlled area
- Making threats to the safety of people or property

The above list of behaviors is a small set of examples. While not all of these behaviors are definitive indicators that the individual is an insider threat, reportable activities should be reported before it is too late.

How Can You Help?

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.

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

ELICITATION & RECRUITMENT: Can You Recognize It? Report It!

Elicitation

>> What is Elicitation?

Elicitation is the strategic use of conversation to subtly extract information about you, your work, and your colleagues.

Foreign intelligence entities elicit information using both direct and indirect questioning, thereby guiding casual conversations to desired topics. They may create a cover story to explain the line of questioning in their attempts to make the discussion less suspicious.

Elicitation attempts can occur in both work and casual settings; cleared employees need to be wary regardless of the setting.

While elicitation may seem like a technique specific to spy tradecraft, we all use it at some level to gather information about our friends and family (e.g., covertly getting input on gift ideas). Because it is so common, it can be difficult to tell whether it is innocent, friendly conversation or intelligence gathering. Foreign intelligence entities look for anything from details about programs you or your colleagues work on to personal information they can use in future targeting efforts.

Elicitation requires patience and persistence. Pieces of information, collected over an extended period, can provide the final piece of the puzzle to a complex problem or save scarce research money. The aggregate of unclassified data could give the adversary a classified look at technology, programs, and processes.

>> Why is Elicitation So Successful?

Foreign intelligence officers are trained in elicitation tactics; their job is to obtain protected information. Because of this, not all elicitation attempts are obvious to the target.

The trained elicitor understands human behavior and will try to exploit natural 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
- The desire to convert someone to our opinion

>> Deflecting Elicitation Attempts

In the event that you are targeted, you need to 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
- Feign ignorance and ask the elicitor to explain what they know

>> End Game

Elicitation is non-threatening. It is hard to recognize

as an intelligence technique, and it is easy to deny any wrongdoing.

The intelligence officer's ultimate goals are to:

- Collect the pieces of the puzzle that will allow foreign entities to replicate U.S. research or technology
- Find enough information to be able to entice you to provide classified or sensitive information
- Test your willingness to talk about matters of intelligence interest and assess your suitability for recruitment

Recruitment

>> What is Recruitment?

Recruitment is obtaining cooperation from someone to provide sensitive or classified information.

An intelligence service typically conducts recruitment after careful assessment and patient cultivation of the target. By the time the offer to work for the foreign government or entity is made, the intelligence officer is relatively confident of the target's willingness to cooperate and the target is likely aware that a dubious relationship is developing. If the target agrees to the recruitment, that person becomes an agent.

Money is frequently used as a recruitment tool, but there are alternate methods, such as appealing to the target's ideology, ego, or need for revenge, or using blackmail.

Safeguard your actions and words to avoid becoming an easy target. Be honest with yourself about your own vulnerabilities and exploitable behaviors and adjust your lifestyle to close gaps that hostile entities could exploit.

>> Damage Potential

Indisputably, those Americans who have betrayed their country, regardless of whether they volunteered or were recruited, have caused immeasurable damage to the security of the United States. In some cases, lives were lost. In others, persons and their families were ruined. In all cases, lives were irreparably damaged.

Americans who have spied have betrayed a special trust to the country and to their friends, colleagues, and families. Despite their personal rationale for committing espionage, all had other means at their disposal for fulfilling their aspirations, needs, and desires.

Most, if not all, spies eventually regret their actions and their decisions to commit espionage.

Providing classified information to any unauthorized individual is illegal. Espionage against the U.S. government is a very serious crime punishable by imprisonment, fines, or death.

>> Reporting

Elicitation is a "suspicious contact", and is reportable by cleared companies to DSS (NISPOM 1-302b). Examples of reportable activity include:

- Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to 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

Because elicitation is subtle and difficult to recognize, you should report any suspicious conversations to your FSO, DSS industrial security representative, or DSS CI special agent. These individuals can assess your information and determine whether a potential CI concern exists.

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

PREPARING FOR FOREIGN VISITORS

International Visits

International visitors are common in today's global economy and are often a welcome opportunity to boost business. However, cleared contractors need to be aware that there are potential CI vulnerabilities.

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 sensitive and classified information resident in cleared industry.

Research and Development

It is cheaper for foreign entities to illicitly obtain sensitive or classified information and technology than it is to fund the initial research and development (R&D) themselves.

The U.S. government spends more on R&D than any other country in the world, making the U.S. contractors performing R&D a prime target for foreign collection of both classified and unclassified commercial technology.

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

Techniques Visitors Use to Elicit Information

- **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 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

Preparing for Foreign Visitors *

** 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
- Develop standard, acceptable responses to questions that may arise, especially if the projects are sensitive or classified, are not applicable to the country visit, or include proprietary information
- If the delegation attempts to make additional contacts with escorts and speakers, make sure they keep discussions to the agreed-upon topics and information

- 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
- Train escorts on detecting suspicious behavior and questions; ensure they know to maintain visual contact with all visitors at all times
- After the visit, debrief the host and all escorts to uncover any strange and/or suspicious activities exhibited by their visitors or unusual and 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 clear need to know that has been communicated and verified in advance of the visit.

Inform your DSS industrial security representative or DSS 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.

If any suspicious incidents occur during the visit, report them to your FSO immediately.

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

ACADEMIC SOLICITATION

What is Academic Solicitation?

Academic solicitation is the fastest growing method of operation and took over as the primary collection method cleared contractors reported in FY13. 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 experts (SMEs) requests to review research papers, in hopes the SME 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.

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/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

Preferred Tactics

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 trade shows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment.

Computer Security

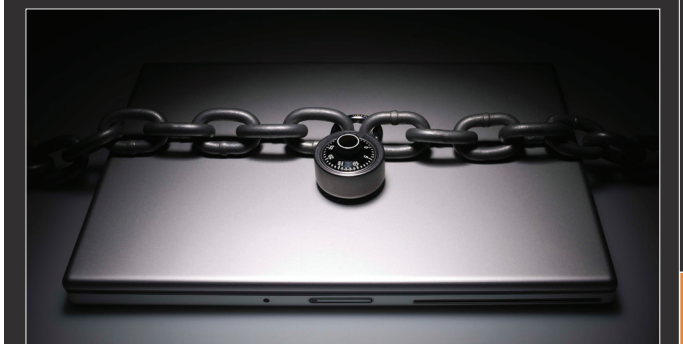
Cleared contractors provide critical research and support to programs giving the United States an economic, technological, and military advantage. In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops and cell phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of

surreptitious entry of their portable electronics.

>> The following countermeasures can decrease or prevent the loss of sensitive information:

- 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



Inadvertent Leaks versus Conscious Disregard

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.

Security Countermeasures

- 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.

How to Prepare for CONFERENCES, CONVENTIONS & TRADE SHOWS

Be Prepared

- 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. You can be targeted at any foreign or domestic conference, convention, or trade show
- Be informed on general security guidelines and the handling of sensitive or 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

Be Careful

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

Reportable Behaviors You May Experience

- Offers 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 FSO 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 strategic use of conversation to subtly extract information about you, your work, and your colleagues. A skilled elicitor can guide a conversation to areas of interest without directly asking questions that make his or her intent obvious.

You may experience the following elicitation techniques while attending conferences, conventions, or trade shows:

- 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

What 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

Practical 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 local DSS CI special agent prior to traveling to a conference, convention, or trade show located outside the United States
- Do not publicize travel plans and 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 FSO
- Do not post pictures or mention you are on travel on social media until your return
- Retain unwanted sensitive material pending proper disposal
- Do not use foreign computers or fax machines, and limit sensitive discussions

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.

Countering Threats to Networks and Cleared Individuals

>> Employees

- 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 clarifies National Industrial Security Program Manual (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 TRAINING for Industry

CI Training

DSS offers several web-based CI and threat awareness courses available for cleared contractor employees.

Individually, these courses are designed to help cleared employees recognize potential threats and emphasize NISPOM reporting requirements. Taken together, the courses are part of a larger CI curriculum for FSOs.

While these courses are not required, DSS encourages FSOs to use these free training opportunities to enhance cleared employee security awareness and improve existing security programs through more thorough integration of CI.

Counterintelligence Awareness and Reporting Course for Department of Defense Employees

This course sensitizes students to foreign intelligence collection goals and methods. It describes key indicators for potential insider threats, how to respond if you have been solicited for information or observed suspicious activities, and outlines what should be reported and how to report. Students will go through multiple case studies outlining recent espionage cases that have played out in the media.

Of interest to those contractor personnel who must meet the initial and annual training requirements of DoD 5240.06, "Counterintelligence Awareness of Reporting", this course will meet the requirements of that directive.

The training takes approximately 60 minutes to complete.

Insider Threat Awareness

This course provides a thorough understanding of how insider threat awareness is an essential component of a comprehensive security program and promotes the reporting of suspicious activities observed within the workplace.

The course teaches the common indicators that can signify an insider threat and promotes a proactive approach to reporting suspicious activities.

The training takes approximately 30 minutes to complete.

Cyber Security Awareness: A Cyber Security Awareness Course from the Defense Security Service

This course improves awareness of cyber threats affecting cleared contractor personnel. The course will promote awareness of potential cyber threats, improve recognition of subtle cyber attacks, promote familiarity with effective countermeasures, and emphasize the need to report possible cyber intrusions.

The training takes approximately 30 minutes to complete.

Integrating CI and Threat Awareness into Your Security Program

This course provides a thorough understanding of how CI and threat awareness are essential components of a comprehensive security program.

The course provides an overview of industry security program elements. This includes identifying the purpose of a CI and threat awareness program; identifying CI and threat awareness policies; identifying common security risks & countermeasures; recognizing types of information most likely to be targeted; identifying types of information that should be reported; and reporting procedures.

It also provides several threat information sources to assist in enhancing security programs.

The training takes approximately 1.5 hours to complete.

Sensitizing Facility Employees to Counterintelligence Concerns

This course is tailored toward FSOs. It provides guidance for educating facility personnel and enhances the FSO's understanding of the threats their facility and its employees may encounter.

The course emphasizes the importance in understanding how key employee groups may be targeted, their vulnerabilities, and the types of contacts they may experience so the FSO can better protect them. It identifies ways FSOs can promote employee awareness and reporting.

Students will gain an increased awareness of common foreign intelligence entity collection methods and the importance of making timely reports of suspicious activities.

The training takes approximately 30 minutes to complete.

The Relationship between Counterintelligence and Security

This course is tailored toward FSOs and emphasizes the complementary relationship between CI and security. CI is an essential part of a comprehensive security program. The course explains how a properly integrated security program can ensure your facility and its information and technology are as secure as possible.

The course outlines the FSO's key security and CI responsibilities, explains how to integrate CI into an existing security program, and outlines elements of a successful CI program.

The training takes approximately 30 minutes to complete.

Protecting Your Facility's Technology

This course is tailored toward FSOs. It provides the FSO guidance for identifying the types of technology an adversary could exploit at the FSO's facility.

FSOs will be equipped with the functional knowledge of how to identify and prioritize the critical information, determine the threat, and make sound security decisions based on a risk assessment.

The course will walk the FSOs through a risk assessment and the resources they should seek out to conduct one. It will also assist the FSO in identifying the assets, threats, and vulnerabilities of the FSO's facility's technology.

The training takes approximately 45 minutes to complete.

Thwarting the Enemy: Counterintelligence and Threat Awareness Information to the Defense Industrial Base

This course sensitizes employees to potential threats directed against U.S. technology through a series of real world scenarios.

The scenario-based course walks students through multiple examples of foreign collection attempts and identifies the appropriate responses and when to report. It highlights major collection methods and reinforces the employee's role in protecting cleared contractor facilities and critical technology.

The training will take approximately 30 minutes to complete.

How to Access

All courses are available on the DSS Center for Development of Security Excellence webpage: www.cdse.edu/catalog/counterintelligence.html

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

COUNTERINTELLIGENCE

Defense Security Service

www.dss.mil