Security Briefing

THIS BRIEFING IS UNCLASSIFIED

This briefing satisfies the requirements of the National Industrial Security Program Operating Manual (NISPOM)
### Topics

<table>
<thead>
<tr>
<th>Need-To-Know</th>
<th>Automated Information Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearance Levels</td>
<td>Badges/Security Color Code</td>
</tr>
<tr>
<td>Combination Controls</td>
<td>Classified Visits</td>
</tr>
<tr>
<td>Safeguarding Classified</td>
<td>Export Compliance</td>
</tr>
<tr>
<td>Reportable Information</td>
<td>Adverse Information</td>
</tr>
<tr>
<td>The Threat</td>
<td>Think Defensively</td>
</tr>
<tr>
<td>Foreign Travel</td>
<td>Foreign Visitors</td>
</tr>
<tr>
<td>Foreign Recruitment</td>
<td>Security Violations</td>
</tr>
<tr>
<td>Economic Espionage</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>Facility Access</td>
<td>Foreign Ownership, Control or Influence (FOCI)</td>
</tr>
</tbody>
</table>
Classified Information

Classified information is information that, in the interest of national security, requires protection against unauthorized disclosure.

(Company Name) is assessed annually on its security compliance performance and its ability to properly safeguard classified information. A positive rating on this assessment is critical in maintaining our facility clearance and continuing to do business with the U.S. Government.
Need-to-Know

**DEFINITION:** Need-To-Know is the determination by an authorized holder of classified or CUI information that another appropriately cleared individual requires access to the information in order to perform official duties.

**KEY POINTS:**

If you have any doubt, check with your supervisor before releasing any classified information or controlled unclassified information (CUI).

Possessing a badge that indicates a clearance does not automatically grant individuals a Need-To-Know.

When working with contractors, it is important to determine the degree of Need-to-Know BEFORE sharing program or project information.

The Need-To-Know principle applies to computers as well. Do not share your password with anyone. Always secure your system by logging out or locking your computer.
Need-to-Know – cont’d

• Your security clearance does not give you approved access to all classified information. It gives you access only to:

  Information at the same or lower level of classification as the level of the clearance granted; and,

  Information that you have a “need-to-know" in order to perform your work.

• Need-to-know is one of the most fundamental security principles. The practice of need-to-know limits the damage that can be done by a trusted insider who betrays our trust. Failures in implementing the need-to-know principle can cause serious damage to our organization.

• Need-to-know imposes a dual responsibility on you and all other authorized holders of protected information:
Need-to-Know – cont’d

When doing your job, you are expected to limit your requests for information to that which you have a need-to-know. Under some circumstances, you may be expected to explain and justify your need-to-know when asking others for information.

Conversely, you are expected to ensure that anyone to whom you give protected information has a legitimate need to know that information. In some cases, you may need to ask the other person for sufficient information to enable you to make an informed decision about their need-to-know.

You are expected to refrain from discussing protected information in hallways, cafeterias, elevators, rest rooms or smoking areas where the discussion may be overheard by persons who do not have a need-to-know the subject of conversation.

You should report to your security office any co-worker who repeatedly violates the need-to-know principle.
The responsibility for determining Need-to-Know in connection with a classified visit rests with the individual who will disclose classified information during the visit.

Visits that may require a Need-To-Know certification are usually non-contractual and may depend on the destination. If you are attending a symposium, follow the instructions given by the host. The security section of these instructions will be completed by the Security department, but the Need-To-Know section is typically completed by your government customer.
Clearance Levels

(Company Name) clearances parallel DoD classification levels. It follows that access to classified defense information is contingent upon you having at least a comparable level of security clearance. The primary D.o.D. clearances are:

• **Confidential:** Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *identifiable* damage to the national security.

• **Secret:** Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *serious* damage to the national security.

• **Top Secret:** Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *exceptionally grave* damage to the national security.
Badges/Color Security Code

- The color strip located below your badge photo signifies your clearance level.

- Your badge must be worn at all times above the waist (and visible) while on the premises.

- No piggybacking into the building (scan your badge even if the door is already open). This does not include the glass lobby doors during business hours.

- Stop and question employees/visitors who are not wearing their badge, or contact Security. Nobody is exempt from wearing a badge at any time while in the building.

- If an employee/contractor told you they forgot their badge or that their badge does not work, let Security know or have the person contact Security from the lobby.

- Remove your badge when you leave the property. It should never be displayed in public.

- Your badge shall not be used as an alternate form of identification for non-(COMPANY NAME) purposes.

- Never let your badge be copied.

- Finally, if you misplace your badge, notify Security immediately so we can deactivate it. Do not wait until you conclude that it is lost to let us know.

UNCLASSIFIED
Combination Controls

- Combinations which protect classified material shall be memorized, not written down.

- Combinations shall be changed upon initial issuance, when persons knowing the number have been debriefed, when the number is believed to have been compromised, or when otherwise deemed necessary by Security.
Facility Access

(Procedures for granting visitors access to your facility)
Facility Access

Proof of Citizenship

Visitors, contractors, consultants and contract labor will be required to provide proof of U.S. citizenship or legal residency prior to being granted access to the facility. A picture identification and one of the following documents is required:

1. U.S. Passport
2. Certificate of U.S. Citizenship (INS Form N-560 or N-561)
3. Certificate of Naturalization (INS Form N-550 or N-570)
4. Certificate of Birth Abroad issued by the Dept of State (Form FS-240 or Form DS-1350)
5. Original or certified copy of a birth certificate
6. Permanent Resident Card I-551

The requesting (Company Name) host/designee is responsible for informing their visitor/contractor of the Proof of Citizenship/Residency requirement.
A Visitor Authorization Letter (VAL), also called a visitor clearance, may be faxed or sent via the Joint Personnel Adjudication System (JPAS) by the visiting party’s security office to (Company Name) Security. VALs are only accepted from facilities that possess a DOD facility clearance. This method would meet the requirement for Proof of Citizenship/Residency.

If acceptable documentation has not been received prior to the visit or commencement of work, access privileges may be significantly restricted or facility access will be altogether denied.
Classified Visits

Government and Contractor Visits

• A Visit Request is required when planning a visit that will involve the disclosure of classified information to the Government or another contractor.

• Visit requests, both inbound and outbound, shall be forwarded to Security no later than 5 business days before the visit.

• International visitors shall allow at least 30 days notice for classified visits abroad.
Classified Visits – cont’d

Hosting a Visit

Prior to holding a classified business meeting, the host shall verify that (Company Name) Security has received a Visitor Clearance Letter which includes the visitor’s clearance information, purpose of the visit, and the appropriate need-to-know.
If you are the host of a classified visit, it is your responsibility to make certain that the visitor’s clearance level is at least as high as the classified information being discussed.
Safeguarding Classified Information

CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT
(for cleared personnel)

As a cleared employee of a Department of Defense contractor, you have been the subject of a personnel security investigation. The purpose of this investigation was to determine your trustworthiness for safeguarding classified information. When the investigation was completed, your employing or sponsoring department or agency granted you a security clearance based upon a favorable adjudication of the investigation results. By being granted a security clearance, you have met the first of three requirements necessary to have access to classified information.
The second requirement that you must fulfill is to sign an SF 312, "Classified Information Nondisclosure Agreement." The President established this requirement in a Directive that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." The SF 312 is a contractual agreement between the United States Government, and you a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of:
Safeguarding Classified Information

CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT
(for cleared personnel)

(1) the trust that is placed in you by providing you access to classified information;

(2) your responsibilities to protect that information from unauthorized disclosure; and

(3) the consequences that may result from your failure to meet those responsibilities.

Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of non-compliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for a violation of this agreement by initiating a civil or administrative action.
Safeguarding Classified Information

CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT

The third and final requirement for access to classified information is the "need-to-know," that is, you must have a need to know the information in order to perform your official duties. The holder of classified information to which you seek access is responsible for confirming your identify, your clearance, and your need-to-know." As a holder of classified information, you are responsible for making these same determinations with respect to any individual to whom you may disclose it.
Safeguarding Classified

When not in use, classified material shall be secured in a GSA-approved security container.

A locked room, desk or file cabinet is not an approved method of classified storage unless specifically authorized, in writing, by the Defense Security Service (DSS).

Containers shall be checked upon opening, closing, and at the end of the workday. Proof of checks shall be recorded on signature cards provided by the Security Department.
Classification Markings - U.S. Government Mandated

- Security procedures require us to mark letters, reports, messages, data sheets, technical papers, and other material containing classified information.

- Classified items such as hardware, models, and videos shall also be properly marked.

- The markings are word symbols such as CONFIDENTIAL or SECRET, designed for clarity and uniformity and placed according to definite criteria.

- Cleared individuals who have responsibilities for creating/producing classified material shall comply with the guidance provided in DSSA Marking Classified Information,

- Accurate classification of data is imperative. Contact Security if you have questions.
Transmitting Classified Information

• Transmission of classified information by unsecured telephone, facsimile or any other method not approved by Security is prohibited.

• Hand carrying of classified material is prohibited unless written authorization is obtained from Security.

• All requests for transmission (incoming and outgoing) of classified material shall be coordinated through Security.
Reproduction of Classified Material

Reproduction of classified data, photographs and artwork shall be coordinated through Security.

Destruction of Classified Material

Classified material that becomes outdated or no longer has reference value shall be destroyed. Upon making this determination, the classified material shall be brought to the Security Office for destruction. Non-Security personnel shall not destroy classified material unless specifically authorized by Security.
Safeguarding Classified – cont’d

• Foreign Government Information (FGI) material shall be controlled and brought into accountability. FGI material shall not be co-mingled with U.S. collateral material.

• If FGI and U.S. collateral material are stored in the same container, they shall be separated by folders and clearly marked.

• FGI shall be returned to the foreign government upon contract termination, unless the contract authorizes destruction.
Safeguarding Classified – cont’d

Retention

• Classified information retained after the closing of a contract shall be dispositioned according to contract instructions. Authorization for retention may be requested of the customer, provided the information can be transferred to an active classified contract.

• If you do not have authorization to keep the material, it shall be brought to Security for disposition.
NEVER divulge classified information to unauthorized personnel regardless of the passage of time, public source disclosure of data, changes in your clearance, access, or employment status.
Reportable Information

Cleared employees shall contact Security if any of the following apply:

• Name change.

• Change in marital status.

• Change in family status which results in having a foreign national as a relative.

• Reoccurring contacts with Foreign Nationals, or relationships with foreign businesses.

• Requests from anyone for unauthorized access to classified or export-controlled technical information.
Adverse Information

Adverse information is any information that adversely reflects on the integrity or character of a cleared employee. Such information would suggest that his or her ability to safeguard classified information may be impaired, or, that his or her access to classified information clearly may not be in the interest of national security.

It is the responsibility of all employees to report to Security any adverse information concerning another cleared employee.
Adverse Information

Examples of Adverse Information:

- Criminal activity.
- Use of illicit drugs or misuse of controlled substances.
- Any pattern of security violations or disregard for security regulations.
- Excessive indebtedness/recurring financial difficulties.
Export Compliance

• Per the International Traffic in Arms Regulations (ITAR), Technical data in any form that pertains to the U.S. Munitions List (a list of defense-related articles) is “export controlled.”

• Access to, or disclosure of, such data to a Foreign Person is an export. U.S. Persons employed by Foreign Persons are generally treated as Foreign Persons themselves for the purpose of export compliance.

• In such a case, if the U.S. State Department has not issued an Export License (based on a Technical Assistance Agreement or Manufacturing License Agreement), a violation of ITAR has occurred.
Export Compliance – cont’d

Definitions:

EXPORT

• Shipping or transporting technical data or hardware out of the U.S.
• Transferring control or disclosing hardware, technical data, technology, software, electronic data to a foreign person (whether in the U.S. or abroad).
• Providing a Defense Service or Technical Assistance to a Foreign Person.
• Providing site visits/tours to Foreign Persons.

FOREIGN PERSON

• NOT a U.S. Citizen
• NOT a U.S. Permanent Resident (e.g., Green Card)
• NOT a "Protected Individual" (e.g., Refugee or Asylee)

DEFENSE ARTICLE

• An article or service that is specifically designed, developed, configured, adapted or modified for a military application and does not have predominant civil applications.
Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export-controlled information must be controlled as sensitive information and marked accordingly. A large, frequently updated database of information on export regulations is available at www.bis.doc.gov.
One objective of the ITAR and EAR is to prevent foreign citizens, industry, or governments, or their representatives, from obtaining information that is contrary to the national security interests of the United States.

Different laws and regulations use different definitions of a U.S. person, U.S. national, and foreign national. This is a source of considerable confusion in implementing international security programs.

The rules are especially confusing when dealing with an immigrant alien who possesses a green card for permanent residence in the U.S. For the purpose of export control regulations, such an individual is a "U.S. person" and can be allowed access to export-controlled information without an export license. If the export controlled information is classified, however, the regulations for release of classified information apply. According to the National Industrial Security Program Operating Manual, a permanent resident with a green card is still a foreign national and not a "U.S. person." Therefore, such an individual cannot have access to classified export-controlled information.
Access to Export-Controlled Information:

Export-controlled information may be disseminated only to U.S. citizens or immigrant aliens. It is important to note that discussion with a foreign national in the United States, or a person "acting on behalf of a foreign person," constitutes an "export" if it reveals technical information regarding export-controlled technology.

Marking Export-Controlled Information:

All documents that contain export-controlled technical data must be properly marked. Refer to the company marking procedures.
Export Compliance

ITAR violations can result in hefty fines and/or debarment from international business arrangements. Violations may also result in personal criminal liability. An export violation is also a violation of the (Company Name) Standards of Conduct, which may result in disciplinary action to include suspension, termination and/or criminal prosecution.

Prior to the export of technical data or hardware, contact your local trade officer.
Automated Information Systems (AISs)

• All systems used for processing classified information including computers and test equipment shall be evaluated for NISPOM applicability. A formal approval is required by the Defense Security Service (DSS) **PRIOR** to operating these systems.

• As a general rule, any hardware or equipment that has memory storage capability needs to be evaluated for DoD accreditation.

• All classified processing shall be coordinated through the Facility Security Officer.

• Classified information processed on a non-approved system is a security violation which is reportable to the Defense Security Services (DSS).
Automated Information Systems (AISs)

- Do not connect a classified computer system to an unclassified system or network. In the event that this occurs, the unclassified system is considered contaminated. The classified information is then considered “potentially” compromised and an investigation will be conducted by Security.

- Notify Security immediately if you suspect that classified information has been processed on any non-approved system.

- Custodians and users of classified processing systems require special training and briefings.
UNDERSTANDING THE THREAT
The Threat

America's role as the dominant political, economic, and military force in the world makes it the number one target for foreign espionage. In addition to the intelligence services of friendly as well as unfriendly countries, sources of the threat to classified and other protected information include:

• Foreign or multinational corporations.
• Foreign government-sponsored educational and scientific institutions.
• Freelance agents (some of whom are unemployed former intelligence officers).
• Computer hackers.
• Terrorist organizations.
• Revolutionary groups.
• Extremist ethnic or religious organizations.
• Drug syndicates.
• Organized crime.
The Threat

Individuals in both government and industry in almost 100 countries are involved in legal and illegal efforts to collect intelligence in the United States. These countries conduct espionage against the United States for one or more of the following reasons:

• The country competes with the United States for global or regional political and economic influence.

• The country has a developing economy and sees its economic future as being dependent upon the rapid acquisition and development of new technologies by every possible means, whether legal or illegal.

• The country competes with U.S. companies in the global marketplace for the sale of advanced technologies or military weaponry.

• The country feels threatened by a hostile neighbor and seeks to develop or obtain the most advanced military technology. It may also seek information on U.S. policy, and to influence U.S. policy, toward itself and the neighboring country.
The Threat

Important changes in the international economic environment and technological advances have increased our vulnerability to espionage by insiders with access to classified and other protected information.

• The increasing value of technology and trade secrets in the both global and domestic marketplaces, and the temporary nature of many high-tech employments have increased both the opportunities and the incentives for economic espionage.

• The development of a global economy, with a rapid expansion in foreign trade, travel, and personal relationships of all kinds, now makes it easier than ever for insiders to establish contact with potential buyers of classified and other protected information. It also makes it easier for foreign intelligence officers or agents of foreign corporations to establish personal contact, assess, and sometimes recruit Americans with access to valuable classified, controlled, or proprietary information.

• The development of automated networks and the ease with which large quantities of data can be downloaded from those networks and stored and transmitted to others increases exponentially the amount of damage that can be done by a single insider who betrays his or her trust.
The Threat

What are the spies and other intelligence collectors after?

Everything that will help another country, organization, corporation, research institute, or individual achieve their political, military, economic, or scientific goals.
The Threat

National Security Threat List

The FBI's foreign counterintelligence mission is set out in a strategy known as the National Security Threat List (NSTL). The NSTL combines two elements:

First is the Issues Threat List -- a list of eight categories of activity that are a national security concern regardless of what foreign power or entity engages in them.

Second is the Country Threat List -- a classified list of foreign powers that pose a strategic intelligence threat to U.S. security interests. The activities of these countries are so hostile, or of such concern, that counterintelligence or counterterrorism investigations are warranted to precisely describe the nature and scope of the activities as well as to counter specific identified activities.

Only the Issues Threat List is discussed here, as the country list is classified. The FBI will investigate the activities of any country that relate to any of the following eight issues:
The Threat

1. Terrorism

This issue concerns foreign power-sponsored or foreign power-coordinated activities that:

• Involve violent acts, dangerous to human life, that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any state;

• Appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping; and,

• Occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
The Threat

2. Espionage

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons, which involves the identification, targeting and collection of U.S. national defense information.
The Threat

3. Proliferation

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments or persons, which involves:

• The proliferation of weapons of mass destruction to include chemical, biological, or nuclear weapons, and delivery systems of those weapons of mass destruction; or

• The proliferation of advanced conventional weapons.
The Threat

4. Economic Espionage

• This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons, which involves:

• The unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information, proprietary economic information, or critical technologies; or,

• The unlawful or clandestine targeting or influencing of sensitive economic policy decisions.
5. Targeting the National Information Infrastructure

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons, which involves the targeting of facilities, personnel, information, or computer, cable, satellite, or telecommunications systems which are associated with the National Information Infrastructure. Proscribed intelligence activities include:

• Denial or disruption of computer, cable, satellite or telecommunications services;

• Unauthorized monitoring of computer, cable, satellite or telecommunications systems;

• Unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite or telecommunications systems;

• Unauthorized modification or destruction of computer programming codes, computer network databases, stored information or computer capabilities; or,

• Manipulation of computer, cable, satellite or telecommunications services resulting in fraud, financial loss or other federal criminal violations.
6. Targeting the U.S. Government

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons, which involves the targeting of government programs, information, or facilities or the targeting or personnel of the:

• U.S. intelligence community;
• U.S. foreign affairs, or economic affairs community; or
• U.S. defense establishment and related activities of national preparedness.
The Threat

7. Perception Management

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons, which involves manipulating information, communicating false information, or propagating deceptive information and communications designed to distort the perception of the public (domestically or internationally) or of U.S. Government officials regarding U.S. policies, ranging from foreign policy to economic strategies.
The Threat

8. Foreign Intelligence Activities

This issue concerns foreign power-sponsored or foreign power-coordinated intelligence activity conducted in the U.S. or directed against the United States Government, or U.S. corporations, establishments, or persons, that is not described by or included in the other issue threats.
The Threat

Who is a potential threat?

ANY PERSON who lacks proper clearance and a need-to-know, but still seeks to gain access to classified information or CUI. *This includes our nation’s adversaries, as well as our competitors.*

Examples:

• Cleared/accessed employees

• Visitors

• Other defense contractors

• Overly curious family, friends or neighbors

• Foreign nationals

• Students

Elicitation techniques are often subtle and difficult to recognize. Report all suspicious contacts to the Security Office.
Think Defensively

• Being mindful and thinking defensively will make it difficult for someone to obtain technical and/or classified information from you. As a (Company Name) employee, you are considered to be a rich source of information by those people involved in both classic and industrial or economic espionage.

• Your increased awareness is essential when meeting with foreign nationals domestically and abroad or while vacationing outside the continental U.S. For current requirements and warnings for international travelers, visit http://travel.state.gov

• When you travel, refrain from discussing business in public places. Report to Security any suspicious contacts from individuals that you do not know.
COUNTERINTELLIGENCE

FOREIGN RECRUITMENT

TRAVEL-RELATED VULNERABILITY

FOREIGN VISITS
FOREIGN RECRUITMENT

WHAT IS RECRUITMENT?

An intelligence definition of recruitment is the attainment of someone’s cooperation to provide sensitive or classified information, usually after careful assessment and patient cultivation of the target by an intelligence service. By the time the “pitch” (the offer to work for the foreign government) is made, the intelligence officer (the “recruiter”) is relatively confident of the target’s willingness to cooperate. If a failed recruitment attempt is reported, serious consequences may result for the involved Intelligence Officer (IO).

If the target agrees to the recruitment, that person becomes an “asset” or “agent”, i.e. he has become a spy. The IO also called a “case officer,” handles the asset by clandestinely receiving the information, paying his agent, and guiding the asset in his illicit activities. Why a person betrays his country is a complex issue, but money is almost always involved. Pursuit of financial gain often represents some other personal or psychological need such as ego enhancement, revenge, etc.
FOREIGN RECRUITMENT

Recruitment is usually a subtle and carefully orchestrated process to determine a person’s receptiveness to working for a foreign government. If success is perceived to be possible, the pitch will eventually be made. Initially, an IO's interest in you may be imperceptible, but may become more obvious as the relationship develops.

Reporting questionable relationships, whether involving yourself, a co-worker, supervisor, neighbor, family member, or friend, is crucial to effective intervention. Espionage is never a “victimless crime.” It damages lives and threatens the security of this nation. Notify Security should you have any indication that the company or any of your co-workers may be the target of an attempted exploitation by a representative of another country.

BOTTOM LINE: BE ALERT... BE AWARE... REPORT SUSPICIOUS OCCURRENCES!
FOREIGN TRAVEL

OVERSEAS TRAVEL

Overseas travel increases the risk of being targeted by foreign intelligence activities. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you and their actions are not restricted when they are operating within their own countries. Information Age spying includes:

- Wired hotel rooms
- Intercepts of fax and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, theft of hardware and software
- Break-ins and/or searches of hotel rooms, briefcases, luggage, etc.
- Bugged airline cabins
- Substitution of flight attendants by spies/information collectors.
FOREIGN TRAVEL

FAVORITE TACTICS

The overseas traveler and the information in their possession are most vulnerable when on the move. Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside the hotel room) may be recorded. These recorded observations can then be analyzed for personal vulnerabilities (useful for targeting and possible recruitment approaches) and/or useful information (collections).
FAVORITE TACTICS

A favored tactic for industrial spies is to attend trade show/conference type events. This environment allows them to ask a lot of questions, including questions that might seem more suspect in a different type environment. One estimate reflected that one in fifty people attending such events were there specifically to gather intelligence.
FOREIGN TRAVEL

COMPUTER SECURITY

Another area of concern while traveling is computer security. Foreign Intelligence Services are not usually fortunate enough to have information simply dropped into their hands. They rely on tactics such as stealing laptops. These portable systems may contain access capabilities that serve as doorways to additional information and systems. In addition to theft, travelers have reported unauthorized access, attempted access, damage and evidence of surreptitious entry of their portable electronic devices.

UNCLASSIFIED
FOREIGN TRAVEL

COMPUTER SECURITY

Effective countermeasures to the aforementioned vulnerabilities include but are not limited to the following:

– Refrain from bringing portable electronic devices unless it is mission critical

– Use of removable hard drives

– Maintain personal cognizance of portable electronic devices

– Data on portable electronic devices should contain only what is needed for the purpose of your travel
FOREIGN VISITS

International visits are a common part of everyday business in today’s international market/economy and are a welcome opportunity to boost any business. The cleared Department of Defense (DoD) Contractor is no exception to this growth in the International Market. Visits to DoD Cleared Contractors by foreign delegations and individuals have been noted as one of the most frequently utilized modus operandi for targeting US Defense Industry for the past five years in the Defense Security Service publication, Technology Collection Trends in the US Defense Industry.
FOREIGN VISITS

TECHNIQUES

Remember, it is always cheaper for any country to elicit, improperly obtain or buy a new technology or the means of producing a new technology than it is for them to pay for the research and development (R&D) themselves. There are more funds expended on R &D by the US Government and Industry than any other country in the world, making US Contractors a prime target for collection of both classified and commercial/proprietary technology by foreign countries. There are several techniques and indicators to be aware of when a foreign visit is to take place at your facility. While hosting the visit, watch for any of the following techniques to help you decide if there is the potential for you to be targeted by the foreign visitor.
FOREIGN VISITS

TECHNIQUES

• Peppering - Several of the visitors asking the same question in different styles or one visitor asking the same question to multiple US Contractor employees.

• Wandering visitor - The visitor uses the distraction provided by a large delegation to slip away, out of the control of the escort.

• Divide and Conquer - The foreign visitors take the US team members into different areas to discuss issues, thus, relieving the US person of his safety net of being assisted in answering questions or eliminating oversight of what he releases.

• Switching visitors at the last minute – A tool that is sometimes used to add a collector to the group without leaving enough time for a background check to be performed on the new visitor.

• Bait and Switch - The delegation says they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions and discussions.

• The distraught visitor - When the visitor does not have questions answered he/she has a temper tantrum or acts as though they are insulted, thereby trying to get the US person to answer the questions and not be upset.
REPORTING OBLIGATIONS

SUSPICIOUS CONTACTS

• In accordance with paragraphs 1-302b and 1-301 of the NISPOM, cleared facilities are required to report to Defense Security Service (DSS) any attempts or suspected attempts to obtain technical information or company data. Reporting this information enables comprehensive analysis and the detection of potentially illegal or unauthorized activity directed against our company. (COMPANY NAME) and DSS have a mutual goal of protecting defense-related information and activities within our facility, and we can only do this with your steadfast support and prompt reporting.

• The information you provide is carefully analyzed, catalogued, and shared with relevant national-level intelligence or law enforcement agencies, as deemed appropriate. While DSS considers no suspicious contact report to be benign in nature, some information will inherently be more actionable than others. If ever in doubt about the contact, do not hesitate to contact Security and we can decide whether it should be forwarded to DSS. Prompt reporting is critical not only for DSS analysts, but it enables us to implement preventive measures internally if necessary.

• Only through your vigilance and our partnership with DSS will we succeed in deterring, detecting, and neutralizing external threats to the information our nation has entrusted us to safeguard. Please report all suspicious contacts immediately to Security.
REPORTING OBLIGATIONS

FOREIGN CONTACTS

- Report all foreign contacts to security.

- Report all foreign travel to security.

- Be sure to receive your pre-travel briefing before leaving the country. Complete your debriefing upon return.

- Immediately report any attempts to obtain classified or controlled unclassified information.
REPORTING OBLIGATIONS

• REPORT ALL FOREIGN CONTACTS TO SECURITY.

• REPORT ALL FOREIGN TRAVEL TO SECURITY.

• BE SURE TO RECEIVE YOUR PRE-TRAVEL BRIEFING BEFORE LEAVING THE COUNTRY. COMPLETE YOUR DEBRIEFING UPON RETURN.

• IMMEDIATELY REPORT ANY ATTEMPTS TO OBTAIN CLASSIFIED OR CONTROLLED UNCLASSIFIED INFORMATION.
Economic Espionage Act of 1996

Protecting Proprietary Information
Economic Espionage Act of 1996

- The Economic Espionage Act (EEA) specifically proscribes the various acts defined under economic espionage and addresses the U.S. national and economic security aspects of the crime. The law also addresses the theft of trade secrets where no foreign involvement is found.

- As defined in the Economic Espionage Act of 1996, the term trade secret refers to all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

1. The owner thereof has taken reasonable measures to keep such information secret;

2. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public; and,

3. The owner of a trade secret is the person or entity that has rightful legal or equitable title to, or license in, the trade secret.
Economic Espionage Act of 1996

• The EEA contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, any instrument of a foreign government, or foreign agent. In contrast, the second provision, under Section 1832, makes the commercial theft of trade secrets a criminal act regardless of who benefits.

• Reflecting the more serious nature of economic espionage, a defendant convicted for violating Section 1831 can be imprisoned for up to 15 years and fined $500,000 or both. Corporations and other organizations can be fined up to $10 million. A defendant convicted for theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined $500,000 or both. Corporations and other entities can be fined no more than $5 million.
Economic Espionage Act of 1996

The EEA is a powerful deterrent and is a very important law enforcement and security management tool for protecting intellectual property rights. The EEA is not intended to convert all thefts of trade secrets into criminal cases; however, the EEA substantially raises the stakes in the arena of economic espionage. To report violations of the EEA or to obtain additional information, contact Security.
Protecting Proprietary Information

There is no general definition for proprietary information in the U.S. legal code. The Federal Acquisition Regulation (48 CFR 27.402 Policy) does, however, provide a definition.

"…contractors may have a legitimate proprietary interest (e.g., a property right or other valid economic interest) in data resulting from private investment. Protection of such data from unauthorized use and disclosure is necessary in order to prevent the compromise of such property right or economic interest, avoid jeopardizing the contractor’s commercial position, and preclude impairment of the Government’s ability to obtain access to or use of such data."
Protecting Proprietary Information

This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 USC 1905) makes it a crime for a federal employee to disclose such information.
Protecting Proprietary Information

Safeguarding Proprietary/Trade Secret Information

• Effective enforcement of laws governing unauthorized disclosure of proprietary or trade secret information generally requires that the owner of this information must have taken reasonable measures to safeguard it from unauthorized disclosure.

• Reasonable measures include building access controls, escorting visitors, marking sensitive documents, non-disclosure agreements, and shredding material when no longer needed.

• In the case of defense contractors, the government contract may require a contractor to follow certain safeguarding requirements. The government, in turn, is required to protect proprietary or trade secret information submitted to it during the bidding process (FAR 14.401). Bids must be "kept secure" and remain "in a locked bid box or safe."
Protecting Proprietary Information

Marking Proprietary/Trade Secret Information

• Effective enforcement of laws governing unauthorized disclosure of proprietary or trade secret information generally requires that this information be clearly identifiable through appropriate markings. The nature of these markings is left to the discretion of the company. The terms "Company Sensitive" or "Company Proprietary" are sometimes used.

• In soliciting bids, the government is required to inform potential contractors how to mark proprietary information (FAR 15.407) to ensure its protection. When a contract is granted, a data rights clause must be included in the contract (FAR (52.227-14) to advise the contractor how to mark proprietary data for protection. The title page and each page containing proprietary information must be marked. The regulations provide no guidance on marking of electronic media while on an electronic system (screen display or file marker).
Protecting Proprietary Information

Enforcement

• The Economic Espionage Act contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, instrumentality, or agent. In contrast, the second provision, under Section 1832, makes the commercial theft of trade secrets a criminal act regardless of who benefits.

• A defendant convicted of economic espionage under Section 1831 can be imprisoned for up to 15 years and fined $500,000 or both. Corporations and other organizations can be fined up to $10 million. A defendant convicted for theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined $500,000 or both. Corporations and other entities can be fined no more than $5 million.
Foreign Ownership, Control or Influence (FOCI)
Foreign Ownership Control or Influence (FOCI)

A U.S. company is under FOCI when a foreign interest has the power, whether or not exercised, to direct or decide matters affecting the management or operations of the company which may result in unauthorized access to classified information or may adversely affect performance of classified contracts (NISPOM, paragraph 2-300a).
FOCI Indicators

- Substantial foreign holdings of company stock
  - > 5% of the ownership interests
  - > 10% of the voting interest
- Existence of foreign subsidiaries
- Foreign corporate officers or board directors
- Contractual agreements with foreign sources
- Foreign debts/income
- Shared corporate officers or board directors

UNCLASSIFIED
Q: What is the USG’s concern about foreign investment?

A: Theft of U.S. classified and unclassified technology.
Business Impact of FOCI

• If a defense contractor is determined to be under FOCI:
  – DSS takes immediate action to safeguard classified information.
  – Contractor is not eligible for a new facility clearance until FOCI review.
  – Existing facility clearance can continue if DSS sees no risk of compromise.
  – Existing facility clearance will be revoked if security measures inadequate.

• If a contractor doesn’t currently possess, or have a current/impending requirement for access to classified information, their facility clearance is administratively terminated.

• USG can impose any security methods it deems necessary to protect classified information.
Defense Security Service (DSS) Requirements

• U.S. companies that have some degree of foreign ownership or control must develop and implement a mitigation plan.

• FOCI mitigation requires the company to develop a plan to control or deny access to technical information by the foreign entity.

• The U.S. Government and the contractor have to concur on the mitigation plan.
DSS Objectives

- To protect classified and export-controlled information.

- To recognize and assess the influence and direction exerted by the foreign parent (and/or foreign government).

- To develop and to put into effect remedies when foreign influence may be adverse to U.S. national security interests.
What is FOCI Mitigation?

DSS allows FOCI to be mitigated through a Proxy, Voting Trust or Special Security Agreement. These mitigation instruments enable U.S. contractors to perform on classified programs with provisions in place to negate foreign influence over that company, and to deny the foreign entity access to classified or export-controlled data.
Proxy Agreement - Summary

- Proxy Agreement:
  - Places the company under the control of U.S. trustees (cleared to the level of the company);
  - The foreign owner derives the benefit of ownership but relinquishes control over business operations;
  - Trustees are appointed by the company and approved by the U.S. Government;
  - Day-to-day operations of the company are closely overseen by the trustees.
Security Violations

- Security Violations are acts or omissions that violate established security procedures developed to protect classified information. Violations can be a loss or compromise of classified information, or, an act that does not necessarily result in any compromise or loss but is nevertheless considered serious. Not reporting a security violation is also a violation.

- A security violation is also a violation of the (Company Name) Standards of Conduct, which may result in disciplinary action to include suspension, termination and/or criminal prosecution.

- Security Violations are costly, but preventable.

- Report immediately!

UNCLASSIFIED
The Law

It is against the law to:

• Disclose classified information to unauthorized persons.

• Fail to report a known or suspected compromise of classified information.

• Destroy National Defense Material without proper approvals.
The Law

Penalties for unauthorized disclosure of classified information can include significant monetary fines and life imprisonment.

There is NO statute of limitations regarding the unauthorized disclosure of classified information.

Espionage Law Title 18 - Sections 793, 794, 798
Questions?

Questions regarding the information contained or referenced in this briefing should be directed to:

(FSO NAME), FACILITY SECURITY OFFICER
number (OFFICE)
number (MOBILE) 24/7