STUDENT GUIDE

COUNTERINTELLIGENCE AWARENESS AND SECURITY BRIEF

Opening

Every day, United States sensitive and classified technologies and information are targeted and stolen using various collection vectors. As a result, the United States' technological lead, competitive edge, and strategic military advantage are at risk; and our national security interests could be compromised.

Countering this threat requires knowledge of the threat and diligence on the part of all personnel charged with protecting classified information. You play a role. You must be vigilant.

Welcome to your initial or annual counterintelligence awareness and security briefing.

Welcome

I will be guiding you through this briefing. I'm a Facility Security Officer, or FSO, for a cleared defense contractor. I'm responsible for the overall security of my facility.

You will also hear from a Defense Counterintelligence and Security Agency, or DCSA, Counterintelligence Special Agent, or CISA. They will let us know how DCSA can help us and how we can help DCSA. Finally, we will also learn from a former agent of a foreign intelligence entity—an FIE.

We'll only take about 25 minutes of your time. As we proceed through this course, keep in mind that additional information is also available to you from the course Resources page. Let's get started.

Adversary Targets

As members of the national industrial base, both you and I have access to sensitive and classified information in the course of our daily work. We are responsible for protecting that information. We are also responsible for reporting any suspicious activity that may indicate a threat to the security of U.S. technology or systems.

Because of our access, we are targets of adversaries seeking to gain information and technology. We may be targeted for what we know and for what we have access to. So, what, exactly, should we be protecting? Adversaries target assets, in the form of people, information, equipment, facilities and networks, activities and operations, and suppliers.

When targeting people, adversaries employ a wide range of methods and may even look for exploitable weaknesses— such as financial problems, drug and alcohol issues, adultery, and gambling problems.

When targeting information, adversaries know that while a single piece of information—classified or not—may not be of critical importance alone, when put together with other pieces of information, it may reveal sensitive, or even classified, information. Because of this, we must protect not only classified information, but also, sensitive unclassified information, and proprietary information.

Loss of any of these directly affects not only our companies' economic viability, but also affects national security. You can find details on how to protect your information in the Resources.

Top Secret: Top Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the Original Classification Authority is able to identify or describe.

Secret: Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause serious damage to the national security that the Original Classification Authority is able to identify or describe.

Confidential: Confidential information is information or material of which unauthorized disclosure could reasonably be expected to cause damage to the national security that the Original Classification Authority is able to identify or describe.

Targeted Information and Technologies

Let's talk more specifically about the technology and information targeted by adversaries. As a former foreign intelligence officer, I know a lot about this. While adversaries are interested in anything that will strengthen their advantage—whether it is a military, competitive, or economic advantage—technology assets are the greatest target.

Both classified and unclassified technologies are targeted. We also seek out contingency plans; personnel information; and information on programs, deployments, and response procedures. When adversaries are able to collect enough information, they can piece it together and learn things—even classified things—which have serious consequences to U.S. national security.

Critical Technology:

- Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service that makes or could make a significant contribution to the military potential of any country, including the United States.
- Includes, but not limited to, design and manufacturing know-how, technical data, software, keystone equipment, and inspection and test equipment
- May be export controlled and subject to the International Traffic in Arms Regulations (ITAR)

Dual Use Technology:

- Technology that has both military and commercial use
- Export is strictly controlled and enforced under the Export Administration Regulations (EAR)
- Illegal export of this technology often results in fines and/or criminal charges

Sources of Threat

Threats come in many forms and may materialize in different ways. As a CI Special Agent, I see examples of this every day. For example, some threats are found within your office and look just like you and your coworkers. In fact, they may be your coworkers. Others originate within foreign intelligence entities.

Threats may be physical and come in the form of terrorist activity or they may be electronic and carried out by hackers and cyber criminals. Other threats come from those seeking to damage your business while building their own.

In order to identify these threats, you must understand what or whom to look for, and you must understand how they operate.

Consider This

Would you consider any of these scenarios to be suspicious? Consider the following scenarios. Which, if any, may indicate a threat? Select all that apply.

- □ Your company's sales department receives a purchase request from an unknown vendor.
- □ A scientist at your facility receives a request to review a research paper.
- □ During a conference overseas, a researcher's laptop is stolen.
- □ As you arrive at your building early one morning, you encounter a coworker leaving the building. The coworker nervously explains that he sometimes prefers to work overnight without the distraction of others.
- □ Your organization's network service is disrupted following a denial of service attack

How Is Information Targeted?

Any of these scenarios might point towards a possible threat. Examining past cases reveals that adversaries commonly use certain collection methods—some of which are identified here. Note that this list is not all inclusive. Additional methods are identified in the course Resources. Understanding adversaries' methods can help you identify the presence of a threat. Let's take a closer look at the identified collection methods.

Exploitation of Cyber Operations

Cyber operations and other kinds of suspicious network activity are attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information. This may be done through phishing operations, cyber intrusion, malicious network scans, the emplacement of viruses or malware, backdoor attacks, or the acquisition of usernames and passwords to gain access to networks.

This is a dangerous and very real threat. An adversary can target you from anywhere, obfuscate their trail, and target multiple assets at a time. It is a low-risk and potentially high-reward method for our adversaries. Here are some indicators you should be aware of. Take a look; then select Countermeasures to see what you can do to protect against this collection method.

Indicators

The following is a list of suspicious indicators related to suspicious network activity and cyber operations:

- Unauthorized system access attempts
- Unauthorized system access to or disclosure of information
- Any acts that interrupt or result in a denial of service
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- E-mails received from unknown senders (that include social engineering attempts such as phishing)
- If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

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

- Comply with the measures in your company's Technology Control Plan (TCP)
- Conduct frequent computer audits
  - Ideally: Daily
  - At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Avoid responding to any unknown request and report these requests
- Disconnect computer system temporarily in the event of a severe attack

Technology Control Plan (TCP)

- Stipulates how a company will control access to its export-controlled technology
- Outlines the specific information that has been authorized for release
- May be required by the National Industrial Security Program Operating Manual (NISPOM) and the International Traffic in Arms Regulations (ITAR) under certain circumstances
- Protects classified and export-controlled information
- Controls:
  - Access by foreign visitors
  - Access by employees who are foreign persons

Attempted Acquisition of Technology

Attempted acquisition of technology includes attempts to acquire protected information via direct purchase of firms, through the use of front companies, or through third countries. Adversaries may attempt to purchase controlled technologies, whether it's the equipment itself, or diagrams, schematics, plans, or spec sheets. Successful use of this method may land an adversary protected technology and information and bring grave consequences to the United States.

Indicators

The following is a list of suspicious indicators related to the attempted acquisition of technology:

Initial Request

- The request is directed at an employee who does not know the sender and who is not in the sales or marketing office
- Solicitor is acting as a procurement agent for a foreign government
- Company requests technology outside the requestor's scope of business
- Individual has a lack of/no knowledge of the technical specifications of the requested type of technology

Order details

- Vagueness of order: Quantity, delivery destination, or identity of customer
- Unusual quantity
- Requested modifications of technology
- Rushed delivery date

Shipping

- End user is a warehouse or company that organizes shipments for others
- End user address is in a third country
- Address is an obscure PO Box or residence
- Multiple businesses are using the same address
- Buyer requests all products be shipped directly to them
- Requestor offers to pick up products rather than having them shipped

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

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

- Comply with the measures in your company's Technology Control Plan (TCP)
- Avoid responding to any unknown request and report these requests
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified:
  - Do not respond in any way
  - Report the incident to security personnel

Exploitation of Experts

The exploitation of experts is an increasingly common method of operation. The number of foreign academics requesting work with classified programs continues to rise. Adversaries exploit experts to acquire protected information via requests for peer or scientific board reviews, requests to study or consult with faculty members, or applications for admission into academic institutions. Placing academics at, and requesting to collaborate with, U.S. research institutions under the guise of legitimate research provides adversaries with access to developing technologies and research.

Indicators

Collection efforts through the exploitation of experts may include, but are not limited to:

- U.S. academics, scientists, engineers, or researchers receive:
  - Requests to provide dual-use components under the guise of academic research
  - Unsolicited emails from peers in their academic or scientific field soliciting assistance on fundamental and developing research
  - Invitations to attend or submit a paper for an international conference
  - Requests to review research papers, in hopes the expert will correct any mistakes
- Collection via foreign academics may involve:
  - Foreign students accepted to a U.S. university or at postgraduate research programs who are recruited by their home country to collect information, and may be offered state-sponsored scholarships as an incentive for their collection efforts
  - 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

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

The following countermeasures may guard against this collection method:

- Review all documents being transmitted; use a translator, when necessary
- Provide foreign representatives with stand-alone information systems
- Share the minimum amount of information appropriate to the scope of the research
- Be aware of project scope and how to handle and report elicitation
- Attend threat awareness training
- Refuse to accept unnecessary foreign representatives into the facility
- Comply with the measures in your company's Technology Control Plan (TCP), including badging systems to identify both foreign and domestic visitors

Request for Information (RFI) / Solicitation

Adversaries employ requests for information and solicitations to establish a connection and collect protected information by directly or indirectly asking or eliciting personnel or protected information and technology. Adversaries may do this through simple requests, usually via email; requests for technical information and manuals; sales, representation, or agency offers; or responses to technical or business services.

Adversaries may also directly request information under the guise of price quotes, marketing surveys, or other direct and indirect efforts. Adversaries primarily request this information using email, phone, or web form submissions approaches. While not every request is an indication you are being targeted, adversaries often use this method, and you must be alert to the potential threat.

Indicators

There are several possible indicators of this collection method, including, but not limited to, those listed below.

The requestor:

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

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

The following countermeasures can protect against requests for information and solicitation of services:

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

Foreign Visit

Using foreign visits as a collection methodology, adversaries attempt to gain access to and collect protected information that goes beyond what is permitted and intended for sharing.

This applies to visits to cleared contractor facilities that are pre-arranged by foreign contingents and also to unannounced visits. It is important that your organization have procedures in place for foreign visits. During a visit, your information and technology may be vulnerable.

Indicators

Suspicious or inappropriate conduct during foreign visits can include:

- Requests for information outside the scope approved for discussion
- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information and becoming irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed
- Individuals providing last-minute changes to visitor list
- Individuals attempting access to areas that are not part of the visit

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

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

- Contractors may coordinate with DCSA prior to visit
- Prior to visit: attend briefings on approved visit procedures
- Prior to visit: walk visitor route and identify vulnerabilities
- Be aware of restrictions on the visitors, and the nature of the threat
- Participate in post-visit debriefs
- Ensure visitors do not bring recording devices, including cell phones, into the facility

Foreign Travel

Americans are frequently targeted while travelling abroad for both work-related and personal reasons.

In countries with very active intelligence and security services, everything foreign travelers do—including inside the hotel room—may be monitored and recorded.

Travel is also often used as an opportunity for an initial contact. It is much easier for a foreign entity to contact foreign travelers away from home where they may be more vulnerable.

Indicators

The following are suspicious indicators related to foreign travel:

- Bugged hotel rooms or airline cabins
- Intercepts of communications and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment attempts via bribery, blackmail, or coercion

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

- Do not publicize travel plans and limit sharing of this information to people who need to know
- Conduct pre-travel security briefings
- Maintain control of sensitive information, media, and equipment
  - Do not pack these types of articles in checked baggage; carry them with you 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
- Limit sensitive discussions; public areas are rarely suitable for discussion of sensitive information
- Do not use information systems at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely

Insider Threat

The threat that an insider will use their authorized access to do harm to the security of the United States makes the insider threat the most potentially damaging of all collection methods.

This threat can cause damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of resources or capabilities. The threat can come either wittingly or unwittingly from employees, contractors, or anyone with legitimate access to an organization.

There are certain personality traits and life experiences that are more likely to lead a person to become an insider threat. There are also certain lifestyle cues to watch out for.

While certainly not everyone exhibiting these behaviors is a spy—and most are not—you need to be familiar with the indicators.

Indicators

Potential espionage indicators include, but are not limited to:

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

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Countermeasures

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

- Request training on the insider threat
- Attend briefings on elicitation methods
- Be alert to actions of other employees
- Monitor the activities of foreign visitors for indications that they are targeting company personnel
- Report suspicious behaviors and activities including potential espionage indicators and signs of foreign targeting of personnel
- Limit the dissemination of sensitive information based on need-to-know
- Monitor classified systems for reportable anomalies

Methods and Indicators

Now that you're aware of the various collection methods, it's important you are also aware of recruitment methodology. In my foreign intelligence days, I used these methods myself.

Foreign entities are constantly looking for people to recruit. They use elicitation as a technique to subtly extract information about you, your work, and your colleagues. When done well, elicitation can seem like small talk.

Social networking is an excellent tool for elicitation and is often used in recruitment. An adversary's recruitment efforts often play to their target's background, ego, and ideological beliefs or fears—including job security. When elicitation uncovers an exploitable weakness, blackmail or bribery may be used.

Recruitment often involves contacts with individuals or organizations from foreign countries. However, an already committed U.S. spy may attempt to recruit colleagues. Some indicators of recruitment include signs of sudden or unexplained wealth and unreported foreign travel.

Recruitment Methods

- Elicitation
- Social media
- Blackmail or bribery

Indicators

Reportable indicators of recruitment include, but are not limited to:

- Request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism
- Offer of financial assistance, gifts, or favors by a foreign national or stranger: Beware of those bearing gifts
- Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company

Critical Assets: Assets essential to an organization's mission or to national security that, if exploited, could result in serious harm, including the loss of:

- Classified information
- Proprietary information
- Intellectual property
- Trade secrets
- Personnel

If you suspect that you, a coworker, or your company have been a target of this method, report it to your FSO.

Consider This

DCSA relies on reports from cleared industry. If you were personally targeted, or you became aware of targeting of your company or a co-worker, would you know what to do? Would you know how to report it?

If you suspected that you were targeted by any collection method, would you know the channels to report it?

- ○ Yes; I know exactly what to do and would report it immediately.
- ○ I'm not sure; I'd have to look it up or check with somebody.
- ○ No; I have no idea what I should do, maybe call the hotline?

Reporting Procedures

Every one of us is an owner of security—both the security of information and the security of personnel. We are all responsible for its safekeeping. The National Industrial Security Program Operating Manual, or NISPOM, outlines the reporting requirements that apply to industry.

Employees of cleared industry must report potential threats to their FSO. Depending on the situation, the FSO will then report the possible threat to the facility's DCSA Industrial Security Representative and DCSA Counterintelligence Special Agent. If the possible threat includes actual, probable, or possible espionage; sabotage; terrorism; or subversive activities, the FSO will report it to the FBI and copy DCSA. As you learned earlier, you must be aware of potential espionage indicators.

You must also be familiar with reportable cyber issues and reportable counterterrorism issues.

- Unauthorized access to classified information, systems, or technologies
- Unusual requests for ITAR, EAR, Dual Use technologies or equipment, or any request from embargoed countries
- Attempted exploitation by a Foreign Intelligence Entity (FIE)
- Contact with a known or suspected foreign intelligence officer
- Information of planned, attempted, actual, or suspected terrorism, espionage, sabotage, subversion, or other intelligence activities against defense, U.S. facilities, organizations, or citizens
- Close, continuing associations with foreign nationals
- Contact with foreign diplomatic establishment
- Attempts to gain access without need-to-know
- Unreported foreign travel
- Unexplained affluence
- Unauthorized downloads of information or odd download patterns not consistent with general office policy
- Association with anomalies

Potential Espionage Indicators

- Unauthorized access to classified information, systems, or technologies
- Unusual requests for ITAR, EAR, Dual Use technologies or equipment, or any request from embargoed countries
- Attempted exploitation by a Foreign Intelligence Entity (FIE)
- Contact with a known or suspected foreign intelligence officer
- Information of planned, attempted, actual, or suspected terrorism, espionage, sabotage, subversion, or other intelligence activities against defense, U.S. facilities, organizations, or citizens
- Close, continuing associations with foreign nationals
- Contact with foreign diplomatic establishment
- Attempts to gain access without need-to-know
- Unreported foreign travel
- Unexplained affluence
- Unauthorized downloads of information or odd download patterns not consistent with general office policy
- Association with anomalies

Reportable Cyber Issues

- Network spillage
- Unauthorized use of DOD account credentials
- On-line attempts to target or recruit personnel including elicitation, solicitation and marketing of services, direct request for information, or phishing scams
- Suspicious network activity and/or penetration and intrusion attempts

Reportable Counterterrorism Issues

- Providing financial or material support for a known or suspected terrorist organization
- Advocating violence or the threat of violence to achieve the goals of a known or suspected terrorist group

Examples of Reportable Events or Behaviors

The following is not intended to be an exhaustive list. When in doubt, report an event or behavior.

Recruitment

Report events or behaviors including, but not limited to:

- Contact with an individual associated with a foreign intelligence, security, or terrorist organization
- Offers of financial assistance by a foreign national other than close family
- Requests for classified or unclassified information outside official channels
- Engaging in illegal activity or a request to do so

Information Collection

Report events or behaviors including, but not limited to:

- Requests to obtain classified or protected information without authorization
- Requests for witness signatures for destruction of classified information when destruction was not witnessed
- Operating unauthorized cameras, recording devices, information systems, or modems in areas where classified data are stored, discussed, or processed
- Presence of any listening or surveillance devices in sensitive or secure areas
- Unauthorized storage of classified material
- Unauthorized access to classified or unclassified automated information systems
- Seeking access to sensitive information inconsistent with duty requirements

Information Transmittal

Report events or behaviors including, but not limited to:

- Unauthorized removal of classified or protected material from the work area
- Transmission of classified material via unsecured means
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure means

Suspicious Behavior

Report behavior including, but not limited to:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements
- Repeated or un-required work outside of normal duty hours
- Unexplained or undue affluence
- Sudden reversal of financial situation or sudden repayment of large debts
- Attempts to entice DOD personnel into situations that could place them in a compromising position
- Attempts to place DOD personnel under obligation through special treatment, favors, gifts, money, or other means
- Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person’s interests or financial means
- Indications of terrorist activity
- Concealment of foreign travel
- Making statements expressing support of or sympathy for a terrorist group
- Making statements expressing preference for a foreign country over loyalty to the United States
- Expressing radical statements or actions threatening violence against a coworker, supervisor, or others in the workplace

Derived from the NISPOM and DODD 5240.06

Conclusion

You have just learned how cleared industry and people like you may be targeted. You need to be aware of the threats you and your organization may face.

You need to consider your facility, its technology, networks and programs, and the information you know. How might you be targeted? If you suspect a potential threat, you must report it.

To review additional information on collection methods, recruitment and elicitation, or reporting procedures, refer to the course resources.