

STUDENT GUIDE

**THWARTING THE ENEMY: PROVIDING
COUNTERINTELLIGENCE AND THREAT
AWARENESS INFORMATION TO THE
DEFENSE INDUSTRIAL BASE
PATH 1: PHYSICAL ATTACK**

Contents

Contents 1

Course Overview.....3

Course Introduction.....4

Targeting at Conferences, Conventions, and Trade Shows.....6

Targeted Technology and Information..... 11

Insider Threat..... 13

Recruitment and Elicitation..... 18

Unsolicited and Direct Request 19

Reporting Requirements 24

Suspicious Network Activity 27

Collection Trends 32

Foreign Visits 33

Stolen Technology 38

Solicitation and Seeking Employment 39

Investigation Wrap Up..... 44

Real-Life Case Study 46

Conclusion 47

Appendix: Resource List 48

Course Overview

This is a scenario-based course in which you will learn about various collection methods used by foreign intelligence operatives to target cleared defense contractors (CDCs). One main scenario is threaded throughout the course to provide an overarching context for more detailed scenarios that are specific to each collection method.

The most common foreign collection methods, which are used in more than 80 percent of targeting cases, include the following:

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

Throughout the course, each scenario will end with a question to help you assess your understanding of these collection methods. Your responses will not be judged in any way; in fact, all responses will provide an opportunity for you to broaden your knowledge of the subject matter.

NOTE: If at any time you suspect that you or your facility may have been a target of any of these collection methods, you must report it to your FSO. For further information, refer to the Counterintelligence section of the DSS Web site at www.dss.mil.

Course Introduction

Setting the stage

A series of bombings at both cleared defense contractor (CDC) and military facilities has resulted in damage to assets of the defense industrial base.

Scenario

Our nation is under attack.

Some attacks are obvious. They are physical. They end up on the nightly news and on the front pages of newspapers around the world.

Other attacks are less obvious, yet they happen every day in alarming numbers and the damage they do can be immeasurable and irrevocable.

These less obvious attacks are often targeting United States defense-related technologies and information. These attacks come from multiple sources. They are pervasive, relentless, and at times successful. 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 not only knowledge of the threat and diligence on the part of government and military personnel, but it also relies heavily on all personnel of the defense industrial base. You play a role. You must be vigilant.

BREAKING NEWS

We're learning more tonight about yesterday's bombings across the conflict region and here at home. What we've learned is that the targets included both military and civilian personnel and both military and cleared contractor facilities.

Your role

When a disaster occurs, the resulting investigation often reveals that the disaster was actually made up of many smaller events.

As you follow this investigation, you will learn about events that led up to the disaster, and you will consider the decisions that were made.

Along the way, you will meet people that both knowingly and unknowingly played a part in the events leading up to the disaster.

You will also accumulate a library of resources, including the adversary's files. These files contain the information the adversary collected and used to carry out the attack. Take note of the valuable information that is presented to you, as you may want to turn back a few pages to review it from time to time.

Other key players

Before we get started, let's first review some of the key players that are involved not only in protecting against such disasters but also in causing them.

Every cleared defense contractor (CDC) has a **facility security officer (FSO)** who is responsible for the overall security of the facility and for ensuring that security regulations and policies are followed. This role should be familiar to you, because your facility also has an FSO.

The **field counterintelligence (CI) special agent** represents the Defense Security Service, or DSS, which is an agency within the Department of Defense. One role of the DSS is to support cleared defense contractors like you. The DSS also relies on you to be its eyes and ears within the defense industrial base.

The term "**adversary**" is used throughout this course to represent the adversary organization that the FSO and CI special agent are trying to protect you from.

Targeting at Conferences, Conventions, and Trade Shows

Timeline Introduction

Disasters don't "just happen." Many small events must first take place, building the perfect storm that invites disaster in.

The investigators have discovered one of the adversary's safe houses and have used files found there to piece together a timeline. To follow the investigation, you will review the investigation files on the following timeline.

Date	Event
August	List of potential contacts is purchased
September	Investigation File: Targeted CDC at conference
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	Investigation File
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Investigation File
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	Investigation File
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	Investigation File
December	Investigation File
Now	Bombings

Contact: September Targeted at: Conference

Scenario: Jack Smith, an engineer for a major cleared defense contractor (CDC), attended an industry trade show a few years before the bombings. While there, Mr. Smith was befriended by a man who shared similar professional interests.

Mr. Smith has a SECRET clearance; he has no security violations on his record; and he has a record of exceptional performance reviews. He would never knowingly reveal sensitive or classified information. Yet, unbeknownst to him, he did.

Through a series of seemingly innocent conversations, he shared many details. Although no one detail was classified, taken together they painted a more complete picture.

As it turns out, his new friend was a representative of a foreign group and was trolling the trade show for information on technology developed by Mr. Smith's facility. The pieces provided by Mr. Smith put this foreign group one step closer to its ultimate goal.

Take a look at what the adversary collected from Mr. Smith. When you're satisfied with your review of this file, you may move on to the knowledge check and feedback.

Adversary File: Information collected from J. Smith
Information obtained: <ul style="list-style-type: none">• Unmanned aerial vehicle (UAV) technology details• UAV component information• Leads on sensor technology contacts• Identity of key positioning and navigation technology
Leads: <ul style="list-style-type: none">• Specific components to locate and obtain• Possible cleared defense contractors (CDCs) to target• Possible industry experts to elicit

Scenario Question

Mr. Smith was targeted at a conference. When discussing work details at a conference, what philosophy would you follow? Select your response; then review the feedback that follows.

- a. Sharing ideas with colleagues is a great way to learn. As long as classified or confidential details are not discussed, there's no harm.
- b. Exchanging ideas with others in the same field is the best way to advance technology. Within the safe environment of an invitation-only conference, no topic should be off limits.
- c. It's best to do more listening and less talking.

Scenario Question Feedback

Even when surrounded by colleagues within your field, you always have to be careful in what you say and aware of those around you. Any event that places people with similar knowledge and interests in the same location has the potential to be exploited. Adversaries can steal things, like computers, equipment, cell phones, and mobile devices, and they can learn things just by talking to you.

Targeting personnel at conferences and other industry events is common. Because these events place knowledgeable people together, they are a potential gold mine of information for an adversary. In fact, it is estimated that as many as one in 20 conference attendees is there solely to collect information. It's a much more common practice than you may realize, but it's an efficient method for an adversary.

Of course, attending an industry event doesn't make you an automatic target of an adversary, but there are several indicators to be aware of. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Targeting at Seminars, Conventions, and Trade Shows
This method directly links targeted programs and technologies with knowledgeable personnel.
Technique
<ul style="list-style-type: none"> • Technical experts may receive invitations to share their knowledge • Experts may be asked about restricted, proprietary, and classified information
Indicators
<p>The following are suspicious indicators related to seminars, conventions, and exhibits:</p> <ul style="list-style-type: none"> • Prior to event: <ul style="list-style-type: none"> ○ Personnel receive an all-expenses-paid invitation to lecture in a foreign nation ○ Entities want a summary of the requested presentation or brief 6-12 months prior to the lecture date ○ Host unsuccessfully attempted to visit facilities in the past ○ Travel to event may pose targeting opportunities • During event: <ul style="list-style-type: none"> ○ Telephone monitoring and hotel room intrusions

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

Countermeasures

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

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

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Targeted Technology and Information

What do foreign entities want?

The short answer is that foreign entities want anything that may be of value. Obviously, they like to get their hands on the latest sensitive or critical technology; but nothing is too small.

The information that foreign entities target is not limited to classified information. Oftentimes, foreign entities are able to piece together enough unclassified data to learn things—even classified things—that you, your employer, and your country wouldn't want them to know.

Review the table below to learn about the types of information and technology that foreign entities may target.

Targeted Technology and Information
<ul style="list-style-type: none"> • Technology information, which includes both classified and unclassified <ul style="list-style-type: none"> ○ Militarily Critical Technology: <ul style="list-style-type: none"> • Any technology that would allow potential adversaries to make significant advances in the development, production, and use of military capabilities • Department of Defense maintains a list of applicable technology • Export is strictly controlled by the International Traffic in Arms Regulations (ITAR) • Illegal export of this technology often results in fines and/or criminal charges ○ Dual Use Technology: <ul style="list-style-type: none"> • 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 • Contingency plans • Personal and personnel information • Programs, deployments, response procedures • Critical program information

What do foreign entities do with the information they collect?

Foreign entities have numerous uses for the information that they obtain from contractor organizations like yours. Sometimes they use it simply to see what you are up to.

Sometimes they use it to help their countries or others build a similar program. They can save millions—sometimes billions!—of dollars taking advantage of the research and development that your company has spent years building. In an instant, your strategic and competitive edge can be gone.

Other times, they sell or trade the information they have obtained to others. Once they have your information and technology, there's really no telling what they may do with it or where it may end up.

Review the table below to learn about top 10 targeted technologies that foreign entities may target.

Top 10 Targeted Technologies
<ul style="list-style-type: none">• Information systems• Aeronautics, including technology related to unmanned aerial vehicles (UAVs)• Lasers and optics• Sensors• Marine systems• Positioning, navigation, and time• Electronics• Industrial Based Technology List (IBTL)• Armaments and energetic materials• Materials and processing

*NOTE: To view the most up-to-date information on targeted technology and information, refer to the *Targeting U.S. Technologies: A Trend Analysis of Defense Reporting from Industry* report. This report is accessed within the Counterintelligence section of the DSS website at www.dss.mil.*

Insider Threat

Timeline update

BREAKING NEWS
<i>There's still no word on who is responsible, but we do now know who the targets were. The bombed locations include both the U.S. headquarters and a foreign office of a cleared U.S. defense contractor. One of our military installations was also hit. Officials are not providing further details at this time.</i>

There's much more information to go through before we'll be able to fully see what happened here. Let's continue by looking at the next investigation file on the timeline.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	Investigation File: Insider Threat
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Investigation File
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	Investigation File
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	Investigation File
December	Investigation File
Now	Bombings

Contact: November
Threat: Insider

Scenario: Julie Sims, an employee at a cleared defense contractor, was a talented and knowledgeable engineer. Over the past few years, Julie's work habits changed. She often worked long and irregular hours. Though her work schedule seemed to show she was overworked, she constantly requested to be put on additional projects. She was also always very interested in the work of those around her and was known to ask very detailed questions about projects she was not a part of, sometimes to the discomfort of others.

There was an agenda behind Ms. Sims' schedule, work requests, and propensity to ask many questions. Over the course of the two years leading up to the bombing, Ms. Sims was collecting information that she then sold to a foreign group. While Ms. Sims was seen as a trusted employee within her firm, she was actually a traitor not only to her company, but also to her country.

Adversary File: Information collected from J. Sims
Information obtained: <ul style="list-style-type: none">• UAV schematics• UAV component specifications
Leads: <ul style="list-style-type: none">• UAV program details• UAV CDC locations• Overseas UAV production facilities

Scenario Question

The cleared defense contractor was the target of an insider threat. If you had worked with Ms. Sims, which of her behaviors might you have found suspicious? Select all that apply; then review the feedback that follows.

- a. Working long and irregular hours
- b. Requesting additional work
- c. A tendency to ask many questions
- d. These characteristics are typical of a diligent, ambitious employee. I wouldn't have thought of any of them as being suspicious.

Scenario Question Feedback

The insider threat is the collection method that has the potential to do the most damage. It isn't limited to government and military targets; facilities like yours may be targeted as well.

Answer options A, B, and C can all be indicators of an insider threat. While it is true that Ms. Sims could simply be an ambitious employee, many of her behaviors can also be indicators of an insider threat. Of course, not everyone exhibiting these behaviors is a spy; in fact, most are not. But you need to be aware that this type of threat is possible within your facility.

Placing someone within your facility to gather information is an ideal situation for an adversary. An insider has a level of access that no other method enjoys. There is no end to what an adversary can learn from an insider!

Potential indicators of espionage are listed below. Notice that certain behaviors and lifestyle characteristics, such as those that Ms. Sims showed, can be signs. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Insider Threat
The insider threat has the potential to inflict the greatest damage of any collection method.
Technique
<p>Targets of the insider threat include:</p> <ul style="list-style-type: none"> • Employees • Contractors • Anyone with legitimate access to an organization
Indicators
<p>The following is a list of potential espionage indicators:</p> <ul style="list-style-type: none"> • Alcohol or other substance abuse or dependence • Mental health issues • Extreme, persistent interpersonal difficulties • Hostile or vindictive behavior • Criminal behavior • 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
- Works hours inconsistent with job assignment
- Repeated security violations
- Reluctance to take polygraph

Countermeasures

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

- 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
- Limit the dissemination of sensitive information based on need-to-know
- Monitor classified systems for reportable anomalies

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Recruitment and Elicitation

Do you know how a person goes from being a regular American citizen to an insider threat or a spy?

Foreign entities are constantly looking for people to recruit. They look for certain backgrounds, behaviors, and lifestyles that they can exploit. They especially look to people like you who work within the defense industrial base.

They also 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. You never know if entities are using small talk to pass the time or to gather intelligence.

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

The DSS Elicitation brochure is available for your review in the online course library.

Unsolicited and Direct Request

Timeline update

BREAKING NEWS
<i>We're just now learning that at least one employee for a cleared U.S. defense contractor was involved in the bombings. The person has been taken into custody, though officials have yet to release a name. We've also learned that the contractor facilities hit were responsible for developing unmanned aerial vehicles, referred to as UAVs within the industry.</i>

We still have much to investigate, so we need to keep moving. Let's continue by looking at the next investigation file on the timeline.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	CDC employee working for adversary
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Investigation File: Unsolicited and Direct Request
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	Investigation File
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	Investigation File
December	Investigation File
Now	Bombings

Contact: January
Targeted by: Unsolicited and Direct Request

Scenario: Bob Lopez, a scientist for a cleared defense contractor, was contacted by a student working on her master's thesis in aeronautics. The student asked several questions regarding sensors and unmanned aerial vehicles, or UAVs. Mr. Lopez was happy to help and answered all of her questions thoroughly.

Unknown to Mr. Lopez, the student wasn't a student at all. She was an agent for a foreign group working on a UAV program of its own. Mr. Lopez's assistance provided them with a dangerous amount of information.

The loss of this information was devastating from a competitive and strategic advantage standpoint, for both Mr. Lopez's company and his country. From a military standpoint, the loss has proven to be catastrophic. Until the other day, Mr. Lopez had no idea what he had done.

Adversary File: Information collected from B. Lopez
Information obtained: <ul style="list-style-type: none">• UAV essential components and their manufacturers• Sensor manufacturers• Confirmation of U.S. and overseas UAV and sensor production facilities location
Leads: <ul style="list-style-type: none">• UAV and sensor components• UAV component and sensor manufacturers

Scenario Question

Mr. Lopez was the target of an unsolicited and direct request. How would you handle a call soliciting information about your work? Select your response; then review the feedback that follows.

- a. If the requestor can provide a good reason for needing the information, I'd provide the requested information.
- b. As long as the information provided is neither confidential nor classified, I see no harm in sharing it.
- c. I view all unsolicited requests with suspicion. If I can't verify the requestor's identity and legitimate need-to-know, I don't provide any information

Scenario Question Feedback

You should always be suspicious of unsolicited requests for information, because sharing even unclassified information can be dangerous. In counterintelligence, we often see examples where putting together enough pieces of unclassified information allows an adversary to learn classified information.

Adversaries rely upon people like you to acquire the information they need. They are skilled at providing what seem to be legitimate reasons for needing information, and they often pose as students. You must always be alert to the potential of this threat.

So what should you watch out for? Some of the indicators are listed below. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Unsolicited and Direct Requests
This method uses an information request from an unknown source that was not sought or encouraged.
Technique
Requests may originate from: <ul style="list-style-type: none"> • Foreign companies • Individuals • Foreign government officials • Organizations
Indicators
There are several possible indicators of unsolicited and direct requests, including, but not limited to, those listed below. The requestor: <ul style="list-style-type: none"> • Sends a request using a foreign address • Has never met recipient • Identifies self as a student or consultant • Identifies employer as a foreign government • States that work is being done for a foreign government or program • Asks about a technology related to a defense program, project, or contract • Asks questions about defense-related programs using acronyms specific to the program

- Insinuates the third party he/she works for is "classified" or otherwise sensitive
- Admits he/she could not get the information elsewhere because it was classified or controlled
- Advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- Advises the recipient not to worry about security concerns
 - Assures the recipient that export licenses are not required or not a problem

Countermeasures

The following countermeasures can protect against unsolicited and direct requests:

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

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Reporting Requirements

As an employee of a cleared defense contractor, or CDC, you are the first line of defense against espionage.

It is essential you report any incident or behavior that may be related to a potential compromise of classified information or inappropriate disclosure of sensitive unclassified information.

The National Industrial Security Program Operating Manual, or NISPOM, outlines reporting requirements that all contractor facilities must follow. It requires contractors to report certain events, which are listed in the table below.

NISP Reporting Requirements
<p>NISPOM requires contractors to report certain events that affect:</p> <ul style="list-style-type: none">• Status of facility clearance• Status of employee's personnel security clearance• Proper safeguarding of classified information• Indication of classified information loss or compromise• Possible cyber intrusions <p>Must specifically report:</p> <ul style="list-style-type: none">• Security violations• Suspicious contacts• Indications of:<ul style="list-style-type: none">○ Potential Insider Threats○ Espionage○ Sabotage○ Terrorism○ Subversive activity

When submitting a report, you must provide the context of the incident. Because targeting can be subtle and difficult to recognize, you should report any suspicious conversations to your Facility Security Officer (FSO). He or she will direct your information to the appropriate authorities, who will assess it and determine whether a potential counterintelligence concern exists. Specifically, your FSO will report any probable espionage incidents directly to the FBI with a copy to DSS.

Review the table on the following pages for examples of reportable events and behaviors.

Examples of Reportable Events or Behaviors
Note that this 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: <ul style="list-style-type: none"> • Contact with an individual associated with a foreign intelligence, security, or terrorist organization • An offer of financial assistance by a foreign national other than close family • A request 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: <ul style="list-style-type: none"> • 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, computers, 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 • Making statements expressing support of or sympathy for a terrorist group • Making statements expressing preference for a foreign country over loyalty to the U.S. • Expressing radical statements or actions threatening violence against a coworker, supervisor, or others in the workplace

Information Transmittal

Report events or behaviors including, but not limited to:

- Unauthorized removal of classified or protected material from the work area without appropriate authorization
- Transmission of Classified material via unsecured means
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure telephone
- Concealment of foreign travel

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
- 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

Suspicious Network Activity

Timeline update

BREAKING NEWS
<p><i>It's been discovered that American citizens played a large role in the bombings. Over the course of several months, dozens of employees of cleared U.S. defense contractors were contacted. Much information was taken from some of these people. Authorities close to the investigation disclosed that individual investigations are ongoing and may result in criminal charges ranging from the illegal export of critical technology to the unauthorized disclosure of classified information.</i></p>

We're getting closer to wrapping this thing up. Let's look at the next investigation file on the timeline.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	CDC employee working for adversary
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Critical information revealed via unsolicited request
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	Investigation File: Suspicious Network Activity
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	Investigation File
December	Investigation File
Now	Bombings

Contact: June
Targeted by: Suspicious Network Activity

Scenario: John Wick, a network administrator at a major cleared defense contractor, was passed up for promotion. In an apparent act of retaliation, Mr. Wick disarmed a series of network defense tools, including the firewalls that protect the contractor's information systems. The changes made by Mr. Wick opened the contractor's system up to outsiders.

On the other side of the world, the adversary was searching for information on technology related to Mr. Wick's facility. It didn't take long for the group to locate a hacker who had obtained information using the access Mr. Wick provided.

The adversary purchased this information, including program details, specifics about the technology they develop, contingency plans, and personnel data.

This loss places sensitive technology in foreign hands. It is unknown if the U.S. can ever regain the strategic advantage it has now lost.

Adversary File: Information collected from J. Wick
<p>Information obtained:</p> <ul style="list-style-type: none"> • Sensor technology and technical specifications • Positioning and navigation technology and components • UAV technical specifications
<p>Leads:</p> <ul style="list-style-type: none"> • UAV facility targets • UAV program development further advanced
<p>Program funding secured:</p> <ul style="list-style-type: none"> • Sale of sensor technology complete • Sale of navigation technology complete

Scenario Question

A cleared defense contractor was the target of Suspicious Network Activity. What measures are in place at your facility to protect against this type of threat? Select all that apply; then review the feedback that follows.

- a. Computer audits are frequently conducted.
- b. Intrusion attempts are reported.
- c. A Technology Control Plan is in place.
- d. I am not aware of any specific measures in place at my facility.

Scenario Question Feedback

Also known as cyber threats, cyber terror, or cyber war, Suspicious Network Activity is the fastest growing method of operation for adversaries. As a low-risk and potentially high-reward method, it is a favorite among adversaries because they can target your facility from anywhere. Your facility should be doing all it can to protect against this threat.

Answer options A, B, and C can all be used to protect your facility from Suspicious Network Activity and cyber threats. If your facility does not already have protections in place, it should implement all of these measures and more to protect against this type of threat.

There are several indicators that can clue you in that you are being targeted. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Suspicious Network Activity and Cyber Threat
Suspicious Network Activity is the fastest growing method operation for foreign entities seeking to gain information about U.S. interests. It may also be referred to as cyber terror, cyber threats, and cyber warfare, among other names.
Technique
<p>An adversary may target anyone or any system at any facility, using a number of methods:</p> <ul style="list-style-type: none"> • Input of falsified, corrupted data • Malware, malicious code, viruses • Hacking • Chat-room elicitation • E-mail solicitation <p>Target: <i>Anyone at any facility</i></p>
Indicators
<p>The following is a list of suspicious indicators related to Suspicious Network Activity and cyber threats:</p> <ul style="list-style-type: none"> • 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 (for example, social engineering attempts such as phishing)

Countermeasures

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

- Comply with the measures outlined 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 to report these requests
- Disconnect computer system temporarily in the event of a severe attack

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

* 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
 - Control access by foreign visitors
 - Control access by employees who are foreign persons

Collection Trends

The DSS Counterintelligence Directorate publishes an annual report entitled Targeting U.S. Technologies. This report compiles all of the suspicious contact reports submitted to DSS within the previous year and summarizes the types of threats, the origins of the threats, and the targets of the threats.

The importance of you being aware of this information cannot be overstated. If you don't know what the threats are and what is being targeted, then how can you protect yourself, your coworkers, and your facility? As a member of industry and the defense industrial base, this report applies directly to you.

Here are some of the key points of the report.

- Commercial actors continue with aggressive collection attempts
- Collectors continue with bold and overt exploitation of the Internet to acquire information by direct request
- Unmanned aerial vehicle (UAV) technology is a priority target of aggressive collectors from various regions

You can also visit the DSS Web site to see the most recent report and the latest information. The Web address can be found in the Resources List in the appendix to this Student Guide.

Foreign Visits

Timeline update

BREAKING NEWS
<p><i>Tonight, the plot thickens. As more details about the bombing are unraveled, a complicated web is forming. We know that several employees of cleared U.S. defense contractors played a role—the majority, unwittingly. We’re now learning that the information systems and networks of major cleared defense contractors were also breached. In a mass cyber attack, much information was taken from these networks. Officials are looking into why these network breaches were never reported.</i></p>

We have just a few more files to sort through. Let’s see what we learn from the next investigation file on the timeline.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	CDC employee working for adversary
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Critical information revealed via unsolicited request
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	CDC networks compromised
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	Investigation File: Foreign Visits
December	Investigation File
Now	Bombings

Contact: November

Targeted by: Foreign Visit

Scenario: A cleared defense contractor hosted a potential client at its facility. The purpose of the visit was for the potential client to tour the contractor's facility and attend a presentation. The contractor hoped to win a major contract as a result of the visit.

Executives for the cleared defense contractor were surprised when the visitors brought out recording equipment. The visitors explained that needed recordings in order for their executive team to make a final decision. Reluctantly, the cleared defense contractor's CEO agreed to the recording, and the tour and presentation continued.

Unknown to the cleared defense contractor, the visitors had more in mind than simply sharing the tour and presentation with their executive team. The visitors instead studied the recordings closely and were able to learn much about the contractor, including information on key schedules, vendors, and other program details.

The information collected by the adversary not only placed the contractor's relationship with the military in jeopardy, but more importantly, it endangered our nation's war fighters.

Adversary File: Information collected from visit to CDC
<p>Information obtained:</p> <ul style="list-style-type: none"> • Confirmation of necessary UAV components and vendors • UAV program schedule • Positioning and navigation technology and components • Laser technology
<p>Leads:</p> <ul style="list-style-type: none"> • UAV components and configurations confirmed
<p>Program funding secured:</p> <ul style="list-style-type: none"> • Sale of sensor technology complete • Sale of navigation technology complete

Scenario Question

A cleared defense contractor was the target of a foreign visit. How should the contractor have prepared for the visit? Select your response; then review the feedback that follows.

- a. The contractor should have considered various scenarios and been ready to react appropriately. They shouldn't have allowed themselves to be caught off guard.
- b. The contractor should have contacted DSS about the visit and obtained the proper briefing and procedures from DSS.
- c. Being successful in business requires a certain amount of trust in clients and potential clients. Though this situation had consequences, it was handled appropriately

Scenario Question Feedback

It is of the utmost importance that visit procedures are put in place and that the DSS is contacted prior to the visit so that personnel at your facility are prepared to react appropriately. During a visit, your information and technology is extremely vulnerable. Your facility must be prepared for the visit and aware of different ways an adversary may attempt to gain information they are not authorized to have.

Some of the things you should look out for are listed here. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Foreign Visits
Suspicious contact during a foreign visit can occur at any time and may come from many seemingly innocent sources.
Technique
<p>Suspicious contact may come from:</p> <ul style="list-style-type: none"> • One-time visitors • Long-term visitors <ul style="list-style-type: none"> ○ Exchange employees ○ Official government representatives ○ Students • Frequent visitors <ul style="list-style-type: none"> ○ Sales representatives ○ Business associates
Indicators
<p>Suspicious or inappropriate conduct during foreign visits can include:</p> <ul style="list-style-type: none"> • Requests for information outside the scope of what was approved for discussion • Hidden agendas associated with the stated purpose of the visit • Visitors/students requesting information and becoming irate upon denial • Individuals bringing cameras and/or video equipment into areas where no photographs are allowed • Visitors providing last-minute changes to visitor list
Countermeasures
The following countermeasures can protect cleared defense contractors against unauthorized access by foreign visitors:

- Contractors may coordinate with DSS prior to visit
- Prior to visit: 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 that visitors do not bring recording devices, including cell phones, into the facility

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Stolen Technology

People are often skeptical about the urgency of protecting technology and information. They may feel that claims about the threat are overstated.

Listed below are some examples of technology that has been stolen. These examples are not hypothetical thefts; these examples are of technology that has actually been stolen from us and is now in foreign hands.

As you look through these examples, think about the implications. You can decide for yourself how serious each is.

Examples of Stolen Technology
<p>Stolen Technology: Aegis Radar System and Ballistic Missile Defense System</p> <p>Capability: Locate and destroy incoming missiles</p> <p>Years in Development: 20+</p> <p>Cost to U.S. Taxpayers: Billions of dollars</p> <p>Technology Stolen: Late 1990s</p>
<p>Stolen Technology: Military aircraft technology, including F-15, B1 Bomber, and AWACS</p> <p>Capabilities: Several, including surveillance, reconnaissance, defense</p> <p>Years in Development: 50+</p> <p>Cost to U.S. Taxpayers: Trillions of dollars</p> <p>Technology Stolen: Repeatedly over decades</p>

Solicitation and Seeking Employment

Timeline update

BREAKING NEWS
<i>As officials learn more about the bombings, they've discovered that those responsible actually visited cleared U.S. defense contractors. Officials are piecing together what they learned there and if anyone at the involved companies will be fined or prosecuted.</i>

This has been a lot to sort through, but we're almost done. Let's take a look at the final investigation file on the timeline.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	CDC employee working for adversary
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Critical information revealed via unsolicited request
February	Sale of obtained information
March	Joint ventures sought
April	Adversary's online chatter increases
June	CDC networks compromised
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	CDC exploited during visit
December	Investigation File: Solicitation/Joint Venture
Now	Bombings

Contact: December
Targeted by: Solicitation/Joint Venture

Scenario: A cleared defense contractor in the sensor technology field entered into a joint venture with a foreign firm.

Over the course of the venture, representatives of the foreign firm were often seen transmitting documents written in their native language. While some employees of the contractor found this strange, the foreign representatives were never questioned.

The foreign representatives should have been questioned. They were able to collect an enormous amount of information. The consequences of this loss are devastating.

Adversary File: Information collected from the CDC
Information obtained: <ul style="list-style-type: none">• Final details needed to complete UAV program
MISSION OBJECTIVES MET!

Scenario Question

A cleared defense contractor was the target of a solicitation that resulted in a joint venture, and the joint venture was abused. When a facility enters into a joint venture or research, what types of protection measures, if any, should be put into place? Select all that apply; then review the feedback that follows.

- a. All documents being transmitted should be reviewed and translated, if necessary.
- b. Foreign representatives should be given stand-alone computers and have limited network access.
- c. The minimum amount of information should be shared and be limited to what is necessary for the scope of the joint venture/research.
- d. If the defense contractor trusts their partner, there shouldn't be a need to put additional procedures in place.

Scenario Question Feedback

Regardless of how well you think you know a partner, it is very important that the proper measures are put in place to protect your facility's information and technology. Answer options A, B, and C are all measures that can be used to protect your facility from potential adversaries.

You may be solicited in a number of ways: by students seeking internships, by firms seeking partnerships, or by individuals or groups seeking employment. Regardless of the method, successful solicitation provides outsiders with great access and proximity to your facility's most valuable assets: its personnel, information, and technology.

Although many solicitations are legitimate, there are several indicators that you should be aware of. Take a moment to review the table below to learn how to identify and protect yourself against this method.

Collection Method: Solicitation and Seeking Employment
The solicitation and seeking employment collection method may take many forms, including joint ventures or research partnerships, offers of services, or internship programs for foreign students.
Technique
<ul style="list-style-type: none"> • Places foreign personnel in close proximity to cleared personnel • Provides opportunity to build relationships that may be exploited • Places adversary inside facility to collect information on desired technology
Indicators
Indicators include: <ul style="list-style-type: none"> • Foreign visitors transmit documents written in a foreign language to a foreign embassy or foreign country • Foreign visitors request: <ul style="list-style-type: none"> ○ Access to the LAN ○ Unrestricted facility access ○ Company personnel information
Countermeasures
The following countermeasures may guard against this collection method: <ul style="list-style-type: none"> • Review all documents being transmitted; use a translator, when necessary • Provide foreign representatives with stand-alone computers

- Share the minimum amount of information appropriate to the scope of the joint venture/research
- Be aware of project scope and how to handle and report elicitation
- Attend sustainment 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

NOTE: If you suspect you may have been targeted using this method, contact your FSO. For further information, refer to the Counterintelligence section of the DSS website at www.dss.mil.

Investigation Wrap Up

Timeline update

BREAKING NEWS
<p><i>We're hearing from our overseas bureau that a raid was conducted early this morning and several suspects have been arrested. Officials say the final piece to their investigation came from a cleared U.S. defense contractor who had previously partnered with a foreign firm. Officials are also releasing more details about the attack.</i></p> <p><i>The suspects cast a wide net, gathering any information they could from a large number of cleared defense contractors. While they were specifically looking for aeronautical and UAV technology, they sold other information and technologies to help fund their cause. The investigation into where the sold information ended up continues, and investigations into the American citizens and companies who helped the group, wittingly or not, continue.</i></p>

What a picture this paints. Look at all of the events that had to come together. Notice how each one, on its own, is a significant threat that may have dire consequences, never mind the larger disaster each helped to create.

We've covered a lot of information during this investigation. If you'd like to review any of the information that the adversary took from each of the scenarios that we reviewed, you can do so by reviewing the adversary files with each scenario.

Date	Event
August	List of potential contacts is purchased
September	Critical information revealed at industry event
October	American citizen recruitment efforts begin
November	Multiple CDC networks are attacked
November	CDC employee working for adversary
November	CDC contact begins
January	Contact attempts with CDC employees increase
January	Critical information revealed via unsolicited request
February	Sale of obtained information
March	Joint ventures sought

April	Adversary's online chatter increases
June	CDC networks compromised
August	Obtained information is traded
September	Adversary poses as CDC client, solicits proposals
November	CDC exploited during visit
December	Technology lost during joint venture
Now	Bombings

Results

The investigation we've just walked through and its events are all fictitious. These particular events never happened, though events similar to the scenarios you saw happen every day.

The vast majority of targeting cases will not end or result in a physical attack and breaking news headlines around the world. More often, the attacks are on a smaller scale, though they can be just as insidious.

You might see brief mentions of them buried in your local newspaper, or you may not hear of them at all.

Let's quickly take a look at a real case that did make headlines.

Real-Life Case Study

In May 2010, Chi Tong Kuok, a Chinese national, was convicted on charges of conspiring to export defense articles without a license, smuggling goods from the United States, and money laundering.

How did Mr. Kuok obtain the defense articles? By soliciting cleared contractors—some of those he solicited may be just like you. Over a two-year timeframe, Kuok requested communications, encryption, and military grade global positioning system, or GPS, equipment. He often used e-mail to target contractors and changed email addresses and aliases often.

In late 2006, a contact he made with one cleared defense contractor resulted in a suspicious contact report being submitted to DSS. An investigation involving Immigration and Customs Enforcement, or ICE, led to Kuok's arrest in June 2009.

After his arrest, Kuok stated he had been acting at the direction of officials from his country and that items were sought to listen to or monitor the U.S. government and military.

Conclusion

You have just followed an investigation that involved the targeting of cleared defense contractors and people like you.

You need to be aware of these threats. You need to consider your facility, its technology, and the information you know. You need to consider how you might be a target.

If you are subject to a suspicious contact or observe suspicious behavior or events, you must report it.

To review information on any of the ways you may be targeted, information on reporting procedures, or information on specific and technologies that may be targeted, please refer to the online course library.

Appendix: Resource List

The following is a partial listing of the counterintelligence resources available to the Defense Industrial Base. Contact your FSO, DSS Industrial Security Representative (IS Rep), or local DSS Counterintelligence (CI) Office for more information.

Defense Security Service (DSS) and the DSS Counterintelligence (CI) Directorate

DSS has several resources available to cleared contractors. Specifically, the DSS CI Directorate publishes an annual threat trend analysis report, brochures, and other information related to specific threats and collection methods. Resources available from the DSS CI Directorate are accessible via the counterintelligence page of the DSS website at <http://www.dss.mil> or through your DSS IS Rep.

Federal Bureau of Investigation (FBI)

The FBI has primary responsibility for counterintelligence investigations within the U.S. It has a variety of resources, including the following:

- **Counterintelligence Strategic Partnership:** A program that shares information related to the U.S. vulnerability to foreign powers, terrorist groups, and other criminal elements
- **InfraGard:** Provides information related primarily to cyber threats and threats to critical infrastructure

Security officials may contact their local FBI offices to become involved in these programs and to request more specific threat information, when appropriate and needed. To locate contact information for your local FBI office, refer to <http://www.fbi.gov>.

Other Federal Sources of Counterintelligence Information

In addition to the FBI, other federal sources of information include the following. Please note that this is NOT an exhaustive list.

- **Department of Homeland Security (DHS):** <http://www.dhs.gov>
- **Defense Intelligence Agency (DIA):** <http://www.dia.mil>
- **Department of State Bureau of Diplomatic Security:** <http://www.state.gov/m/ds/>

- **National Counterintelligence Executive (NCIX):**
<http://www.ncix.gov>
- **The Interagency OPSEC Support Staff:** <http://www.ioss.gov>

Government Contracting Activity (GCA)

Your facility's GCA may provide contract-specific threat information and program threat assessments. Contact your GCA for program-specific information.