

STUDENT GUIDE

**THWARTING THE ENEMY: PROVIDING  
COUNTERINTELLIGENCE AND THREAT  
AWARENESS INFORMATION TO THE  
DEFENSE INDUSTRIAL BASE  
PATH 2: ECONOMIC ATTACK**

***Contents***

Course Overview.....3  
Course Introduction.....4  
Targeting at Conferences, Symposiums, and Trade Shows .....6  
Targeted Technology and Information..... 11  
Insider Threat..... 13  
Recruitment and Elicitation..... 18  
Unsolicited and Direct Requests ..... 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](http://www.dss.mil).*

## Course Introduction

### Setting the stage

An economic disaster has resulted in loss of our nation's competitive advantage, widespread unemployment, and compromise of personal information.

### Scenario

Our nation's technical lead, competitive edge, and strategic military advantage are at risk. Our intellectual property, innovative skills, and military technology are under attack.

Individually, these attacks go largely unnoticed, but the cumulative effect and the damage done can be immeasurable and irrevocable, and our national security interests could be compromised.

Attacks on United States defense-related technologies and information come from multiple sources. They are pervasive, relentless, and, at times, successful.

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**

*Tonight we're hearing from officials that attacks on our nation's defense-related technology and information have increased dramatically. As the global battle for markets and technologies heats up, there is growing concern over the loss of American defense-related technology and intellectual property. We're learning that the lines of espionage are becoming less clearly defined and many of the targets are not what you may expect. In addition to the military concerns posed, these losses are also impacting the U.S. economy, as foreign competition narrows in on domestic firms. Investigators are looking into recent cases in hopes of preventing additional losses.*

### Your role

Strategic and competitive advantages are neither born nor lost in an instant. When advantages are lost, it is through the accumulation of several smaller losses.

As you follow this examination of the loss of U.S. defense-related information and technology, you will learn about events that contributed to these losses, and you will consider the decisions made by those involved.

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 analyst 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 pieced together a timeline using reports from individual cases. They have also obtained files from several adversary groups. To follow the investigation, you will review the case files on the following timeline.

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

## Contact: March

### Targeted at: Conference

Scenario: Christina Crego, an engineer for a cleared defense contractor (CDC), represented her facility at an industry trade show. The CDC sponsored a booth at the show, and Ms. Crego brought along a prototype of the company's latest technology to demonstrate.

Over the course of the trade show, she was asked many questions about her company's prototype, and she answered each as thoroughly as possible. When the trade show was over, employees of the venue offered to help Ms. Crego pack up her things. In the process of doing so, the prototype was somehow lost.

Ms. Crego was specifically targeted for the information she knows and for what the prototype could reveal. While she was busy answering questions about the prototype, she revealed far more information than she should have. She also failed to notice that most of the questions came from the same three people. The venue employees helping her pack were actually members of a foreign group.

The information she revealed and the "lost" prototype are now in foreign hands. This is devastating not only for Ms. Crego's company, but also for her country.

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

<b>Adversary File: Information collected from C. Crego</b>
Information obtained: <ul style="list-style-type: none"> <li>• Sensor component manufacturers</li> <li>• Sensor technology specifications and schematics</li> </ul>
Lead: <ul style="list-style-type: none"> <li>• Develop and bring to market competing product</li> </ul>

## Scenario Question

*Ms. Crego was targeted during a conference. What measures should cleared defense contractors put in place to protect against this type of threat? Select your response; then review the feedback that follows.*

- a. Defense contractors and attendees should consider what information is being exposed and to whom.
- b. Defense contractors should take mock-up displays instead of real equipment.
- c. Conference attendees should restrict the information provided to only what is necessary for travel and hotel accommodations.
- d. Government or military personnel are far more likely to be targeted in this way; contractor personnel don't need to be concerned with this.

## 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. Answer options A, B, and C are all measures that can be taken to protect yourself from this method.

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.

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

- Conversations involving classified, sensitive, or export-controlled 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
- Provide employees with detailed travel briefings concerning:
  - The threat
  - Precautions to take
  - How to react to elicitation
- 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](http://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.

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

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.

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

*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](http://www.dss.mil).*

## ***Insider Threat***

### **Timeline update**

<b>BREAKING NEWS</b>
<i>A major U.S. sensor technology firm announced today the downsizing of 20,000 employees. The announcement comes following dramatic stock losses that began with the introduction of competing technology. In recent years, the once dominant company has faced increasing competition from foreign firms. In related news, the U.S. military is concerned over increased sensor technology development within the militaries of hostile nations.</i>

There are several more cases to review before we'll have a complete picture of what happened here. Let's continue by looking at the next case file on the timeline.

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

## **Contact: May**

### **Threat: Insider**

Scenario: Ricardo Suarez, an engineer at a cleared defense contractor, was known to be boastful and overstate his involvement in sensitive government programs. He spent a great deal of time on social networking sites and proudly shared that he worked for a cleared defense contractor. He would also tell any coworker that would listen about his ability to count cards and how he routinely won big at casinos.

In the office, he was known to drop into sensitive meetings where he didn't belong and to access classified information, even though he had no need-to-know. Many of his coworkers found him to be quirky, and even entertaining, but no one considered him a threat in any way.

Mr. Suarez's boastfulness and interest in sensitive programs warranted concern. He was not the skilled gambler he presented himself to be, and over the course of several years, he ran up considerable gambling debts.

When Mr. Suarez was contacted by a foreign group, he readily accepted their generous offer to purchase classified information. Mr. Suarez sold a great deal of information to the foreign group, at great cost both to his company and to the security of U.S. war fighters overseas. The damage done by Mr. Suarez was most serious.

<b>Adversary File: Information collected from R. Suarez</b>
<p><b>Information obtained:</b></p> <ul style="list-style-type: none"> <li>• UAV schematics</li> <li>• UAV component specifications</li> <li>• UAV program details</li> <li>• Overseas U.S. military installations with UAV capabilities</li> </ul>
<p><b>Leads:</b></p> <ul style="list-style-type: none"> <li>• UAV program details</li> <li>• UAV CDC locations</li> <li>• Target U.S. military installations</li> </ul>

## Scenario Question

*The cleared defense contractor was the target of an insider threat. How do you feel about reporting a coworker's behavior or details of their personal life or lifestyle? Select your response; then review the feedback that follows.*

- a. Work is work. The personality or behavior of my coworkers, their personal lives, and lifestyles are none of my business. I wouldn't report it.
- b. I may wonder about a person like Mr. Suarez, but unless I can provide a specific work-related example, it wouldn't ever be my place to report anything. Doing so would be unprofessional.
- c. It might make me uncomfortable, but I'd report it.

## 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.

While it is true that Mr. Suarez could simply be a big talker who enjoys casino life, many of his personality and lifestyle traits can also leave him vulnerable to targeting by foreign operatives. It is this potential vulnerability that makes it your responsibility to take note of and report certain aspects of your coworkers' behaviors and lifestyles.

Of course, not everyone exhibiting these behaviors is a spy; in fact, most are not. But you need to be aware that the insider threat is possible within your facility.

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

<b>Collection Method: Insider Threat</b>
The insider threat has the potential to inflict the greatest damage of any collection method.
<b>Technique</b>
<p>Targets of the insider threat include:</p> <ul style="list-style-type: none"> <li>• Employees</li> <li>• Contractors</li> <li>• Anyone with legitimate access to an organization</li> </ul>
<b>Indicators</b>
<p>The following is a list of potential espionage indicators:</p> <ul style="list-style-type: none"> <li>• Alcohol or other substance abuse or dependence</li> <li>• Mental health issues</li> <li>• Extreme, persistent interpersonal difficulties</li> <li>• Hostile or vindictive behavior</li> <li>• Criminal behavior</li> <li>• Unexplained or sudden affluence</li> <li>• Unreported foreign contact and travel</li> <li>• Inappropriate, unusual, or excessive interest in classified, sensitive, or</li> </ul>

proprietary information
<ul style="list-style-type: none"><li>• Misuse of information systems</li><li>• Divided loyalty or allegiance to the United States</li><li>• Works hours inconsistent with job assignment</li><li>• Repeated security violations</li><li>• Reluctance to take polygraph</li></ul>
<b>Countermeasures</b>
<p>The following countermeasures can be taken by cleared defense contractors to guard against the insider threat:</p> <ul style="list-style-type: none"><li>• Request training on the insider threat</li><li>• Attend briefings on elicitation methods</li><li>• Be alert to actions of other employees</li><li>• Monitor the activities of foreign visitors for indications that they are targeting company personnel</li><li>• Limit the dissemination of sensitive information based on need-to-know</li><li>• Monitor classified systems for reportable anomalies</li></ul>

*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](http://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 Requests***

### **Timeline update**

<b>BREAKING NEWS</b>
<i>Tonight we're learning that an employee of a cleared U.S. defense contractor has been arrested for espionage. Officials are not yet releasing a name, but they did say they were first tipped off to the existence of a potential spy when the defense contractor was suspended from government contracts due to suspicion over the export of militarily critical technology.</i>

We still have a ways to go, so we need to keep moving. Let's continue by looking at the next case file on the timeline.

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

**Contact: July****Targeted by: Unsolicited and Direct Request**

Scenario: Susan Black, a sales manager for a cleared defense contractor, received an e-mail from a potential client asking for a price quote on several of the firm's laser and optics products.

When Ms. Black learned that the potential client was located in another country, she questioned her ability to sell it. However, she quickly dismissed her concern when the potential client indicated he had done the necessary research and no export issues existed. The deal went through, and Ms. Black approved the sale.

Of course, it was Ms. Black's job to know whether her product was subject to export restrictions. Contrary to what she was told, it was a violation of export laws to sell the technology products.

Ms. Black's carelessness put protected technology in foreign hands. This has consequences for Ms. Black personally, for her company, and potentially for her country.

<b>Adversary File: Information collected from S. Black</b>
<p><b>Information obtained:</b></p> <ul style="list-style-type: none"> <li>• Laser technology specifications</li> <li>• Optics components and their manufacturers</li> </ul>
<p><b>Leads:</b></p> <ul style="list-style-type: none"> <li>• Proper laser technology settings</li> <li>• Optics component manufacturers</li> <li>• Information needed to build laser and optics program</li> <li>• Provide information to foreign companies to secure foreign production of components</li> </ul>

## Scenario Question

*Ms. Black was the target of an unsolicited and direct request. Which of the following, if any, would you consider suspicious? Select all that apply; then review the feedback that follows.*

- a. You receive an e-mail from a foreign address and don't know the sender.
- b. Someone you don't know contacts you with questions related to a defense program, project, or contract.
- c. You receive a request from someone indicating that export issues are of no concern.
- d. When I'm contacted, I trust that it's for a good and legitimate reason. I wouldn't necessarily view any of the above as suspicious.

## Scenario Question Feedback

You should always be suspicious of unsolicited and direct requests for information, because sharing even unclassified information can be dangerous. Therefore, answer options A, B, and C should all be considered suspicious.

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. In counterintelligence, we often see examples where putting together enough pieces of unclassified information allows an adversary to learn classified information.

Although not every request is an indication that you are being targeted, 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.

<b>Collection Method: Unsolicited and Direct Requests</b>
This method uses an information request from an unknown source that was not sought or encouraged.
<b>Technique</b>
Requests may originate from: <ul style="list-style-type: none"> <li>• Foreign companies</li> <li>• Individuals</li> <li>• Foreign government officials</li> <li>• Organizations</li> </ul>
<b>Indicators</b>
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"> <li>• Sends a request using a foreign address</li> <li>• Has never met recipient</li> <li>• Identifies self as a student or consultant</li> <li>• Identifies employer as a foreign government</li> <li>• States that work is being done for a foreign government or program</li> </ul>

- 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](http://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.

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

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.

<b>Examples of Reportable Events or Behaviors</b>
Note that this is not intended to be an exhaustive list. When in doubt, report an event or behavior.
<b>Recruitment</b>
Report events or behaviors including, but not limited to: <ul style="list-style-type: none"> <li>• Contact with an individual associated with a foreign intelligence, security, or terrorist organization</li> <li>• An offer of financial assistance by a foreign national other than close family</li> <li>• A request for classified or unclassified information outside official channels</li> <li>• Engaging in illegal activity or a request to do so</li> </ul>
<b>Information Collection</b>
Report events or behaviors including, but not limited to: <ul style="list-style-type: none"> <li>• Requests to obtain classified or protected information without authorization</li> <li>• Requests for witness signatures for destruction of classified information when destruction was not witnessed</li> <li>• Operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed</li> <li>• Presence of any listening or surveillance devices in sensitive or secure areas</li> <li>• Unauthorized storage of classified material</li> <li>• Unauthorized access to classified or unclassified automated information systems</li> <li>• Seeking access to sensitive information inconsistent with duty requirements</li> <li>• Making statements expressing support of or sympathy for a terrorist group</li> <li>• Making statements expressing preference for a foreign country over loyalty to the U.S.</li> <li>• Expressing radical statements or actions threatening violence against a coworker, supervisor, or others in the workplace</li> </ul>

**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>The U.S. dollar fell sharply again today, a sign of today's troubling economic times. The U.S. is simply not as competitive as we once were. In other news, several U.S. defense contractors were fined heavily today for illegally exporting restricted technology to a foreign country. According to an anonymous official, the security clearances of the employees involved were also revoked. Investigators are looking into filing criminal charges</i></p>

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

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

## **Contact: January**

### **Targeted by: Suspicious Network Activity**

Scenario: The network of a major cleared defense contractor was compromised. Network administrators at the facility noticed system abnormalities, including changes to system hardware and software. Several employees reported access issues and receiving denial of service messages, but no outside report was ever submitted.

The cleared defense contractor's information system was targeted by a foreign group. The group was able to obtain volumes of information and data from the contractor. The group sold several pieces of the information and used other pieces to advance related programs in their own country.

This loss has potentially devastating consequences for the cleared contractor, its employees, and the safety of our nation's war fighters.

<b>Adversary File: Information collected from cyber attack on CDC</b>
<p><b>Information obtained:</b></p> <ul style="list-style-type: none"><li>• Identification of information system vulnerabilities</li><li>• Positioning and navigation technology and components</li><li>• Electronics</li><li>• Company personnel information, including Social Security numbers and birth dates</li></ul>

## Scenario Question

*The defense contractor was the target of Suspicious Network Activity. How would your facility handle such activity? Select your response; then review the feedback that follows.*

- a. As far as I know, network activity is not routinely monitored. System administrators are busy enough as it is.
- b. Suspicious Network Activity is dealt with internally. If it involves an employee, that person is subject to reprimand.
- c. Suspicious Network Activity is a serious concern and there are specific procedures in place, including reporting activity to authorities, if warranted.

## 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.

If your facility does not already have protections in place, it should. Facilities like yours and mine must protect themselves by having the proper procedures in place and by reporting instances of compromise.

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.

<b>Collection Method: Suspicious Network Activity and Cyber Threat</b>
Suspicious internet 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.
<b>Technique</b>
<p>An adversary may target anyone or any system at any facility, using a number of methods:</p> <ul style="list-style-type: none"> <li>• Input of falsified, corrupted data</li> <li>• Malware, malicious code, viruses</li> <li>• Hacking</li> <li>• Chat-room elicitation</li> <li>• E-mail solicitation</li> </ul> <p>Target: <i>Anyone at any facility</i></p>
<b>Indicators</b>
<p>The following is a list of suspicious indicators related to Suspicious Network Activity and cyber threats:</p> <ul style="list-style-type: none"> <li>• Unauthorized system access attempts</li> <li>• Unauthorized system access to or disclosure of information</li> <li>• Any acts that interrupt or result in a denial of service</li> <li>• Unauthorized data storage or transmission</li> <li>• Unauthorized hardware and software modifications</li> <li>• E-mails received from unknown senders (for example, social engineering)</li> </ul>

attempts such as phishing)
<b>Countermeasures</b>
<p>The following countermeasures can be taken by cleared defense contractors to guard against this collection method:</p> <ul style="list-style-type: none"> <li>• Comply with the measures outlined in your company's Technology Control Plan (TCP)*</li> <li>• Conduct frequent computer audits <ul style="list-style-type: none"> <li>○ Ideally: Daily</li> <li>○ At minimum: Weekly</li> </ul> </li> <li>• Do not rely on firewalls to protect against all attacks</li> <li>• Report intrusion attempts</li> <li>• Avoid responding to any unknown request and to report these requests</li> <li>• Disconnect computer system temporarily in the event of a severe attack</li> </ul>

*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](http://www.dss.mil).*

<b>* Technology Control Plan (TCP)</b>
<ul style="list-style-type: none"> <li>• Stipulates how a company will control access to its export-controlled technology</li> <li>• Outlines the specific information that has been authorized for release</li> <li>• May be required by the National Industrial Security Program Operating Manual (NISPOM) and the International Traffic in Arms Regulations (ITAR) under certain circumstances</li> <li>• Protects: <ul style="list-style-type: none"> <li>○ Classified and export-controlled information</li> <li>○ Control access by foreign visitors</li> <li>○ Control access by employees who are foreign persons</li> </ul> </li> </ul>

## ***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>Wall Street took another pounding today with a 1,000 point loss. Analysts blame several factors, though the major trigger was severe losses in the electronics sector. In other news, over 20,000 people, all U.S. defense contractor employees, are reportedly the victims of identity theft. We're learning that the information systems and networks of several cleared defense contractors have been breached. Employee information was taken as part of a mass cyber attack. Officials are also reporting that sensitive military information and proprietary technology was also lost in the attack. Officials are looking into why these network breaches were never reported.</i></p>

We have just a few more cases to sort through. Let's see what we learn from the next case file on the timeline.

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

## **Contact: June**

### **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 attend a presentation. The visit was the final stage of the bidding process for a major contract the contractor hoped to win.

Before the presentation began, the visitors insisted on meeting some of the employees involved in the bidding process. Although no meeting had been planned, the contractor complied.

As the visitors spoke with the employees, they asked questions far outside the scope of what was previously agreed upon. Eager to impress the potential client, the employees answered all of their questions.

The cleared defense contractor was unprepared for this visit and failed to recognize that the visitors had an agenda outside of what had been previously discussed. By visiting the facility, the adversary was able to collect an alarming amount of information. This information affects the contractor's relationship and contracts with the military. But a more serious outcome is that it puts our nation's war fighters in danger.

<b>Adversary File: Information collected from visit to CDC</b>
<p><b>Information obtained:</b></p> <ul style="list-style-type: none"><li>• Marine technology program details</li><li>• Positioning and navigation technology capabilities</li><li>• Laser technology limitations and vulnerabilities</li></ul>

## 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 notified all employees about the visit.
- b. The contractor should have identified vulnerabilities.
- c. The contractor should have stuck to the visit schedule.
- d. The contractor had no way of knowing that the visitors had malicious intentions. These sorts of events can be neither predicted nor prepared for.

## 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.

Answer options A, B, and C are all methods the contractor should have used to prepare for the visit.

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.

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

**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](http://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.

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

## Solicitation and Seeking Employment

### Timeline update

BREAKING NEWS
<p>The unemployment numbers were released today and, frankly, they're not good. Unemployment rose again this month and is currently at 13 percent nationally. In other news, government officials are concerned tonight about reports that members of a foreign intelligence group were able to enter a major U.S. cleared defense contractor facility. Officials are piecing together what they learned there and if anyone at the involved companies will be fined or prosecuted. For now, all government contracts with the companies involved have been suspended.</p>

These cases have been a lot to sort through, but we've learned a lot about how information and technology are lost. Let's take a look at the final case file on the timeline.

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

**Contact: August**  
**Targeted by: Solicitation/Joint Venture**

Scenario: A cleared defense contractor that develops aeronautical technology was approached by a foreign university looking to place graduate students in internships. The university eventually convinced the contractor that sponsoring an internship program would be to the mutual benefit of both parties. The resultant internship program allowed interns from the foreign university unrestricted access to the contractor's facilities and systems.

Over the course of the two-month program, and unknown to the contractor, the interns were slowly collecting data on all of the contractor's program details and technology. By the end of the program, the interns had collected enough information to replicate the proprietary technology developed by the contractor.

As a result of this loss, the contractor will lose its competitive edge and market standing as companies within the intern's foreign country introduce competing technology and products. The potential consequences to national security and military assets are grave.

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

## Scenario Question

*The defense contractor was the target of solicitation and allowed foreign students unrestricted access to its facility. How would your facility handle such activity? Select all that apply; then review the feedback that follows.*

- a. My facility would be unlikely to sponsor such a program in the first place; we prefer to keep our research and development activities to ourselves.
- b. My facility might be interested in sponsoring an internship program, though we would likely closely restrict the student access.
- c. My facility appreciates that some of the best ideas come from students and universities. If the internship program was a good fit, we'd welcome the opportunity.

## Scenario Question Feedback

Allowing universities and students into your facility can be valuable, but it's very important that the proper measures are put in place to protect your facility's information and technology.

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.

<b>Collection Method: Solicitation and Seeking Employment</b>
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.
<b>Technique</b>
<ul style="list-style-type: none"> <li>• Places foreign personnel in close proximity to cleared personnel</li> <li>• Provides opportunity to build relationships that may be exploited</li> <li>• Places adversary inside facility to collect information on desired technology</li> </ul>
<b>Indicators</b>
<p>Indicators include:</p> <ul style="list-style-type: none"> <li>• Foreign visitors transmit documents written in a foreign language to a foreign embassy or foreign country</li> <li>• Foreign visitors request:                             <ul style="list-style-type: none"> <li>○ Access to the LAN</li> <li>○ Unrestricted facility access</li> <li>○ Company personnel information</li> </ul> </li> </ul>
<b>Countermeasures</b>
<p>The following countermeasures may guard against this collection method:</p> <ul style="list-style-type: none"> <li>• Review all documents being transmitted; use a translator, when necessary</li> <li>• Provide foreign representatives with stand-alone computers</li> <li>• Share the minimum amount of information appropriate to the scope of the</li> </ul>

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](http://www.dss.mil).*

## Investigation Wrap Up

### Timeline update

BREAKING NEWS
<p><i>Our economic spiral continues tonight as additional reports of significant losses in the technology and defense sector continue. Investigators have discovered that several breaches occurred within U.S. defense contractor facilities. Investigations into the American citizens and companies involved are ongoing. Fines and charges may result.</i></p>

What a picture this paints. Each of these cases involved significant losses to individuals, to their companies, and to the country as a whole. 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 cases we reviewed, you can do so by reviewing the adversary files with each scenario.

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

<b>August</b>	<b>Technology lost via solicitation</b>
Now	Economic disaster

## Results

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

Some result in losses that affect a company's ability to compete within its market. Others affect the individuals involved and can result in revocation of security clearance, fines, or even criminal charges. The cumulative effect of these losses affects our nation's economy greatly. These losses translate to hundreds of billions of dollars each year.

The potential impact to national security and our strategic military advantage cannot be overstated. You might see brief mentions of these losses 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 February 2010, Greg Chung, a naturalized U.S. citizen, was convicted of economic espionage.

How did Mr. Chung commit this crime? He was an engineer for a prominent U.S. defense contractor and stole from his employer for more than 30 years. He stole information related to the U.S. space shuttle program, a booster rocket program, and military troop transports, among others.

Chung stored 300,000 pages of sensitive papers in his Southern California home. The information contained in the papers represented more than \$50 million invested by Chung's employer. He amassed \$3 million in personal wealth stealing from his company and his country.

In 2006, the FBI began investigating Mr. Chung. He is currently serving a 15-year prison sentence.

## ***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) Directorate 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.iooss.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.