Student Guide

The Relationship between Counterintelligence and Security

Course Introduction

Opening

It starts with an idea. A team of researchers examines if it's even possible.

If it is, it moves into development. Along the way, it is touched by countless hands and eyes in organizations just like yours. But there are those who seek to do harm. If they succeed, the result is the same—it damages the businesses in the U.S. industrial base, it degrades U.S. assets, and it can cause great harm to our national security.

At times, it seems these threats exist in all corners…as if they are an invisible cloud constantly surrounding us. Yet, in reality, the threats we face are often predictable…and there are actions we can take to mitigate them.

Incorporating counterintelligence into your security program will help you, as a Facility Security Officer, to protect your facility, its valuable assets, and the national security of the United States.

Welcome to The Relationship between Counterintelligence and Security course.

Course Objectives

To successfully complete this course, you will need to demonstrate your ability to carry out the activities listed in the course objectives. Please take a moment to review them.

- Identify the relationship between CI and security
- Identify the role of risk management in a security program
- Identify how to use threat information in your security program
- Recognize the elements of a successful CI program

CI Role in Industrial Security

The FSO and CI

As a Facility Security Officer (FSO) you know you are responsible for protecting sensitive and classified information and technology within your organization. But what does that really mean?

In the past, this involved traditional security measures, like storage containers for classified material, managing personnel security clearances, and periodic vulnerability assessments. But the threat is becoming more complex. So your job needs to involve more now.

While strong physical security is important; most losses, thefts, and compromises of sensitive and classified information and technology do not involve obvious breaches of physical security or information systems security.

Foreign intelligence services and commercial adversaries have devised methods to steal technology that is protected by robust physical security measures. It is essential that you learn how modern adversaries operate… and how to stop them.

A strong understanding of how counterintelligence (CI) fits into security will enable you to do just that. It will give you the tools to understand the threats you face and help you prioritize and then select the best CI and security program measures to protect both your company's valuable assets and the national security of the United States.

Let's take a closer look at counterintelligence.

Why You Need a CI Program

As an FSO, what does CI mean to you?

It is the information you gather and the activities you perform to deter, detect, and mitigate espionage and sabotage.

The purpose of CI is to protect valuable assets from theft and compromise.

As an FSO, having an effective CI program makes your job easier because it provides you the tools to focus your security resources on what you need to protect and how, where, and when you need to protect it.

You can learn more about CI integration in the DSS web-based training course *Integrating Counterintelligence and Threat Awareness in Your Security Program*, available through CDSE's Security, Training, Education and Professionalization Portal (STEPP.)

The DSS Role in CI

Having a CI strategy requires you to understand the sensitive and classified information, technology, and systems that need to be protected within your facility, and the sources and nature of threats to it

The Defense Security Service (DSS) has several resources available that outline threats to cleared industry. The main one is an annual publication, *Targeting U.S. Technologies.*

Each facility also has an assigned a DSS CI Special Agent, formerly referred to as Field CI Specialist (FCIS.) Your CI Special Agent can provide specific, even classified information, about threats to your facility.

Finally, you can always reach out to your facility's Industrial Security Representative, or IS Rep, for assistance.

The *Targeting U.S. Technologies* report consolidates and presents the threat information DSS learned over the past year, organized in various ways—for example, by region, by methods of operation, and by technology.

DSS's ability to provide accurate threat information depends on the information you and others in industry report about the suspicious contacts and activities that your facility and its personnel experience.

Evaluating threats works in a cycle. It might start with a suspicious email or network activity. Maybe there is a foreign ownership, control or interest (FOCI) decision. Or an attempt to elicit information from an employee while traveling abroad…

As an FSO, if you continually provide information and suspicious contact reports to DSS about the threats your facility encounters, DSS will be able to continually provide you with the most current tools and information you need to counter those threats.

Comparing CI and Security

How CI Complements Security

Let's take a look at how CI and security relate to one another.

By taking different approaches, they are mutually supportive in protecting critical resources and sensitive information. Where security focuses on establishing and adhering to standards and fixing weaknesses, counterintelligence aims to identify, understand, and counter adversary collection efforts.

While security works to reduce *vulnerability*, counterintelligence works to prevent, detect, and respond to *threat*. Security looks *inside* an organization, while counterintelligence looks *outward*, examining things from the adversary's perspective.

As an FSO, you need to help your organization develop strong practices in both security *and* counterintelligence because, as you can see, they complement one another to combat the threats it may face.

	Security	Counterintelligence
Focus	Establish/adhere to standards; fix system weaknesses …rule driven	Identify/understand/counter adversary collection efforts …mission driven
Objective	Deny/prevent unauthorized access… reduce "vulnerability"	Deter/detect/mitigate adversary collection... reduce or mitigate "threat"
Perspective	Internal perspective…looking "inside-out"	Adversary's perspective… looking "outside-in"

Security and CI Activities

As an FSO, you should be well aware of your security responsibilities and the related security activities you engage in every day.

In addition to these activities, to ensure your facility and its sensitive information and technology are as secure as possible, you also need to include CI activities into your routine.

Examples of CI activities include identifying and prioritizing what needs protection; assessing risk, threat, and vulnerability; sharing CI information and collaborating with the appropriate personnel; and promoting CI training and awareness by giving briefings, sharing materials, and talking to employees inside your facility about CI to ensure they are aware of the foreign and insider threats and their requirement to report CI concerns.

Other examples of FSO CI activities include establishing an insider threat program; collecting information about suspicious contacts and filing Suspicious Contact Reports (SCRs) with DSS; providing cyber notifications; and conducting foreign travel briefings and debriefings for employees who travel.

Incorporating CI into Security

How CI Helps Manage Risk

When you weave CI into your security program, you are improving your facility's ability to manage risk. Taking a CI perspective will help you consider your assets and identify the threats to them—that is, adversaries' attempts to steal protected information and technology from your facility and its personnel.

As you learned, a good start for you to obtain threat information is the DSS publication *Targeting U.S. Technologies*, and your DSS CI Special Agent. Other sources of threat information include DoD Intelligence, local law enforcement agencies, the FBI, the Department of State, as well as any other federal Counterintelligence or Law Enforcement service. Your DSS CI Special Agent can help you identify which ones are best able to assist with your specific facility.

Always remember to look internally as well. Sometimes the insider threat comes from disgruntled employees due to management decisions, business practices, or harsh supervisory practices.

In addition to examining threats, you will also analyze your vulnerabilities—the gaps or weaknesses in your facility's security barrier that an adversary may exploit; and you will examine the risk by considering the potential consequences of an adversary's theft—in other words, the damage to the U.S. government and your

organization; and value, or the benefit to the adversary of acquiring the protected information and technology.

A clear risk assessment will help you identify the right tools and activities—that is, countermeasures—you can use to best effectively counter the threats to your facility.

It is important to keep in mind that risk management is an iterative and continuous process. You need to keep looking at threats to see if new ones emerge. You need to continually reevaluate your vulnerabilities and the consequences of loss or compromise. As any of these, so might the countermeasures you choose to employ.

Elements of a Successful CI Program

When building a CI program, there are several elements that you need to consider and include.

In order for it to be successful, the program must have senior leadership support.

Employee awareness is central to a successful CI program.

An effective reporting process ensures that DSS is aware of and can help you with issues you may face.

Your organization must also be vigilant of cyber threats situational awareness

and have programs in place to address both foreign travel and foreign visitors.

The program must also take into account any special programs requiring protection, for example, Special Access Programs or critical program information.

Finally, a strong and continuously integrated insider threat program is essential.

The foundation of your CI program will rely on a risk-based approach and working with DSS and other resources available to assist you.

NOTE: The information in the box below will not be on the test, but is included here as additional information that may provide useful background and insight.

Senior Leadership Support

Senior leadership includes, but is not limited to, the following positions:

- Chief Executive Officer
- Chief Financial Officer
- Office of General Counsel
- Office of Information Assurance
- Office of Human Resources, and/or
- Office of Security

Risk-based approach

A successful program adopts a risk-based approach to enhanced CI awareness for programs and personnel most likely to be targeted or vulnerable to foreign/competitor collection efforts. Examples:

- The CI program includes the corporate analysis of suspicious contact reporting and uses it in security education training
- The program administers additional CI training to high-risk and targeted programs and personnel

Work with DSS

DSS has several resources available to you and can help mitigate the threats you face. Work with your Industrial Security (IS) Representative and seek out the resources of DSS. Your IS Rep should coordinate with the DSS Counterintelligence Special Agent for direct CI support. The CI Special Agent has the entire intelligence community and law enforcement services at their disposal to assist in whatever support is necessary.

Employee Awareness

Evidence of a comprehensive CI Awareness program includes:

- Verified completion of a current and relevant CI awareness briefing (including initial training, refresher training, and termination). Examples of DSS web-based courses :
    - *Thwarting the Enemy*
    - *Insider Threat Awareness*
    - *Counterintelligence Awareness and Reporting*
- Employees who can describe the threats foreign sponsored entities or competitors pose to their CDC or technology
- Employees who can describe their reporting requirements, including what they should report, to whom, and the urgency of reporting
- A company-wide CI Best Practices Program
- Reporting by employees about suspicious contacts or questionable coworker behavior

Cyber Threats Situational Awareness

The cyber threat is the fastest growing method of operation for adversaries. Work with your information technology department and DSS to ensure that your organization is adequately protected and can identify suspicious cyber activities when they do occur. Report cyber incidents promptly to DSS.

Effective Reporting Process

An effective and timely reporting process for suspicious contact reporting should not be delayed by corporate policies or procedure. FSO must coordinate in a timely manner with corporate in order to provide reporting in a timely manner.

Characteristics of a successful process include:

- Identifying and reporting requests for classified, export-controlled, or proprietary information from entities who do not have a legitimate reason for the requested information
- Identifying and reporting requests to submit professional papers for a journal, conference, or symposium
- Identifying and reporting foreign nationals soliciting post-doctoral research positions or other research positions
- Reporting by employees about suspicious contacts or questionable coworker behavior
- Recognizing and reporting suspicious network activity on both classified and unclassified systems

Foreign Visit Program

Elements of an effective foreign visit program:

- Pre-Visit: Education program for escorts, briefers, and hosts that educates on responsibilities
- Post-Visit: Debriefing program that solicits responses from escorts, briefers, and hosts on reportable incidents
- Verification of visitors' identities
- Identification and reporting of anomalies related to foreign visits

Ensure your Technology Control Plan (TCP) includes procedures for restrictions of any Foreign Liaison Officers or Long Term Visitors with access to the facility.

Foreign Travel Program

Elements of an effective foreign travel program:

- Pre-Travel: Education program for all travelers that educates on potential threats, reporting responsibilities, and restrictions of information sharing
- Post-Travel: Debriefing program that solicits responses from travelers on reportable incidents
- Identification and reporting of anomalies related to foreign visits

Special/Critical Programs Protection

Elements of effective Special/Critical Programs Protection:

- Program Protection Plan
- Technology Control Plan
- Classification Guide
- Current Threat Assessments
- Additional guidance on DD Form 254, *DoD Contract Security Classification Specification*

Example: An effective CI program must protect Critical Program Information (CPI) as required in contracts, DoDI 5200.39, and DoDI 5240.19.

Insider Threat Program

An effective CI program should integrate CI into a company-wide insider threat program that includes company leadership, information technology, security, human resources, and ethics personnel.

Elements of an effective Insider Threat Program:

- Training for Program Manager and Insider Threat Team members
- Initial and annual insider threat awareness training
- IT system monitoring and auditing program
- Records maintenance
- Existence of and adherence to insider threat reporting procedures
- Existence of an Insider Threat Policy

Review Activities

Review Activity 1

Which of the following are reasons for including counterintelligence into a facility security program?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ A CI perspective helps the facility focus on threats to its sensitive information/technology
- ☐ Including CI allows FSOs to better manage risks to their facilities
- ☐ CI helps a facility prioritize and direct its security efforts

Review Activity 2

When building a CI program, which elements should be included in the program?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Cyber threats situational awareness
- ☐ Effective reporting
- ☐ Employee awareness
- ☐ Foreign travel and foreign visit
- ☐ Special programs protection
- ☐ Insider threat program

Answer Key

Review Activity 1

Which of the following are reasons for including counterintelligence into a facility security program?

- ☑ A CI perspective helps the facility focus on threats to its sensitive information/technology
- ☑ Including CI allows FSOs to better manage risks to their facilities
- ☑ CI helps a facility prioritize and direct its security efforts

Feedback*: It is important to include CI in security programs for all of these reasons.*

Review Activity 2

When building a CI program, which elements should be included in the program?

- ☑ Cyber threats situational awareness
- ☑ Effective reporting
- ☑ Employee awareness
- ☑ Foreign travel and foreign visit
- ☑ Special programs protection
- ☑ Insider threat program

Feedback*: These are all important to include in a CI program.*

Conclusion

Course Conclusion

Congratulations. You have completed the course: The Relationship between Counterintelligence and Security. You should now be able to perform all of the listed activities.

- ✓ Identify the relationship between CI and security
- ✓ Identify the role of risk management in a security program
- ✓ Identify how to use threat information in your security program
- ✓ Recognize the elements of a successful CI program

To receive course credit, you MUST take the course examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.