# Developing a Security Education and Training Program

## Introduction

### Course Overview

Working with classified information carries significant responsibilities. Organizations and individuals who handle classified information are charged with keeping it safe from accidental or intentional compromise.

As an employee responsible for managing a security program, you have a special duty to ensure that every individual in your organization is aware of their responsibilities in safeguarding classified information.

Welcome to the Developing a Security Education and Training Program course. In this course you will learn not only the policy requirements for a security education program, but also some best practices for developing and implementing such a program and a variety of instructional strategies and methods you can use to do so.

### Course Objectives

Here are the course objectives. Take a moment to review them.

Course Objectives:

- State the purpose of a security education and training program.
- Identify security education and training policy requirements for DOD and Industry personnel.
- Describe and define the types of required security briefings for all cleared personnel.
- Identify the various audiences of a security program.
- Discuss the training requirements for Industry and the DOD.
- Identify and define the types of briefings and other training required for specific roles/activities.
- Identify the various types of special briefings and recognize when they are required.
- Identify the characteristics of a successful security education program.
- Identify how each of the components of the ADDIE model help in selecting and developing appropriate instructional methods.
- Identify potential roadblocks to implementing a successful security education program and strategies for overcoming those roadblocks.
- Identify the components and purpose of program evaluation and oversight.

**Course Structure**

This course is organized into the lessons listed here.

Lessons:

- Course Introduction
- Introduction to Security Education and Training Requirements
- Basic Security Briefing Requirements
- Special Briefings and Other Training
- Developing an Effective Security Education Program
- Course Conclusion

## Lesson 2 Introduction to Security Education and Training

### Objectives

Because protecting classified information and Controlled Unclassified Information, (CUI), from improper disclosure is so critical, there are specific policies and procedures requiring education and training of personnel who have access to or may come in contact with classified information or CUI.

Here are the lesson objectives. Take a moment to review them.

- State the purpose of a security education and training program
- Identify security education and training policy requirements for Industry and DOD personnel

### The Importance of Security Education

What do all these people have in common? They were all American citizens with authorized access to classified and/or controlled unclassified information and were arrested for espionage. They worked in offices and facilities just like yours. Internal traitors exploit weaknesses in the safeguarding practices designed to protect classified information.

It is only when all employees are vigilant and aware that these spies can be caught early before they cause irreparable damage to national security. This is why security education and training are so important. As a security educator, you must ensure that employees are aware of their obligations to protect classified information and CUI, the policies they must follow to do so, and the threats that exist all around them, so as to prevent future security breaches.

Who might the next spy be? Your office mates? One of your friends? Someone in your family?

Ahmed Fathy Mehalba, Arabic Translator at Guantanamo Bay - Exploited lax physical security practices at Guantanamo Bay by copying and removing 386 classified documents from the facility, which did not regularly perform bag or computer searches.

The importance of security awareness and vigilance on the part of personnel cannot be overemphasized. It helps to detect internal and external threats and vulnerabilities, ultimately assisting in preventing security breaches.

## What Is Security Education?

In order to develop an effective security education and training program, it is essential to have a strong understanding of what security education is and what it should achieve. There are, of course, regulatory requirements that outline what must be covered in such a program, and we will cover those requirements throughout this course. But it is also a valuable exercise for individuals responsible for providing security education and training to reflect on its purpose.

Security education is any activity undertaken to ensure that people have the skills, knowledge, and information to enable quality performance of security functions and responsibilities, understand security program policies and requirements, and maintain continued awareness of security requirements and intelligence threats.

An effective security education and training program enables cleared personnel to protect classified national security information and meet their security responsibilities. The success of such a program depends on four components: training, which instructs personnel in their specific security responsibilities; education, which informs personnel about underlying rationale and the importance of those responsibilities; and awareness, which ensures personnel remain continuously alert to security threats and vulnerabilities. Underlying all these components is motivation, or what instills in personnel a desire and commitment to be proactive in the execution of their security responsibilities.

Security Education and Training:

- Enables quality performance of security functions and responsibilities
- Provides understanding of security program policies and requirements
- Ensures awareness of security requirements and intelligence threats
- Establishes, enhances, and maintains quality security

**Basic Elements Pop-up:**

Basic Elements - TEAM Model suggested by Carl A. Roper, Joseph A. Grau, and Dr. Lynn F. Fischer in their book, Security Education, Awareness and Training.

**Goals Pop-up:**

The goals of a security education and training program are many. The most important outcome of effective security education is that it safeguards national security and protects the warfighter by improving the quality of the security program. More specifically, security education and training make personnel aware of their responsibilities and of the penalties and consequences of noncompliance.

Security education should also communicate threats to classified and sensitive information, promote security best practices and security awareness and provide guidance on how to apply security requirements. Perhaps most overlooked, a truly successful security education program will also attempt to dispel any negative attitudes and debunk any myths personnel hold regarding security requirements.

Major Goals of Security Education and Training:

- Safeguard national security
- Protect the warfighter
- Improve the quality of security programs
- Inform personnel of their security responsibilities and promote quality performance
- Inform personnel of the penalties and consequences of noncompliance
- Communicate threats to classified and sensitive information
- Promote security best practices
- Promote security awareness
- Provide guidance on how to apply security requirements
- Dispel negative attitudes and perceptions

**Nondisclosure of Classified Information**

The overarching legal requirement for security education appears in three executive orders: Executive Order 13526, which prescribes the "uniform system for classifying, safeguarding, and declassifying national security information"; Executive Order 12968, Access to Classified Information, the national level policy that identifies the requirement for Employee Education and Assistance; and Executive Order 12829, upon which the National Industrial Security Program is based. Executive Order 13526 mandates that for individuals to gain access to classified information, they must meet three criteria:

First, the individual must have been granted a security eligibility at the level of classification of the information to be accessed. Second, the individual must sign a Standard Form 312, or SF-312, also known as the Classified Information Nondisclosure Agreement. Third, the individual must have a need-to-know the information. Prior to signing SF-312, the individual must receive a security briefing on the nature and protection of classified information. This briefing may either occur during the individual's initial briefing or upon receiving eligibility, as long as the form is signed prior to access to classified information. The Information Security Oversight Office, (ISOO), provides a Briefing booklet with the information that should be covered in this initial security indoctrination.

**Security Education and Training Requirements**

As you learned, there are three Executive Orders that provide the legal requirement for security education. Executive Order 13526 mandates that every person who receives a favorable determination of eligibility for access receive training on the proper safeguarding of classified information and the sanctions imposed on those who fail to appropriately protect such information.

Additionally, it authorizes the Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, to establish standards for agency security education and training programs. The order also lays out the requirement for agency heads to designate senior agency officials to establish and maintain these programs.

Executive Order 12968, Access to Classified Information, requires that agency heads educate employees about their individual responsibilities for handling classified information and inform them about issues that may affect their eligibility for access to classified information. The Department of Defense has implemented these requirements in DODM 5200.01 Volumes 1 through 3, the DOD Information Security Program, DODI 5200.48, Controlled Unclassified Information (CUI), and DODM 5200.02, the Procedures for the DOD Personnel Security Program (PSP).

Also, Executive Order 12829 mandates special requirements for contractors, as well as in 32 CFR Part 117, National Industrial Security Program Operating Manual, also known as the NISPOM. While the requirements for DOD and Industry are similar, and in many cases identical, some of the terminology is distinct, and there are policy differences. Throughout this course you may assume that requirements apply to both DOD and Industry unless indicated otherwise.

### DOD Requirements Pop-Up

DODM 5200.01, the DOD Information Security Program, which mandates security training for individuals with access to classified information, and DODM 5200.02, the Procedures for the DOD Personnel Security Program (PSP), which includes the security education requirements for DOD personnel, describe the briefings required for DOD personnel who have access to or may come into contact with classified information. Each of these briefings will be discussed in detail later in this course. In addition to the basic briefings listed here, this course will also discuss security briefings required under special circumstances.

Information Security Program:

- Volume 3, Enclosure 5: Security Education and Training
  - Initial Orientation
  - Special Training Requirements
  - Continuing Security Education Training
  - Termination Briefings
  - Program Oversight

Procedures for the DOD Personnel Security Program

- Section 12:1: Security Education
  - Initial Briefings
  - Refresher Briefing
  - Insider Threat Briefing
  - Termination Briefing

### Industry Requirements Pop-up

A signed DD Form 441 is required for any company entering into a contract to provide the U.S. Government with supplies or services affecting national security and requiring access to classified information. The DD Form 441 obligates the contractor to develop and maintain an effective security program in accordance with the NISPOM. The NISPOM describes the security education and training requirements for contractors. Each of these required briefings will be discussed in detail later in this course. In addition to the basic briefings listed here, this course will also discuss security briefings required under special circumstances.

DD Form 441:

- Contractual responsibility to develop an effective security program in accordance with the NISPOM

NISPOM

- Chapter 3: Security Training and Briefings
  - FSO Training
  - Insider Threat Training
  - Government-Provided Briefings
  - Initial Security Briefings
  - Refresher Training
  - Debriefings

**Review Activity 1**

Question (Multiple response)

Which of the following are goals of ongoing security education and training?

Select all that apply.

- ○ Safeguard national security
- ○ Inform personnel of the penalties and consequences of non-compliance
- ○ Prevent personnel from learning of threats to classified information
- ○ Dispel negative attitudes and perceptions regarding security practices
- ○ Provide guidance on how to apply security requirements
- ○ Eliminate the need for formal security briefings

**Answer:** Of the items listed, Safeguarding national security; Dispelling negative attitudes and perceptions regarding security practices; Informing personnel of the penalties and consequences of non-compliance and; Providing guidance on how to apply security requirements are goals of ongoing security education and training.

**Review Activity 2**

Drag and Drop

Match each document to its description.

- ○ DD FORM 441
- ○ NISPOM
- ○ DODM 5200.01 Volumes 1-3
- ○ DODM 5200.02

- Executive Order 12968
- Standard Form SF-312

Descriptions

- Regulation mandating security education for DOD employees
- Contractual agreement establishing Industry's security responsibility
- The manual that includes the security education requirements for Industry
- The form all personnel must sign to access classified information
- Regulation mandating training prior to access to classified information
  The overarching policy that mandates security education

**Answers:**

- DODM 5200.02: Regulation mandating security education for DOD employees
- DD Form 441: Contractual agreement establishing Industry's security responsibility
- NISPOM: The manual that includes the security education requirements for Industry
- SF-312: The form all personnel must sign to access classified information
- DODM 5200.01 Vol 1-3: Regulation mandating training prior to access to classified information
- E.O. 12968: The overarching policy that mandates security education

## Summary

In this lesson, you learned about the purpose and importance of security education. You also learned about the policy documents that mandate security education and the key goals for a security education program.

Security Education and Training:

- Establishes, enhances, and maintains quality security program
- Mandated by E.O. 13526 and E.O. 12968
- Implemented in DODM 5200.01 Vol. 1–3 and DODM 5200.02 for DOD personnel
- Implemented in the NISPOM for Industry through E.O. 12829
- Required prior to signing of SF-312

Key Goals:

- Safeguard national security
- Protect the warfighter
- Improve the quality of security programs
- Communicate threats to classified and sensitive information
- Promote security best practices
- Promote security awareness
- Provide guidance on how to apply security requirements
- Dispel negative attitudes and perceptions

# Lesson 3: Basic Security Briefing Requirements

## Objectives

The DODM 5200.01 Volumes 1 through 3, the DODM 5200.02, and the NISPOM outline several required security briefings: an initial briefing, refresher training and continuing security education, and a termination briefing or debriefing. The main audiences of these briefings, and indeed the security program as a whole, are cleared employees of the DOD and Industry, though certain briefings may also be appropriate for uncleared personnel. The requirements for these briefings are almost identical for the DOD and Industry, but there are some differences that you will learn about in this lesson.

Lesson Objectives:

- Describe and define the types of required security briefings for all cleared personnel
- Identify the various audiences of a security program
- Discuss the training requirements for Industry and the DOD

## What Is the Initial Briefing?

In order for newly cleared personnel to receive access to classified information, they must first receive an initial security briefing and then execute Standard Form 312, the Classified Information Nondisclosure Agreement. The SF-312 briefing may either be included in the initial briefing or upon the individual’s receiving a favorable determination of eligibility for access. If the individual already has an SF-312 recorded in the system of record, it does not need to be executed again.

After the briefing, personnel who sign and execute the SF-312, are granted access to classified information at their authorized access level and on a need-to-know basis. are granted access to classified information at their authorized access level and on a need-to-know basis. Executed SF-312s are then forwarded to the respective repository and entered into the system of record. If an individual refuses to execute the SF-312, action shall be initiated to deny or revoke the individual’s eligibility. An individual MUST sign the SF-312 in order to be granted access to classified information.

All initial briefings must cover basic security roles and responsibilities, provide an overview of the classification system, and discuss the penalties for disclosing classified information to unauthorized individuals. The contents of the initial briefing vary slightly by Refresher and whether it is for DOD or contract employees. Now let's look at the requirements specific to DOD and Industry initial security briefings.

Initial Briefing Contents:

- Covers basic security roles and responsibilities
- Gives overview of classification system
- Discusses penalties for unauthorized disclosure (UD)
- Varies by role and whether DOD or Industry

SF-312 Pop Up:

Standard Form 312, Classified Information Nondisclosure Agreement

## DOD Initial Briefings

The DOD has implemented the requirement for an initial security briefing in the following manuals: in Volume 3 of DODM 5200.01, the DOD Information Security Program, and in DODM 5200.02, Procedures for the DOD Personnel Security Program.

While the requirements laid out in the two manuals are similar in that both discuss the protection of classified information, they focus on different aspects of that important responsibility. The Initial Orientation mandated in the DODM 5200.01, Volume 3 outlines the classification system and establishes the policies that all employees must follow to protect classified information. The Initial Briefing mandated in the DODM 5200.02, on the other hand, focuses more on specific threats to classified information and job-specific actions to protect that information.

### Information Security Initial Orientation:

DODM 5200.01 Volume 3 requires that all personnel in the organization, including DOD civilians, military members, and on-site support contractors, shall receive an initial orientation. The regulation suggests that the initial orientation should include the following: an explanation of security roles and responsibilities, such as the Senior Agency Official and Agency Security Personnel; a discussion of the elements of classifying and declassifying information, including a definition of the levels of classification, the process for declassification, and the procedures for challenging a classification status; and the elements of safeguarding, including proper safeguarding procedures, what constitutes compromise of classified information, and the procedures for transmitting classified information.

The DODM 5200.01, Volume 3 also requires an orientation briefing for personnel who are not eligible for access to classified information as they may inadvertently come into contact with classified information in their normal work environment. The initial briefing for uncleared personnel should include a brief explanation of the classification system and its importance and the steps they should take if they discover unsecured classified information or notice a security vulnerability.

Cleared Personnel:

- Security roles and responsibilities
- Elements of classifying and declassifying information
- Elements of safeguarding

Uncleared Personnel:

- Always a possibility for inadvertent contact with classified information
- Actions to take on discovery of unsecured classified information or a security vulnerability

More:

Security roles and responsibilities include the:

- Senior Agency Official
- Agency Security Personnel
- Agency employees who create or handle classified information
- Point of contact for questions or concerns about security matters

Training should address the security responsibilities of each role and who should be contacted in case of questions.

The initial briefing should discuss elements of classifying and declassifying information, including:

- Definition and importance of classification
- Levels of classification and damage criteria associated with each level
- Classification markings
- General requirements for declassifying information
- Procedures for challenging classification status

The briefing should discuss elements of safeguarding, including:

- Proper procedures
- What constitutes compromise of classified information
- General conditions and restrictions for access to classified information
- Steps to take when standards have been violated
- Steps to take in an emergency evacuation
- Appropriate policies and procedures for transmission of classified information

**Personnel Security Initial Briefing:**

DODM 5200.02 requires training for all individuals cleared for access to classified information, as well as any individuals with duties requiring a trustworthiness determination. This training must include security requirements specific to their particular job, techniques employed by foreign intelligence entities to obtain classified information, employee responsibility for reporting those attempts, the prohibition against disclosure of classified information to unauthorized individuals, the responsibility for continuous evaluation of one's own and others' security activities, and the penalties that may be imposed for security violations.

Topics covered:

- Specific security requirements for particular job
- Techniques employed by foreign intelligence entities
- Employee responsibility to report
- Prohibition against unauthorized disclosure of classified information
- Responsibility for continuous evaluation
- Penalties for security violations

**Industry Initial Briefings:**

Now let's look at initial security briefings for contractor personnel. The NISPOM outlines the required topics that must be included in an initial security briefing prior to employees of a cleared contractor accessing classified information. The topics covered are threat awareness; counterintelligence awareness; an overview of the security classification system; employee reporting obligations and requirements, including insider threat; cybersecurity awareness; and security procedures and duties applicable to the employee's job.

Topics covered:

- Threat awareness
- Counterintelligence awareness
- Classification system
- Reporting obligations and requirements
- Cybersecurity awareness
- Job-specific security procedures

NISPOM: National Industrial Security Program Operating Manual

**Building an Initial Briefing:**

Now that you understand the requirements for initial security briefings, let's talk a little about how you can build your own briefings. As you learned, all initial briefings, whether for DOD or contract employees, should include content on threat awareness, counterintelligence awareness, how information is classified and how it must be protected, requirements for continuous evaluation and reporting, cybersecurity awareness, and job-specific security requirements.

**Threat Awareness**

The threat awareness portion of the briefing should inform employees of techniques employed by foreign intelligence entities to obtain classified information. Most of these techniques are well-known and their use is predictable. You may wish to begin with an overview of the history of espionage and foreign intelligence threats to U.S. national security. Every briefing should cover new threats. Discuss examples of famous espionage cases in which classified information was compromised— such as the cases of Aldrich Ames of the CIA; Christopher Boyce, a contract employee; John Walker of the Navy; the FBI's Robert Hanssen; and others and identify targeted information and technology to help increase employee awareness.

It is also important to provide resources where employees can find information on current threats and techniques on countering those threats. DOD personnel may receive information on current threats and techniques from their supporting counterintelligence activity FSOs may want to review the material available under the Counterintelligence section of the Defense Counterintelligence and Security Agency (DCSA) website. The articles and publications posted provide information that can be used to educate and motivate cleared employees.

More: In addition to the DCSA website, you may wish to access some of the following resources:

- Military CI office: DCSA Counterintelligence (CI) professionals and CI Special Agents (or CISAs) work closely with military CI components and other agencies in an effort to help you recognize potential threats.
- Local Federal Bureau of Investigation (FBI): Contact your local FBI office and arrange to sponsor or participate in an Awareness of National Security Issues and Response, or ANSIR, briefing, or a Domain Initiative and Infraguard briefing.
- Defense Intelligence Agency (DIA)
- Department of State (DoS)
- Immigration and Custom Enforcement (ICE)
- For Industry: DCSA Industrial Security Rep (ISR): Request assistance in obtaining threat information that is relevant and available for your company. If you have employees stationed or traveling overseas, or working with a specific country, contact your ISR for information on that country.

DCSA CISA: Defense Counterintelligence and Security Agency Counterintelligence Special Agent

CI: Counterintelligence

### Counterintelligence Awareness

The next topic included in the initial security briefing is counterintelligence awareness. The primary counterintelligence awareness tools are employee vigilance and awareness of threats. Cleared employees should be made aware that they may be targeted by foreign intelligence entities and must be sure to have the proper authority to release information to foreign nationals, if so required, prior to allowing them access.

Perhaps even more dangerous than external perpetrators of espionage are internal employees who have been compromised. There are several common warning signs of an insider threat, of which all employees should be aware. They include attempts to gain access to classified information without a valid need-to-know or without the required security eligibility, unauthorized reproduction or removal of classified material from the work area and deliberate destruction of documents, unexplained affluence, and foreign travel on a regular basis and without sufficient explanation.

Topics:

- Employees must be:
    - Aware of the danger of espionage
    - Cautious when in contact with foreign nationals
    - Vigilant to internal and external threats
- Warning signs:
    - Attempts to gain unauthorized access to classified or sensitive information

- Unauthorized reproduction or removal of classified material
- Unexplained affluence
- Foreign travel without sufficient explanation

### Classification System

All employees must have a thorough understanding of the security classification system. The initial briefing should cover the difference between original and derivative classification, the three levels of classified information, the procedures for classifying and marking information, the importance of having and maintaining a system of control measures to ensure that classified information is available only to authorized individuals, the importance of appropriate controls and safeguards to protect classified information, prohibitions against the improper use of classified information and the abuse of the classification system, and procedures for challenging classification decisions. In addition, the initial briefing should also cover what Controlled Unclassified Information (CUI) is and the importance of protecting it.

Security Classification System Overview:

- Original vs. derivative classification
- Classification levels
- Proper classification and marking
- Maintaining a system of control measures, such as an information management system (IMS)
- Control safeguards
- Prohibitions against improper use and abuse of classification system
- Procedures for challenging classification decisions
- Importance of protecting CUI

CUI: Controlled Unclassified Information- As defined in the 32 CFR 2002.4(h), CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. In accordance with DODI 5200.48, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

### Continuous Evaluation and Reporting

Any security program is based to a large extent on individual trust and responsibility, and employee evaluation and reporting requirements are critical elements in the program. As part of the initial briefing, you must inform employees of their individual responsibility for continuous evaluation, or CE, and reporting.

Employees must understand the nature of reporting requirements and know that reporting, whether regarding oneself or others, is designed to protect the employee, in addition to countering possible foreign intelligence threats. In addition, the briefing should cover the roles and responsibilities in CE and the types of required reports.

Topics:

- Make sure employees understand the nature of continuous evaluation and reporting requirements:
  - Self-reporting
  - Reporting on others
- Goal: to protect the employee and counter possible intelligence threats
- Roles and responsibilities in continuous evaluation
- Types of required reports

More: Continuous evaluation (CE) is the uninterrupted assessment of an individual for retention of their security eligibility and involves reinvestigation at given intervals. To maintain eligibility, employees must recognize and avoid behaviors that might jeopardize that eligibility. Employees, coworkers, supervisors, and managers all play an important role in the continuous evaluation program, and all must receive training on their responsibilities.

- Management (includes Commanders and Heads of DOD Components) must ensure that personnel are indoctrinated and receive continual instruction on the national security implications of their duties.
- Supervisors should receive guidance on how to recognize matters of personnel security concern related to employees who report to them.
- Individuals must be familiar with the security regulations that pertain to their assigned duties and of the standards of conduct required of persons holding positions of trust.
- Coworkers must advise supervisors or security officers when they become aware of information of security significance regarding an individual with access to classified information.

More: Cleared employees are required to report any information pertaining to the following:

- Any suspicious contacts, including:
  - Travel to or through a foreign country or attendance at international conferences at which representatives of such a country will be in attendance
  - Establishment of residency in a foreign country by an employee's spouse or member of his/her immediate family, or the acquisition of relatives, through marriage, who live in such a country
  - Any association with or intention to represent a foreign interest
  - Any instances in which someone approaches you and requests information pertaining to classified or sensitive information when such person does not have a legitimate "need-to-know" and/or is willing to "pay" you for such information
  - Sabotage, espionage, and any subversive or suspicious activity
- Any security violations or infractions or any problem with security-related equipment or procedures, including:

  - Any loss, compromise, or suspected compromise of classified information in your possession or in the possession of another person
  - Receipt of classified material not related to a classified contract, project, or program for which no safeguarding or disposition instructions have been received
  - Any instances in which classified material is out of the control of the custodian or which cannot be readily located
- Any adverse information related to oneself or another cleared individual to include information on: alcohol and drug abuse, criminal activity, relationships/friendships with foreign nationals, mental health problems, or financial difficulties, financial irresponsibility, or unexplained affluence
- Change in name, residence, or marital status
- Any instances, in which an employee desires not to perform on classified work, declines to accept security responsibility, or requests to terminate eligibility or eligibility processing

### Cybersecurity Awareness

The Cybersecurity portion of the briefing should include the definition of cybersecurity, explain that it is authorized for all information system users, and covers some of the "dos" and "don’ts" of cybersecurity. Cybersecurity training and awareness products developed by DISA will be used to meet the baseline user awareness training.

Topics:

- Define cybersecurity
- Authorized for all information system users
- Dos" and "don’ts" of cybersecurity

### Job-Specific Security Responsibilities

The last topic that needs to be covered in the initial briefing are job-specific security procedures and duties. These are security responsibilities that are tailored to specific job roles. For example, an administrative specialist would have very different concerns in protecting classified information than would an engineer.

For an engineer, you might stress procedures regarding scientific meetings where representatives of foreign countries will attend and the procedures pertaining to working papers. Remember that this briefing should be as specific and thorough as you can make it, with as much hands-on demonstration of security procedures as possible.

Job-Specific Security Responsibilities:

- Tailored to specific job roles

### Refresher Training & Continuing Education

The DODM 5200.01,Volume 3, DODM 5200.02, and the NISPOM all mandate that all cleared personnel attend refresher training at least annually. Refresher training must reinforce the information covered in the initial briefing and in any specialized training including security policies, principles, and procedures, and penalties for engaging in espionage and other security violations. This training must address new threats and foreign intelligence techniques and discuss any changes in security regulations. It should also address any issues or concerns identified during security inspections and self-inspections. The content and format of refresher briefings should be tailored to meet the needs of the audience of experienced personnel.

In addition to annual refresher training, the DODM 5200.01, Volume 3 requires continuous and ongoing education for all cleared personnel. This continuing education should supplement periodic briefings, training sessions, and formal presentations and may take the form of informational and promotional efforts or job performance aids. Maintaining records of attendance at refresher training sessions allows you to keep track of who has received the training. These records must include the topics covered in the session and the names of all attendees.

Refresher Training:

- Performed at least annually
- Reinforce contents of initial briefing, including:
  - Policies, principles, and procedures
  - Penalties for engaging in espionage
- Address new threats and techniques and changes in security regulations
- Address issues or concerns identified during self-inspections
- Tailored to meet the needs of experienced personnel

Continuing Education:

- Supplement formal briefings
- Informational and promotional efforts
- Job performance aids

More: Refresher training methods may include:

- Group briefings
- Interactive videos
- Training sessions
- Online courses
- Job performance aids
- Promotional efforts
- Bulletins
- Newsletters
- Security awareness meetings

## Termination Briefings and Debriefings

The DODM 5200.01, Volume 3; DODM 5200.02; and the NISPOM all mandate termination briefings when an employee terminates employment or is discharged, and when an employee's access is terminated, suspended, or revoked. The NISPOM, which refers to these as debriefings, also requires a debriefing upon termination of a company's facility clearance, or FCL.

The termination briefing should cover the individual's continued responsibility to protect classified information, the continuing requirement for the individual to report attempts by unauthorized individuals to gain access to classified information, the prohibition against retaining classified materials, and the civil and criminal penalties for violating security regulations and disclosing classified information.

The DODM 5200.02 states that the termination briefing should be followed by the execution of a Security Termination Statement, or STS. When an individual refuses to execute an STS, every effort will be made to debrief the individual orally. An employee's refusal to sign the STS must be reported immediately to the security manager of the cognizant organization, to the supporting adjudication facility, and recorded in the system of record.

As a best practice, the STS should be retained by the DOD component for at least two years after employee termination. The individual must be orally debriefed if the individual refuses to sign the STS. If the individual is unwilling to participate, preventing the Security Manager or FSO from completing an oral debriefing, the documentation regarding the attempted oral debriefing must be maintained for two years. For more information review CDSE's Termination Briefing Short available on the CDSE website.

Termination Briefings:

- Debrief employees when:
  - Employee terminates employment or is discharged
  - Employee's access is terminated, suspended, or revoked
  - NISP only: company's facility clearance (FCL) is terminated
- Cover:
  - Continued responsibility to protect classified information
  - Requirement to report unauthorized attempts to gain access
  - Prohibition against retaining materials
  - Civil and criminal penalties for violations
- Security Termination Statement (General Services Administration Form 3162)
  - Refusal to sign reported to security manager
- Orally debrief if employee refuses to sign Form 3162
  - Maintain documentation regarding the failed oral debriefing attempt for two years

## Basic Briefings Job Aid

Take a moment to scroll through this job aid, which outlines information about basic required briefings.

| BASIC BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| **Initial Briefing** | NISPOM | Topics:<br>• Threat awareness<br>• Counterintelligence awareness<br>• Overview of the security classification system<br>• Reporting obligations and requirements to include insider threat<br>• Cybersecurity training<br>• Security procedures and duties applicable to employee's job | Industry |
| **Information Security Initial Orientation** | DODM 5200.01, Vol. 1–3 | **Focus:** Classification system<br>• Cleared Personnel<br>o Roles and responsibilities<br>o Elements of classifying and declassifying information<br>o Elements of safeguarding<br>• Uncleared Personnel<br>o May come into inadvertent contact with classified information<br>o Actions to take on discovery of unsecured classified information or a security vulnerability | DOD |
| **Personnel Security Initial Briefing** | DODM 5200.02 12.1.c. | **Focus:** Threats to classified information and job-specific actions to protect information<br>• Specific security requirements for particular job<br>• Employee responsibility to report<br>• Techniques employed by foreign intelligence entities<br>• Prohibition against unauthorized disclosure of classified information<br>• Responsibility for continuous evaluation<br>• Penalties for security violations | DOD |

| | | | |
|---|---|---|---|
| **Threat Awareness** | DODM 5200.02<br>NISPOM | **Topics**<br>• Define foreign intelligence threat and identify espionage techniques<br>• Provide historical overview<br>• Discuss new threats<br>• Provide examples of famous espionage cases where classified information was compromised<br>• Identify targeted information or technologies<br>• Sources on current threat information | DOD and Industry |
| **Counter-intelligence Awareness** | DODM 5200.02<br>NISPOM | **Topics**<br>• Employees must be:<br>o Aware of the danger of espionage<br>o Cautious when in contact with foreign nationals<br>o Vigilant to internal and external threats<br>• Warning signs:<br>o Attempts to gain unauthorized access to classified or sensitive information<br>o Unauthorized reproduction or removal of classified material<br>o Unexplained affluence<br>o Unreported foreign travel | DOD and Industry |
| **Continuous Evaluation and Reporting Obligations** | DODM 5200.02<br>NISPOM | **Topics**<br>• Make sure employees understand the nature of continuous evaluation and reporting requirements<br>o Self-reporting<br>o Reporting on others<br>• Goal: To protect the employee and counter possible intelligence threats<br>• Roles and responsibilities in continuous evaluation<br>• Types of required reports<br>o Suspicious contacts<br>o Security violations or infractions<br>o Adverse information<br>o Change in employee status<br>o Sabotage, espionage, and any subversive or suspicious activity | DOD and Industry |

| | | | |
|---|---|---|---|
| **Job-Specific Security Procedures** | DODM 5200.02<br>NISPOM | Tailored to specific job roles | DOD and Industry |
| **Refresher Training** | DODM 5200.01, Vol. 1–3<br>NISPOM | Performed at least annually<br>**Topics**<br>• Reinforce contents of initial briefing, including:<br>o Policies, principles, and procedures<br>o Penalties for engaging in espionage<br>• Address new threats and techniques and changes in security regulations<br>• Address issues or concerns identified during self-inspections<br>• Tailored to meet the needs of experienced personnel | DOD and Industry |
| **Termination Briefing/ Debriefing** | DODM 5200.01, Vol. 1–3<br>NISPOM | **Performed when:**<br>• Employee terminates employment or is discharged<br>• Employee's access is terminated, suspended, or revoked<br>• **NISP only**: Company's facility clearance (FCL) is terminated<br>**Topics**<br>• Continued responsibility to protect classified information<br>• Requirement to report unauthorized attempts to gain access<br>• Prohibition against retaining materials<br>• Civil and criminal penalties for violations | DOD and Industry |

**Review Activity 1**

Question (Multiple choice single response)

What should the Initial Briefing include for "Uncleared" personnel?

- ○ An explanation of the targeted information or technologies
- ○ An explanation of the classification system and its importance
- ○ An explanation of the steps that should be taken if unsecured classified information or a security vulnerability is discovered
- ○ An explanation of specific threats to classified information and job-specific actions to protect that information

**Answer:** The initial briefing for uncleared personnel should include a brief explanation of the classification system and its importance, and the steps they should take if they discover unsecured classified information or notice a security vulnerability.

**Review Activity 2**

Question (Survey true/false )

1. A new SF-312 must be executed and recorded in the system of record each time an individual needs access to classified information.

○ True
○ False

**Answer:** If the individual already has an SF-312 recorded in the system of record, then it does not need to be executed again.

2. Job-specific security procedures are usually included as part of an initial security briefing.

○ True
○ False

**Answer:** Job-specific security procedures are usually included as part of an initial security briefing.

3. Information on current security threats must be included as part of security training.

○ True
○ False

**Answer:** Information on current security threats must be included as part of security training.

4. Termination briefings should communicate the continued requirement for individuals to protect classified information, even after resigning or being discharged.

- o True
- o False

**Answer:** Termination briefings should communicate the continued requirement for individuals to protect classified information, even after resigning or being discharged.

5. Refresher training is required only for individuals who have violated security procedures.

- o True
- o False

**Answer:** Refresher training is required for ALL cleared personnel.

**Review Activity 3**

Question (Multiple choice multiple response)

Which of the following are topics that should be included in an initial security briefing?

- o An overview of the security classification system
- o Techniques employed by foreign intelligence entities
- o Prohibition against unauthorized disclosure (UD) of classified information
- o Penalties for security violations

**Answer:** All of these are required elements of an initial security briefing. refresher training,

**Summary**

In this lesson, you learned about the requirements for cleared DOD and Industry personnel to attend initial security briefings, refresher training, and continuing training.

## Lesson 4: Special Briefings and Other Training

### Objectives

In addition to the standard training requirements for all personnel with access to classified information, there are several types of special briefings and other training required under certain circumstances.

They include training for personnel filling special roles, training for personnel working with special programs, and other training, such as briefings for foreign travel and for those with access to foreign government information or automated information systems. Here are the lesson objectives. Take a moment to review them.

Objectives:

- Identify and define the types of briefings and other training required for specific roles/activities
- Identify the various types of special briefings and recognize when they are required

OCA - Original classification authority

### Classification Roles

As you learned in the previous lesson, certain job roles require special security procedures. The DODM 5200.01, Volume 3 specifically identifies special briefing requirements for three different categories of job holders: original classifiers, declassification authorities other than original classifiers, and derivative classifiers, security personnel and others. This last category of job holders can be military, civilian, or contractor personnel.

#### OCA

The DODM 5200.01, Volume 3 mandates that original classification authorities receive security education and training that addresses who is authorized to classify information originally and the standards an original classifier must meet to classify information.

The training must also address the difference between original and derivative classification, the avoidance of over-classification, the process for determining how long information can be classified, the prohibitions and limitations on classifying information, the basic markings that must appear on classified information, the general standards and procedures for declassification, and the requirements and standards for creating, maintaining, and publishing security classification guides. Original classification authority delegation is driven by position, not by name

#### Declassification Authority

Declassification authorities other than original classifiers must receive training addressing the standards, methods, and procedures for declassifying information as mandated by Executive

Order one-three-five-two-six and DODM fifty-two hundred dot zero one. The training must also cover the standards for creating and using declassification guides, the contents of each DOD Component's declassification plan, and the component's responsibilities for the establishment and maintenance of a declassification database. Declassification authorities are always U.S. Government employees or military members who have specifically been given this responsibility.

- Standards, methods, and procedures for declassifying information
- Standards for creating and using declassification guides
- Contents of the Component's declassification plan
- The requirement for each component to maintain a declassification database

**Derivative Classifiers, Security Personnel, and Others**

Derivative classifiers, security managers and specialists, classification management officers, and others with responsibilities relating to the oversight of classified information, must receive training and education on the following topics: the processes for classifying information originally and derivatively, and the standards applicable to each; the avoidance of over-classification; proper and complete classification markings; and the authorities, methods, and process for downgrading and declassifying information.

The training must also cover the methods for the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information, the requirements for creating and updating classification and declassification guides, the requirements for controlling access to classified information, and the procedures for investigating and reporting actual and potential compromises of classified information, and the penalties that may be associated with violations of established security policies and procedures. In addition, these individuals must be briefed on the requirements for oversight of the security classification program, including self-inspections.

Finally, these individuals must receive training on the procedures for the secure use, processing, storage, reproduction, and transmission of classified information on automated information systems and networks. Responsible individuals will also be trained on the required assessment and authorization of these systems.

Training Topics:

- Original vs. Derivative
- Markings
- Downgrading and declassifying
- Storage, reproduction, transmission
- Declassification guides
- Access control
- Investigation and reporting
- Oversight
- Automated information systems

## Job-Specific Training Requirements

In addition to the briefing requirements for individuals involved in the classification and declassification of information, there are special training requirements for DOD security professionals, as identified in DODI 3305.13, for the Facility Security Officer, or FSO, as identified in the NISPOM, and for others with special roles, including the Information System Security Manager and couriers, escorts, and hand-carriers of classified information.

### Security Professionals

DODI 3305.13 identifies additional requirements for security professionals, or any individuals who are educated, trained, and experienced in one or more security disciplines and who provide advice and expertise to senior officials on the implementation, operation, and administration of the organization's security programs.

The responsibility for the establishment and maintenance of the Security Professional Education Development Program is assigned to the Defense Counterintelligence and Security Agency, under the authority of the Under Secretary of Defense for Intelligence and Security. The program consists of a combination of instructor-led, distance learning, blended learning, job aids, and other delivery methods as required to meet mission requirements.

Security Professionals Training:

- As described in DODI 3305.13: DOD Security Training
- Required for individuals responsible for the implementation of security programs
- Established and maintained by the Defense Counterintelligence and Security Agency
- May be conducted in the form of instructor-led, distance learning, blended learning, job aids, and other delivery methods appropriate to mission requirements

### Facility Security Officer

The NISPOM makes Industry responsible for providing training for FSOs, and others performing security duties, with security training as deemed appropriate by the cognizant security agency. Training requirements will be based on the facility's involvement with classified information and should include an FSO orientation and program management courses. FSO training must be completed within one year of FSO appointment.

FSO Training:

- As described in NISPOM Section 117.12(d) and deemed appropriate by cognizant security agency
- Based on facility's involvement with classified information
- May include an FSO Orientation and program management courses
- Received within one year of appointment

NISPOM - National Industrial Security Program Operating Manual

### Information Systems Security Manager

Information systems containing classified and sensitive information are a critical asset in need of protection. Mandated by DOD 8570.01-M, the individuals responsible for managing those systems must receive training at a level commensurate with the complexity of the information system they are responsible for managing.

The DOD refers to these individuals as Information System Security Managers and Officers. This training must communicate the responsibility for providing information system security education for all relevant personnel prior to their use of automated information systems, or AIS.

Training for Information Systems Security Manager (ISSM):

- DODD 8140.01 Cybersecurity Workforce Management
- DOD 8570.01-M, Information Assurance Workforce Improvement Program Downgrading and declassifying
    - Training to level commensurate with IS complexity
    - Responsibility for providing IS security education for relevant personnel prior to their use of  Automated Information System (AIS)

### Courier / Hand-carrier

Courier briefings are provided to cleared personnel, whether U.S. military, government civilians, or DOD contractors, who are couriers for the Defense Courier Service or will be hand-carrying or escorting classified material. During this briefing, the individual will be instructed on procedures for handling classified information while in transit, modes of transportation that may be used, and authorized destinations of classified hand-carried or escorted classified materials.
They will also be informed on points of contact in case of an emergency while performing courier responsibilities. Additional information on this topic is available in the Transmission and Transportation for DOD and the Transmission and Transportation for Industry courses.

Courier Briefing Topics:

- Who is authorized to hand-carry/escort classified information
- Procedures for handling classified information while in transit
- Modes of transportation that may be used
- Where classified information may be carried
- Points of contact in case of an emergency while performing courier responsibilities

Courier - A designated, cleared employee whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

Hand-carrier - A designated, cleared employee who occasionally hand-carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand-carrier except for authorized overnight storage.

Escort - A designated, cleared person who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

## Special Types of Information

Both the DODM 5200.01, Volume 3 and the NISPOM require personnel to receive an indoctrination briefing prior to being granted access to special types of information. For contractors, a U.S. Government representative, usually the DCSA IS Rep, will brief and debrief the FSO. These are considered Government-provided briefings. The FSO then provides briefings to employees prior to them gaining access to the information.

These briefings provide guidance on how to protect these special types of classified information and how to determine who is authorized access to this information. Special types of information include Special Access Program, or SAP; Communications Security, or COMSEC; North Atlantic Treaty Organization, or NATO; Critical Nuclear Weapon Design Information, or CNWDI; and foreign government information, or FGI.

Special briefings are also required for individuals who need access to sensitive compartmented information, or SCI; individuals who need access to information protected by Alternative Compensatory Control Measures, or ACCM; and individuals responsible for Operations Security, or OPSEC.

### Special Access Program

A Special Access Program, or SAP, is any official program or activity as authorized by Executive Order 13526. SAPs employ enhanced security measures, such as safeguarding and access requirements, exceeding those normally required for collateral information at the same level of classification.

Training for those with access to SAPs must be conducted in accordance with DODM 5205.07, Volume 1: DOD SAP Security Manual: General Procedures.

SAP Briefing Topics:

- Any official program or activity employing enhanced security measures
  - Safeguarding
  - Access requirements
- Training conducted in accordance with DODM 5205.07, Volume 1: DOD Special Access Program Security Manual: General Procedures

### COMSEC

COMSEC re-briefings are not required; however, some activities may include them as part of their normal refresher briefing. COMSEC debriefings are not required, unless the employee had access to CRYPTO information, in accordance with NSA/CSS No. 3-16.

And remember, records of all COMSEC briefings and debriefings must be maintained. For contractors with access to COMSEC, the NISPOM sets forth special training requirements.

COMSEC Briefing Topics:

- Mandated by DODI 5205.08, NSA/CSS Policy Memorandum No. 3-16, and DODI 8523.01, Section 4.1 (NSA Net is not publicly accessible)
- Protection of COMSEC
    - Transmission Security
    - Physical Security
    - Emission Security
    - Cryptographic Security
- Special safeguards for protecting this information
- Directives and rules prescribing those safeguards
- Penalties for willful disclosure of this information to unauthorized persons
- Briefing forms
    - COMSEC
    - CRYPTO
- For Industry

If the employee had access to CRYPTO information, a special debriefing must be held.

More COMSEC: Specific requirements for contractors are laid out in the NISPOM, Section 117.21(e), COMSEC Briefing and Debriefing Requirements. A U.S. Government representative (usually the IS Rep) will brief the FSO, the contractor's COMSEC Custodian, and the COMSEC Alternate on the special sensitivity of information and security requirements, who must in turn brief other contractor employees.

More CRYPTO: In accordance with DODI 5205.08, Access to Classified Cryptographic Information, and NSA/CSS Policy Memorandum No. 3-16, Control of COMSEC Material, employees with access to CRYPTO information must:

- Receive a special debriefing
- Execute Section II of Secretary of Defense (SD) Form 572 (Cryptographic Access Certification and Termination) when access is no longer required

COMSEC - Communications Security (COMSEC) is the general term used for all protective measures taken to deny unauthorized access to information derived from telecommunications of the U.S. Government relating to National Security and to ensure the authenticity of such communications.

CRYPTO - CRYPTO is a marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information (per Committee on National Security Systems Instruction (CNSSI) No 4009, Committee on National IA Security System Glossary).

## NATO Information

DODD 5100.55, the United States Security Authority for North Atlantic Treaty Organization Affairs, or USSAN, requires that NATO briefings be provided to personnel who have a valid need to work with NATO classified information.

Access to NATO classified information requires a security clearance at the same classification level as the NATO information to be accessed. Information designated as NATO RESTRICTED does not require a security clearance. The NATO briefing will cover security requirements for handling classified NATO information and the consequences of negligent handling of this information.

Employees must complete a statement acknowledging receipt of the NATO indoctrination briefing and their responsibility for safeguarding NATO information. For contractors, annual refresher briefings are required to reinforce the importance of proper handling and protection of classified NATO information.

When access to NATO information is no longer required, a debriefing is conducted. The debriefing covers the individual's continued responsibility for safeguarding classified NATO information. Records of all briefings, re-briefings, and debriefings must be retained, in accordance with the governing records management system. For contractors with access to NATO information, these special training requirements are found in the NISPOM.

NATO Briefing Topics:

- Mandated by DODD 5100.55
- For those with valid need-to-know NATO information
- "NATO classification markings"
- Handling NATO-classified materials
  - Preparation
  - Reproduction
  - Access
  - Storage
  - Transmission
  - Destruction
- For Industry: NISPOM, Section 117.19(g)(7)

NATO debriefing is required to reinforce ongoing safeguarding responsibilities when access is no longer required.

NATO Information - Classified information that represents military, political, and economic data, circulated with NATO and by NATO, regardless of whether the information originates within the organization itself or is received from a member nation(s).

More:
NATO has the following levels of security classification:

- COSMIC TOP SECRET (CTS)
- NATO SECRET (NS)

- NATO CONFIDENTIAL (NC)
- NATO RESTRICTED (NR)
- ATOMAL information is marked:
  - COSMIC TOP SECRET ATOMAL (CTSA)
  - NATO SECRET ATOMAL (NSA)
  - NATO CONFIDENTIAL ATOMAL (NCA)
- ATOMAL applies to:
  - U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA
  - United Kingdom Atomic information released to NATO

**CNWDI**

Access to Critical Nuclear Weapon Design Information, or CNWDI, is limited to personnel who have a final SECRET or TOP SECRET security eligibility. Prior to access, these personnel must receive a briefing discussing the definition and sensitivity of CNWDI.

The briefing should also cover the regulations laid out in DODI 5210.02, Access to and Dissemination of Restricted Data and Formerly Restricted Data including special CNWDI markings and transmission and other special handling requirements. Upon termination of access, contractor employees must be given an oral debriefing.

Records of all employees authorized to access CNWDI, as well as briefing and debriefing records, must be retained as required. For contractors with access to CNWDI, special training requirements are found in the NISPOM.

CNWDI Briefing Topics:

- Definition and sensitivity of CNWDI
- DODI 5210.02
- Special CNWDI markings
- Transmission and other special handling requirements
- For Industry: NISPOM, Section 117.20(b)

CNWDI: Critical Nuclear Weapons Design Information, CNWDI, is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA that reveals the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition, munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high-explosive materials by type.

**Foreign Government Information**

Employees with access to foreign government information, or FGI, must be briefed on the special handling requirements for FGI. This briefing explains what FGI is and the basic security standards and procedures for safeguarding classified FGI, which are basically equivalent to those for U.S. classified information, although there are some significant differences of which personnel should be made aware.

The biggest distinction that personnel must be aware of when handling FGI are differences in classification markings among various nations. In addition to TOP SECRET, SECRET, and CONFIDENTIAL, many foreign governments have a fourth classification level, known as RESTRICTED, for which there is no U.S. equivalent. The FGI briefing should also cover usage, disclosure, dissemination, and storage guidelines, to ensure that this information is properly protected.

FGI Briefing Topics:

- Definition of FGI
- Basic security standards and procedures
- FGI classification levels
- FGI use and disclosure

FGI - Foreign Government Information

FGI classification levels - A list of classification levels for FGI can be found in DODM 5200.01 Vol. 2, Enclosure 4.

More: As defined by the E.O. 13526, foreign government information (FGI) is:

- Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation [expressed or implied] that the information, the source of the information, or both are to be held in confidence.
- Information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.
- Information received and treated as “foreign government information” under the terms of a predecessor order.

**Sensitive Compartmented Information**

Sensitive Compartmented Information, or SCI, is classified information derived from intelligence sources and requiring special handling. Training for those with access to SCI must be conducted in accordance with DODM 5105.21, Volumes 1 through 3, or the Sensitive Compartmented Information Administrative Security Manual.

SCI Briefing:

- Classified information derived from intelligence sources requiring special handling
- All personnel with access must receive an initial briefing
- In accordance with DODM 5105.21, Vols. 1-3, Sensitive Compartmented Information Administrative Security Manual

SCI - Sensitive Compartmented Information, or classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

### Alternative Compensatory Control Measures (ACCM)

Alternative Compensatory Control Measures, or ACCM, are additional security measures which may be used to ensure strict need-to-know protection when standard security measures are insufficient.

Training on ACCM is required prior to individuals gaining access to ACCM-protected information, and annually thereafter, as described in the DODM 5200.01, Volume 3, Enclosure 2.

ACCM Briefing:

- Additional security measures when standard measures are insufficient for the protection of designated information
- Training required prior to individuals being granted access to ACCM-protected information and annually thereafter, as described in DODM 5200.01 Vol-3, Enclosure 2

### OPSEC

Operations Security, or OPSEC, is a risk management process used to view critical information from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands. Enclosure 7 of the DOD Operations Security (OPSEC) Program Manual, or DOD 5205.02-M, mandates initial and refresher training for individuals with OPSEC responsibilities in order to provide the knowledge and skills necessary to enable quality performance of OPSEC functions.

Awareness training is required for all personnel to include an explanation of OPSEC, its purpose, threat awareness, the organization’s critical information, and the individual’s role in protecting it. Contractors are required to complete OPSEC training when this requirement is included in their contract.

OPSEC Briefing:

- Risk management process used to view critical information from the perspective of an adversary in order to protect sensitive information
- Mandated by DOD 5205.02-M
- Initial and annual refresher training required for employees and contractors assigned OPSEC responsibilities
    - OPSEC Program Managers
    - OPSEC Coordinators
    - Information Operations (IO) Career Force
- Awareness training required for all personnel

## Other Special Briefings

There are several other circumstances requiring special briefings. These include foreign travel, use of automated information systems, antiterrorism, physical security, international programs, and for contractors, procedures surrounding classified visits and meetings.

### Foreign Travel

One type of special security briefing is the foreign travel briefing. Foreign travel briefings are provided to personnel who will be traveling, either officially or unofficially, to foreign countries, professional meetings or conferences where foreign attendance is likely, and any other locations where there are concerns about possible foreign intelligence exploitation. This briefing is usually required for all personnel with SCI or SAP access.

Foreign travel briefings provide important information not only about the potential security risks at a given destination but also, about points of contact if a problem arises. In addition to security warnings, the foreign travel briefings provide valuable information about any applicable safety or criminal issues travelers should be aware of.

The briefing should also cover reporting requirements for any suspicious contact and information on how foreign intelligence entities target and approach cleared personnel. Employees are debriefed upon return as to what occurred during the travel. Records of briefings are maintained in accordance with cognizant security authorities' records management systems. Check with your Component, agency, or local requirements to determine your specific foreign travel briefing policies. Requirements for contractors are laid out in the NISPOM.

Foreign Travel Briefing Topics:

- Security risks at a given destination
- Area awareness
  - Personal protection measures
  - Embassy location
- Applicable safety or criminal issues
- Reporting requirements for suspicious contact
- How foreign intelligence entities target and approach personnel
- For Industry:
  - The NISPOM does not specifically require "Foreign Travel Briefings" each time a cleared contractor leaves the United States, but Section 117.19(f)(4) requires a briefing for employees assigned outside the United States. Specific contracts may include additional briefing requirements. Contractors are required to educate and train their employees on specific duties and threats that they may encounter during their employment, which would include factors related to foreign travel. When contractor employees visit or are assigned to work at a U.S. Government office or U.S. military installation abroad, they may receive security, threat-awareness, and antiterrorism training from their host.

### Cybersecurity

Cybersecurity is the protection of computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. All users who have access to government computer systems must complete a cybersecurity briefing, in which they are informed of their responsibility for protecting the system to prevent any unauthorized disclosure, modification or destruction of information, as well as the prohibition against introduction, removal, or duplication of hardware, software, or media to or from any information technology system without authorization.

In this briefing, personnel also learn the requirements for password and pass-phrase security. Personnel are required to participate in annual refresher training that covers identification of threats to and the physical protection of information systems, as well as providing a basic understanding of malicious content and logic and non-standard threats, such as social engineering. Contractor employees must also be trained in accordance with the approved System Security Plan if they have access to an information system approved for processing classified information

Cybersecurity Briefing:

- Cybersecurity = Protection of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks
- All AIS users must comply with:
  - All security measures to protect information
  - Regulations concerning hardware, software, or portable media
  - Password and pass-phrase security
- Personnel must participate in annual cybersecurity training:
  - Threat identification
  - Physical security
  - Malicious content and logic
  - Social engineering and other non-standard threats
- Mandated by DODI 8500.01 and the NISPOM

AIS - Automated Information System

### Antiterrorism

Antiterrorism, or AT, refers to defensive measures used to reduce the vulnerability of individuals and property to terrorist attacks, including limited response and containment by local military and civilian forces. AT also includes actions taken to prevent or mitigate hostile actions against DOD personnel and their families, resources, facilities, and critical information.

There are specific training requirements for personnel who are responsible for managing AT programs. AT training is required for individuals, commanders, senior executive officers, high-risk personnel, those assigned to high-risk billets, and units preparing to deploy. There are four levels of AT training: level one training is for AT awareness; level two is for antiterrorism officers, or ATOs; level three is pre-command AT training; and level four is an executive seminar. Antiterrorism Officer Training Level II is available online from the CDSE website. See your component for specific ATO training requirements.

What Is AT?

- Defensive measures used to reduce vulnerability to terrorist acts
- Actions taken to prevent or mitigate hostile actions against DOD personnel, resources, facilities, and critical information

AT Briefing Levels:

1. Antiterrorism awareness
2. Antiterrorism officers (ATOs)
3. Pre-command antiterrorism training
4. Executive seminar

**Physical Security**

DOD 5200.08-R, the Physical Security Program, mandates the creation of physical security awareness training for DOD personnel, as a part of physical security planning. This awareness training must be sustained and delivered regularly.
This training should cover common physical security measures as part of security-in-depth, to include perimeter fences, employee and visitor access controls, badges/Common Access Cards, intrusion detection systems, random guard patrols, prohibited item controls, entry and exit inspections, escorting, and closed-circuit video monitoring.

Physical Security Briefing:

- DOD 5200.08-R mandates that physical security awareness training for DOD personnel be created and sustained
- Training should cover physical security measures, focused on security-in-depth:
  - Perimeter fences
  - Employee and visitor access controls
  - Badges/Common Access Cards (CAC)
  - Intrusion Detection Systems (IDS)
  - Random guard patrols
  - Prohibited item controls
  - Entry/exit inspections
  - Escorting
  - Closed-circuit video monitoring

**International Programs**

Special briefings are also required for individuals who require access to international programs or who participate in international activities. These individuals must receive training on international security and foreign disclosure guidelines by taking either the

International Security Requirements course offered by Under Secretary of Defense for Policy (USD(P)), the International Programs Security and Technology Transfer course offered by the Defense Systems Management college, or an equivalent course offered by the DOD Component.

Applicable activities covered in this training included security assistance, cooperative research, foreign disclosure, and specific country relationships. Contractor employees involved in international programs must be trained commensurate with their particular duties and the provisions of their company's Technology Control Plan.

International Programs Briefing:

- Training in International Security and Foreign Disclosure Support
- Courses:
  - International Security Requirements
  - International Programs Security and Technology Transfer
  - DOD Component equivalent course
- Topics include:
  - Cooperative research
  - Foreign disclosure
  - Country relationships

### Visits and Meetings

When cleared individuals visit a cleared contractor or government facility and need access to classified information, visitors must be trained on the security procedures they are expected to follow. This security briefing typically addresses the facility's badging and escort policy, as well as physical security procedures and access areas. It will also discuss use of portable electronic devices, or PEDs, such as cell phones, laptops, and video- and audio-recording devices.

The briefing may also address how to verify another person's personnel security eligibility, how to handle classified documents, and how to transmit and/or transport classified material. This is especially relevant to long-term visitors who are typically co-located at the host facility to work on a contract. Finally, the security briefing may cover the reporting requirements for security incidents, such as loss or compromise of classified material. Heads of DOD Components shall establish procedures to accommodate visitors to their Component facilities in accordance with DODM 5200.01, Volume 3, Enclosure 2.

Additionally, contractors working in a DOD facility are considered long-term visitors in accordance with the NISPOM and are subject to government security education and training requirements as defined in their contract and the DD Form 254, Contract Security Classification Specification.

Security Briefing Topics:

- Badges and escorts
- Physical security procedures

- Access areas
- Use of PEDs
- Verifying PCL
- Handling classified material
- Transmitting and/or transporting classified information
- Reporting requirements for security incidents

Contractors at Government Facilities:

- Considered long-term visitors in accordance with the NISPOM
- Subject to government security education and training requirements

PED - Portable electronic device

PCL - Personnel Clearance

### Nondisclosure Briefings

A common special briefing that was discussed earlier in this course is the SF-312 Nondisclosure briefing which is required for all cleared personnel.

**Prior to signing the SF-312, the individual must receive a security briefing on the nature and** protection of classified information. The Information Security Oversight Office, or ISOO, provides a Briefing booklet with all the information that should be covered in this initial security indoctrination.

The SF-312 briefing may be conducted either as part of an initial briefing, or as a separate briefing, when the individual is granted clearance or access to the classified information.

SF-312 - Standard Form 312, “Classified Information Nondisclosure Agreement”

### Special Briefings Job Aid

A common special briefing that was discussed earlier in this course is the SF-312 Nondisclosure Take a moment to scroll through this job aid, which outlines information about required special briefings.

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| **ACCM** | DODM 5200.01, Vol. 3<br>NISPOM | ACCM stands for Alternative Compensatory Control Measures. These are additional security measures which may be used to ensure strict need-to-know protection when standard security measures are insufficient. | DOD and Industry (If identified in the DD 254) |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | | **Training** is required prior to individuals being granted access to ACCM-protected information. | |
| **AT** | DODI O-2000.16 Vol.1 and 2 | Antiterrorism (AT) is a defensive measure used to reduce vulnerability to terrorist acts, as well as actions taken to prevent or mitigate hostile actions against DOD personnel, resources, facilities, and critical information.<br>**Training**<br>• Antiterrorism awareness<br>• Antiterrorism officers (ATOs)<br>• Pre-command antiterrorism training<br>• Executive seminar | DOD and Industry |
| **CNWDI** | DODI 5210.02,<br>NISPOM, Section 117.20(b) | The abbreviation CNWDI (pronounced SIN-widdy) stands for "Critical Nuclear Weapons Design Information."<br>**Briefings**<br>• Definition of CNWDI<br>• Reminder of the extreme sensitivity of CNWDI<br>• Responsibility for properly safeguarding CNWDI<br>• Requirement that dissemination is strictly limited to other authorized personnel with a need-to-know<br>• Any special local requirements<br>**Debriefings**<br>• Purpose of the debriefing<br>• Serious nature of the subject matter, which requires protection in the national interest<br>• Need for caution and discretion | DOD and Industry<br>**Briefing of FSO**: The facility's DCSA Industrial Security representative will give the FSO a CNWDI briefing. |
| **COMSEC** | DODI 5205.08 | COMSEC stands for "Communication Security" and refers to the steps taken to protect | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | NSA/CSS Policy Memorandum No. 3-16<br>DODI 8523.01, Section 4.1<br>Industrial COMSEC Manual (NSA Manual 90-1) “Annex A”<br>NISPOM, Section 117.21(e) | information of intelligence value when it is being telecommunicated.<br>**Briefings**<br>• Types of COMSEC information<br>• Special safeguards for protecting this information<br>• Directives and rules prescribing those safeguards<br>• Penalties for willful disclosure of this information to unauthorized persons | |
| **Courier** | DODM 5200.01, Vol. 3<br>NISPOM, Section 117.15(f)(4) | Employees authorized to hand-carry or escort classified materials or to serve as courier for Defense Courier Service.<br>**Briefings**<br>• Procedures for handling classified information while in transit<br>• Authorized modes of transportation and authorized destinations<br>• Emergency points of contact | DOD and Industry |
| **Declassification Authority** | E.O. 13526<br>DODM 5200.01, Vol. 3 | Required for individuals given the authority to declassify information.<br>**Topics**<br>• Standards, methods, and procedures for declassifying information<br>• Standards for creating and using declassification guides<br>• Contents of the Component’s declassification plan | Declassification authorities are always government officials. |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | | • The requirement for each component to maintain a declassification database | |
| **Derivative Classifiers, Security Personnel, and Others** | E.O. 13526,<br>DODM 5200.01, Vol. 3,<br>NISPOM, Section 117.13(b) | **Topics**<br>• Original vs. derivative<br>• Markings<br>• Downgrading and declassifying<br>• Storage, reproduction, transmission<br>• Declassification guides<br>• Access control<br>• Investigation and reporting<br>• Special access programs<br>• Oversight<br>• Automated information systems | DOD and Industry |
| **Facility Security Officer** | NISPOM, Section 117.12(d) | FSO stands for Facility Security Officer.<br>**Training**<br>• Requirements based on facility's involvement with classified information<br>• May include FSO Orientation and program management courses<br>• Received within one year of appointment | Industry only |
| **Foreign Government Information** | DODM 5200.01, Vol. 1–3,<br>NISPOM, Section 117.13 | FGI stands for Foreign Government Information and is information classified by a foreign government and shared with cleared U.S. personnel.<br>**Briefings**<br>• Definition of FGI<br>• Basic security standards and procedures for safeguarding<br>• Classification levels | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | | • FGI use and disclosure | |
| **Foreign Travel** | DODM 5200.01, Vol. 3,<br>DODM 5200.02,<br>NISPOM, Section 117.8 | Employees are briefed prior to foreign travel or likely exposure to foreign nationals when there is concern about intelligence exploitation.<br>**Briefings**<br>• Security and safety risks<br>• Reporting requirements for suspicious contact<br>• How foreign intelligence services target and approach personnel | DOD, and recommended for Industry |
| **Information System Security Manager (ISSM)** | DODI 8500.01,<br>NISPOM, Section 117.18 | Individuals responsible for managing information systems containing classified information.<br>**Briefing**<br>• To level commensurate with IS complexity<br>• Including responsibility for providing IS security education for relevant personnel | DOD and Industry |
| **Cybersecurity** | DODI 8500.01,<br>NISPOM, Section 117.18 | Cybersecurity: Protection of, prevention of damage to, and restoration of computers, electronic communication systems, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.<br>**Cybersecurity Briefing**<br>• All security measures to protect information<br>• Regulations concerning hardware, software, or portable media<br>• Password and pass-phrase policy directives | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | | **Refresher Training**<br>• Threat identification<br>• Physical security<br>• Malicious content and logic<br>• Social engineering and other non-standard threats | |
| **International Programs** | International Traffic in Arms Regulations (ITAR)<br>Arms Export Control Act (AECA)<br>NISPOM, Section 117.19 | Special briefings are required for individuals who require access to international programs or who participate in international activities.<br>**Courses**<br>• International Security Requirements<br>• International Programs Security and Technology Transfer<br>• DOD Component equivalent course<br>**Topics**<br>• Security assistance<br>• Cooperative research<br>• Foreign disclosure<br>• Country relationships | DOD and Industry |
| **NATO Information** | United States Security Authority for NATO Affairs (USSAN) Instruction 1-07,<br>DOD Directive 5100.55,<br>DODM 5200.01, Vol. 1–3, | NATO classified information is information circulated within and by the member countries of the North Atlantic Treaty Organization (NATO).<br>**Briefings**<br>Employees briefed prior to having access to NATO information:<br>• Applicable NATO security procedures<br>• Consequences of negligent handling<br>**Debriefings**<br>• When an employee no longer requires access to such information, debrief the employee. | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | NISPOM, Section 117.19(g)(7) | | |
| **OPSEC** | DOD 5205.02-M,<br>NISPOM, Section 117.12 | Operations Security (OPSEC) is a system used to identify critical information.<br>**Initial Training and Annual Refresher Training**<br>• Individuals with OPSEC responsibilities<br>**Awareness Training**<br>• All personnel | DOD and Industry |
| **Original Classification Authority** | E.O. 13526,<br>DODM 5200.01, Vol. 3 | Required for individuals given the authority to originally classify information.<br>**Topics**<br>• Original vs. derivative classification<br>• Who can originally classify<br>• Classification standards<br>• Duration<br>• Prohibitions and limitations<br>• Classification marking<br>• Declassification<br>• Security classification guides (SCG) | OCAs are high-ranking government officials. |
| **Physical Security** | DOD 5200.08-R,<br>NISPOM, Section 117.15 | Physical security measures, focused on security-in-depth.<br>**Training**<br>• Perimeter fences<br>• Employee and visitor access controls<br>• Badges/Common Access Cards (CAC)<br>• Intrusion Detection Systems (IDS)<br>• Random guard patrols | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | | • Prohibited item controls<br>• Entry/exit inspections<br>• Escorting<br>• Closed-circuit video monitoring | |
| **Security Professionals** | DODI 3305.13,<br>NISPOM, Section 117.12 | Individuals responsible for the implementation of security programs.<br>**Training**<br>• Established and maintained by the Defense Counterintelligence and Security Agency<br>• May be conducted in the form of instructor-led, distance learning, blended learning, job aids, and other delivery methods appropriate to mission requirements | DOD and Industry |
| **Sensitive Compartmented Information** | DODM 5105.21, Vol. 1–3<br>NISPOM, Sections 117.15 and 117.23 | Sensitive Compartmented Information, or SCI, is classified information derived from intelligence sources and requiring special handling.<br>**Briefings**<br>• All personnel with access must receive an initial briefing. | DOD and Industry |
| **SF-312** | E.O. 13526, NISPOM, Section 117.8 | Standard Form 312, “Classified Information Nondisclosure Agreement,” must be signed by individuals granted access to classified information.<br>**Briefing**<br>• Nature and protection of classified information<br>• Briefing booklet available from ISOO | DOD and Industry |
| **Special Access Programs** | DODI 5205.11, | Any official program or activity employing enhanced security measures. | DOD and Industry |

| SPECIAL BRIEFING TYPES | | | |
|---|---|---|---|
| **Type** | **References** | **Briefing Notes** | **DOD or Industry?** |
| | DODM 5205.07, Vol.1,<br>NISPOM, Section 117.23 | **Topics**<br>• Safeguarding<br>• Access requirements | |
| **Visits and Meetings Security Briefing** | DODM 5200.01, Vol. 3, Enclosure 2,<br>NISPOM, Section 117.16(a)(5) | Cleared visitors to cleared contractor or government facilities must be trained on the security procedures they are expected to follow.<br>**Briefing**<br>• Badges and escorts<br>• Physical security procedures<br>• Access areas<br>• Use of portable electronic devices<br>• Verifying personnel security clearances<br>• Handling classified material<br>• Transmitting and/or transporting classified information<br>• Reporting requirements for security violations | DOD and Industry |

**Review Activity 1**

Matching Drop-down

Select the item from the list below to indicate to which role the statement applies.

- ______________ must receive security education and training that addresses the process for deciding whether information should be classified and the standards information must meet in order to be classified.
- ______________ must receive security education and training that addresses the process for deciding whether information should be classified and the standards information must meet in order to be classified.
- ______________ are responsible for providing security education for relevant personnel prior to processing classified information on AIS.

  - o Couriers
  - o Information System Security Managers
  - o Original classification authorities

**Answer:**

- OCAs must receive security education and training that addresses the process for deciding whether information should be classified and the standards information must meet in order to be classified.
- Couriers must receive training on the procedures for handling classified information while in transit.
- ISSMs are responsible for providing security education for relevant personnel prior to processing classified information on AIS.

**Review Activity 2**

Question (Multiple choice multiple response)

Which of the following statements are true regarding special briefings? Select all that apply.

- o Access to CNWDI is limited to personnel who have a final SECRET or TOP SECRET security clearance.
- o Only uncleared personnel are required to receive a foreign travel briefing prior to traveling abroad.
- o Personnel who have a TOP SECRET security eligibility do not need an additional briefing prior to accessing NATO information or FGI.
- o An oral COMSEC debriefing is not required unless personnel had access to CRYPTO information.

**Answer:** Access to CNWDI is limited to personnel who have a final SECRET or TOP SECRET security eligibility. An oral COMSEC debriefing is not required unless personnel had access to CRYPTO information.

**Summary**

In this lesson you learned about special briefings and other training required for special roles, special types of information, and other circumstances.

Roles with Special Requirements:

- Original classification authorities
- Derivative classifiers
- Declassification authorities
- Security Professionals
- Facility Security Officers
- ISSM
- Couriers

Special Information Types:

- COMSEC
- NATO
- CNWDI
- FGI
- SCI
- ACCM
- OPSEC
- SAP

Foreign Travel Briefings:

- Cybersecurity
- Antiterrorism
- Physical Security
- International Programs
- Visits and Meetings
- SF-312

## Lesson 5: Developing an Effective Security Education Program

### Objectives

Now that you are familiar with the types of security briefings, training, and other education activities required by policy, you are ready to learn about instructional design methodology and implementation best practices that will make your security education program a success.

Here are the lesson objectives. Take a moment to review them.

Developing an Effective Security Education Program Lesson Objectives:

- Identify the characteristics of a successful security education program
- Identify how each of the components of the ADDIE model help in selecting and developing appropriate instructional methods
- Identify potential roadblocks to implementing a successful security education program and strategies for overcoming those roadblocks
- Identify the components and purpose of program evaluation and oversight

ADDIE - A model of instructional design consisting of the following phases: Analyze – Design – Develop – Implement – Evaluate

### Characteristics of a Successful Program

As discussed earlier, a successful security education program is made up of three main components: training, which instructs personnel in their specific security responsibilities; education, which informs personnel about the underlying rationale and importance of those responsibilities; and awareness, which ensures that personnel remain continuously alert to security threats and vulnerabilities.

Underlying all these components is motivation, or what instills in personnel a desire and commitment to be proactive in the execution of their security responsibilities. Employee motivation to participate in the security program is essential to the ultimate success of the other security education efforts. To encourage that motivation in personnel, you should look to design a security education program that has the following characteristics: A successful program is proactive rather than reactive. A proactive program anticipates problems before they occur. On the other hand, a reactive program simply responds to problems after they occur, which in many cases is too late to prevent serious damage to national security.

Although a security education program should be proactive, it should not be inflexible. An effective program adapts to the needs of the community it serves. For example, if you notice that employees are having trouble with foreign travel procedures, you should consider redesigning your foreign travel briefings to be more effective. As serious as security education is, an effective program can be fun! Fun is an essential element of motivation, and if employees do not enjoy the time they spend receiving briefings, their attention may stray, leading them to miss important messages.

The most successful security briefings are those that are short and simple. Briefings should be to the point and only as long as necessary to communicate security responsibilities. Finally, when designing your program, be creative! Use a variety of methods of instruction and think up new and innovative ways of communicating information. This lesson will explore several instructional methods and provide you guidance on when and how to use them.

Basic Elements:

- Training
- Education
- Awareness
- Motivation

Characteristics:

- Proactive vs. reactive
- Flexible
- Fun
- Short and simple

Basic Elements - TEAM Model suggested by Carl A. Roper, Joseph A. Grau, and Dr. Lynn F. Fischer in their book, Security Education, Awareness and Training.

Training - The purpose of security training is to inform personnel of their security responsibilities and allow them to gain the skills and knowledge they need to successfully protect national security.

Education - The purpose of security education is to communicate the underlying principles and rationales of a security program so that personnel understand the importance of their role in providing security.

Awareness - A security education program should include components designed to increase security awareness, or everyday consciousness on the part of personnel, of security threats and vulnerabilities.

Motivation - Motivation is critical to a security education program because it is the element that gives individuals a personal stake in the outcome, increasing the odds that they will proactively contribute to the program.

More: Your security education program, as well as the security activities of personnel, should be proactive, working to prevent security incidents from occurring in the first place. An example of proactivity is providing employees with the tools and knowledge they need to safeguard the classified information with which they work, thus ensuring it is not inappropriately disclosed.

That said, employees must be prepared to react to security breaches as they occur and respond to other weaknesses in the security program. For example, when a self-inspection reveals a problem, it is necessary to take corrective action in the form of increased security education, training, and awareness focused on the problem area.

### Roles and Responsibilities

Perhaps the most essential component of a successful security education program is participation. The key players in developing and implementing a security education program are the FSO or security manager, senior management, and the audience of the training.

The security manager, or in the case of a contractor, the FSO, is responsible for ensuring that all cleared personnel have the knowledge and understanding to handle and safeguard classified and Controlled Unclassified Information (CUI). These individuals have the direct responsibility for overseeing the security education program. Heads of each DOD Component and senior company managers of DOD contractors are required to commit necessary resources to the effective implementation of the Information Security Program.

Finally, the audience of the training has an essential role to play because everyone is responsible for protecting national security information from threats, both internal and external.

- Responsible for ensuring cleared personnel have knowledge and understanding with regard to handling and safeguarding classified and CUI
- Provide support and funding
- Security is everyone’s responsibility. Protecting national security information is critical to thriving in today’s threat environment.

### ADDIE Model

When creating a training and education program of any kind, it is beneficial to practice sound instructional design. Instructional design is a systematic approach to designing and developing training courses and programs. Application of instructional design principles will allow you to create instructionally sound course content, classroom activities, and other tools designed to facilitate learning.

There are many instructional design models that course designers use to develop educational content. The most basic and universally used of those models is known as the ADDIE model. The ADDIE model is a five-step process that involves: analysis, or the determination of the program’s needs and overall purpose; design, or the selection of the most appropriate instructional methods; development, or the creation of the actual training materials; implementation, or the delivery of the training; and evaluation, or the assessment of the training’s effectiveness.

Although the steps can be performed in a strict linear fashion, it is often executed in an iterative, or cyclical, fashion, with each step feeding into the next and back into the process. In general, it is most useful to begin with “Analysis” and proceed through “Design” and “Development” into “Implementation.”

ADDIE is a model of instructional design, which is a systematic approach to creating course content, activities, and other tools designed to facilitate learning.

- Analysis: Determine program needs and purpose
- Design: Select and outline the best method of delivery

- Development: Create the training material
- Implementation: Deliver the training
- Evaluation: Assess the effectiveness of the training

### Analyze

The first step in the ADDIE model is Analysis. There are several types of analysis that you should engage in when developing your program. First, perform a needs analysis, analyzing program needs and establishing overall program goals. During the needs analysis, you will determine what specific briefings you are required to provide. You will also identify areas where additional education, training, and awareness will make your security program stronger. Another part of analysis is a learner analysis, which involves identifying the target audience and analyzing their prior knowledge, experience, and background.

It is also helpful to consider your audience's age and overall experience level. What is their learning style? Are they verbal or visual learners? And what are their job responsibilities? All these factors will affect your audience's preferences for learning and the instructional media and methods you should select.

You should also consider the size and location of the population that needs the training and whether there is a recurring need for this particular training. The last type of analysis is a resource analysis, in which you identify existing resources and training materials you may be able to leverage in creating your program.

Analyze:

- Establish overall program goals: What is needed/required?
  - Initial Security Briefings, Refresher Training, and so on
- Identify target audience: Who are they and what do they already know?
  - Generational differences
  - Learning styles
  - Job responsibilities
  - Size and location of audience
- Identify existing resources: What training is already available?

Generational differences - With a multigenerational work force, you will have an audience with a range of experiences, expectations, and comfort levels with technology. Keep in mind the distinct needs of Baby Boomers, Gen-Xers, and Millennials when designing your training. There is a great deal of interesting research on generational differences and their effect on how people approach work and learning.

Learning styles - Traditional classroom training tends to rely heavily on lecture, but not all learners find listening the most effective way to learn. Some people are highly visual and learn best from pictures, graphs, and other visual aids. Others need to actually perform a task to learn how to do it. When analyzing your audience, determine whether they prefer learning visually, by listening, or by doing. Then, when you design your training, be sure to include elements for all types of learners.

Job responsibilities - Personnel with different job responsibilities will have different needs and expectations for their training. Consider how analysts vs. administrative support staff vs. technological staff might have different content needs and comfort levels with technology. You should work to ensure that the content of the training is relevant to the audience and covers the security responsibilities of the particular personnel who receive the training.

### Design

The next step in the ADDIE model is one of the most important: Design. This is where you develop your program objectives and select instructional media. For each briefing, training course, promotional item, and workshop, you should develop specific, behavioral objectives that are measurable and testable. Based on the objectives of each of your program elements, you will then be able to select the most appropriate instructional media for each course, briefing, or workshop.

You should base this decision first on the effectiveness of the media in achieving your course objectives, and then on the cost of the available media. Examples of instructional delivery methods and formats include lectures, role plays, case studies, simulations, gaming, job aids, discussions, posters, and more. These approaches will be discussed in more detail later in this lesson.

Design:

- Develop specific, behavioral objectives
- Select instructional media:
  - Effectiveness
  - Cost

Lecture, role-play, case study, simulation, gaming, critical incident, drill, job aid, critiques of performance, directed discussions, posters, and so on.

More: The objectives state what you want the learner to be able to do after they complete the training, rather than what you intend to do in the course. For example, rather than stating, “teach the approved transmission methods for transmitting classified information,” you should state: After completing this training, the student will be able to select the most appropriate transmission method for TOP SECRET classified information when sending from a government office to a cleared contractor.

### Develop

The next step in the ADDIE model is often the most time-consuming: Development. During the Develop phase, you will create your course materials, such as: lesson plans, briefing notes, PowerPoint slides, job aids, posters, and handbooks as needed. Depending on the technical complexity of components of your program, you may need a development team or vendor to produce videos and develop eLearning courses.

Be sure to tailor your program to your audience. Keep their abilities, needs, and interests in mind, and remember to what Component or organization employees belong. A program developed for an Air Force unit may not fit if you are going to train a Navy unit. Employees will only be motivated to participate in a program that has relevance to their own work. This phase is also when you will develop exams and other methods of assessing learner achievement.

Develop:

- Create course materials:
  - Write lesson plans and briefing notes
  - Create PowerPoint slides
  - Make job aids, posters, and handbooks
  - Produce videos
  - Develop eLearning courses
- Tailor the program based on employee interests, needs, and abilities
- Develop exams/other methods of evaluation

**Implement**

The Implement phase is when you actually deliver your training, whether you are presenting a briefing, conducting a class, or simply distributing a job aid or flyer. If you have developed eLearning courses, then your role in implementation will include recruiting participants and ensuring that they complete their training requirements.

Implement:

- Present a briefing
- Conduct a class
- Facilitate a workshop
- Distribute a job aid
- Post a poster
- Get people to complete eLearning courses

**Evaluate**

The last phase of the ADDIE model is Evaluation. The purpose of Evaluation is to assess the effectiveness of your education program and to improve future implementation of the program. Although this is the last phase in the process, do not wait until the end to evaluate your program. You should perform ongoing, formative assessment throughout the creation of your briefings and training courses, especially if they are to be complex web-based courses, which can be costly to revise.

The evaluation performed at the end of a course is known as summative evaluation. This type of evaluation provides several levels of feedback. The first is known as “Reaction.” This type of feedback lets you know whether the learners enjoyed the training and were engaged in the course. This is usually assessed by having learner's complete evaluation forms.

The next level of evaluation is called "Learning," which is designed to assess how much students learned in the course. The easiest way to assess learning is to have students take an exam at the end of the course. The next two levels of feedback are quite a bit harder to evaluate but are probably the most important. "Behavior" tells you whether the students have applied what they learned on the job. Are they now following security procedures? And "Return on Investment" demonstrates whether the desired organizational change was achieved. In the case of security education, are there fewer security violations, and is national security being protected?

Evaluate:

- Four levels of evaluation:
  - Reaction: Did the students like the training?
  - Learning: Did the students pass the test?
  - Behavior: Do former students apply new skills on  the job?
  - Return on Investment: Has the security program improved? (e.g., Is the number of security violations lower?) Donald Kirkpatrick's Evaluating Training Programs: The Four Levels (1994)

## Instructional Media

In addition to traditional one-on-one briefings and classroom training, there are a variety of instructional media and training methods you may use in your security education program. Some methods include newsletters and other printed materials; videos, eLearning courses, and other electronic materials; presentations; posters; contests and promotions; and special events.

The most appropriate instructional method will vary depending on the type of security education you are delivering, and on the needs of your audience. At times, you may use more than one method to deliver your message.

### Newsletters and Printed Materials

Newsletters, top-ten lists, job aids, pamphlets, and other printed materials are a great choice for security awareness and continuing security education. When developing a newsletter or other printed media, be sure to get input from employees. Sometimes they are able to provide the most relevant content, as well as actual success stories of security practices in action. To encourage participation from employees, provide rewards for story submissions. You may also visit the Center for Development of Security Excellence, or CDSE, website and access the SETA Toolkit for ideas.

When creating your newsletter, be sure to make creative use of graphics to keep people interested and engaged. You also want to limit the size of your newsletter to the minimum necessary to deliver your message. A newsletter of more than four or five pages may result in loss of interest by the reader. If necessary, issue newsletters more frequently to ensure interest and a quick read. When employees are geographically dispersed, your budget is limited, or you wish to save paper, consider creating an e-newsletter posted on your facility's intranet or disseminating job aids or other materials through email or other electronic means.

Development Tips:

- Get input from employees
- Gather content and success stories
- Provide rewards for participating
- Visit CDSE website for ideas
- Identify existing resources: What training is already available?
- Use graphics
- Limit size

CDSE - Center for Development of Security Excellence

**Electronic Media**

Videos, eLearning courses, and other electronic media are great methods to use for periodic refresher training and some special briefings. They are especially useful when employees are geographically dispersed. Different agencies produce a variety of security videos that you can obtain and show as part of your security education program. Keep in mind that the cost associated with eLearning and video production can be offset by the versatility of the product. You can reach a lot of people in a lot of places with videos and online training.

Development Tips:

- Use when employees are geographically dispersed
- Find already created security videos if applicable

**Presentations**

Another great delivery method for refresher training and continuing education is to hold periodic presentations and demonstrations on a particular security topic. You may also choose to host a roundtable discussion with a specific group or department to discuss security issues and address questions and concerns.

Whether developing a presentation or preparing for a discussion, follow these development tips: select a topic, know your audience and tailor your presentation and approach accordingly, prepare visual aids and handouts that will engage the audience and will be useful takeaways, be sure to communicate the location and time well in advance, and keep the presentation short and to the point, so that participants do not feel overburdened by attending. Finally, employee participation in the training can be a great motivator for attendees.

Development Tips:

- Pick a topic
- Know your audience
- Prepare visual aids and handouts

- Post the location and time
- Keep it short and to the point and have a sense of humor
- Provide opportunities for attendee participation

**Posters**

Posters with security reminders and messages are an ideal delivery method for continued security awareness, because they help to ensure that employees remain ever-conscious of the importance of constant vigilance, resulting in good security practices. Be creative with your poster design, using interesting artwork and motivational reminders.

Also, display posters and other promotional materials in interesting and unexpected places, so that employees are sure to notice them, and keep them fresh by changing them out often. Maintaining a security bulletin board can also be very useful. The Director of National Intelligence, or DNI, website has many sample posters available.

Development Tips:

- Use motivational reminders
- Be creative with posting location
- Maintain a security bulletin board
- Visit the Director of National Intelligence (DNI) website for sample posters

**Contests and Promotions**

Another creative way to encourage employee participation in security awareness and continuing education is to hold contests. Ask employees to submit their own poster designs and make it rewarding, giving out prizes for the best posters. Use promotions, such as coffee mugs, rulers, luggage tags, and other simple items labeled with security messages as prizes, or simply hand them out to the employees as motivational reminders.

**Special Events**

Because protecting national security is everyone’s responsibility, it can be really effective to get an entire community involved in a security education program. Hold a security awareness fair, with exhibit booths staffed by security experts, and more. Have employees invite their families and have special demonstrations and activities, such as fingerprinting children.

Either as part of a fair, or as a stand-alone presentation, invite local police, FBI agents, other law enforcement, representatives, or counterintelligence specialists to give presentations on the importance of security activities.

Get the community involved!

- Security awareness fairs
- Law enforcement presentations by:
    - Local police
    - FBI agent

  - Other law enforcement representative

## Implementing a Security Education Program

One of the first steps in implementing a security education program is to gain support—both from management and from rank-and-file employees. To do so, you must sell yourself, displaying both knowledge and credibility. If your audience senses that you are credible, your ability to communicate your message and win their support will be greatly enhanced.

To ensure that you are a credible messenger, you must display a commanding knowledge of security policy and its applications and an understanding of the threat to national security and your organization. You must also be able to develop and communicate the overall goals of the security education and training program to your management team. These goals must be clearly expressed and directly tied to the regulations and policy documents discussed earlier in this course.

Your vision for your security education and training program can be delivered through verbal and written communications, both of which require effective presentation skills. You should also develop a security education and training plan for your organization, which can assist you in communicating your knowledge and tailored program goals and in selling your program.

Implementation activities:

- Get management buy-in
- Motivate your workforce
- Sell yourself
- Security policy
- Application
- Perception of threat
- Set overall goals
- Develop security education and training plan

### Management Buy-in

Management support for a security education program is absolutely essential and is mandated by DOD regulations. Supportive management does more than just provide the budget; it also offers organizational motivation and emphasizes good security practice as a critical organization priority. Because lack of management support can become a distraction and major impediment to a successful security education and awareness program, one of your most important jobs in planning your program is winning management support.

To ensure that you receive the budget you need to fund your program, you should establish yourself as a part of the management team when possible. Alternately, you may request that a member of the management team serve as a security advocate. To be part of management decision-making, you and other key security personnel should attend staff meetings to ensure that security programs and security education programs are prioritized appropriately. Attending staff meetings will also allow you to stay informed on what’s going on in the organization. You play an essential role in your organization's success, and you need to remind others of your responsibilities.

Whether you are on the management team or working in support of security management, your organization's management needs to know that security is not an expense; it's an investment and a requirement. Once you have captured management's attention and have established yourself as a key management player, you will be in a position to ensure that security is an essential element of all management activities, including planning, logistics, human resources, operations, and marketing.

Establish yourself as a member of the Management Team!

- Attend staff meetings
- Remind others of your responsibilities
- Sell yourself

Security must be at the heart of management activities:

- Planning
- Logistics
- Human Resources
- Operations
- Marketing

More: Extra information for contractors

Remember: When your organization signed the DD Form 441, it has a contractual responsibility to establish an effective security program and the responsibility to protect classified information fell on your shoulders as a Facility Security Officer.

Advise management that it is better to spend the time and money properly training your employees than investigating violations and compromises, which need to be reported to your paying customers.

Systems and procedures set up to protect the classified information can be used, to a lesser degree, to protect your proprietary information. All of this translates to business survival.

### Employee Motivation

Just as important as gaining management support is ensuring employee participation in your program. Although regulations mandate employee compliance, policy alone is not enough to ensure universal practice of security procedures. You'll need an effective program to motivate your workforce to participate in good security practices. The best way to do that is to inform your employees and keep them knowledgeable of security practices.

Make sure the employees know and understand the threat – who is targeting what? A successful program will provide incentives for employee participation. Communicate to employees the positive roles they can play in the security program and stress that everyone is part of the security team. And, finally, the best way to motivate employees to participate in the program and employ good security practices is to lead by example.

Motivating Employee Participation:

- Keep employees informed of security practices
- Make sure employees understand the changing threat
- Provide incentives
- Involve employees in the program
- Lead by example

**Maintaining a Security Education Program**

The final essential piece of a successful security education program is maintenance and oversight.

DODM 5200.01 Volume 3 requires that DOD Component heads ensure that security education programs are evaluated through both self-inspections and external oversight activities. Contractors are also required to conduct self-inspections, which include evaluation of their security education program.

The purpose of program oversight is to measure success by providing a picture of how the system is working and to assess the quality and effectiveness of the security education efforts. The evaluation activities may also identify areas where additional training is needed. Program oversight activities should be performed on a regular basis or when there is an administrative inquiry or reported security violation. Records of program oversight must be maintained with records management instructions, in accordance with DODI 5015.02, DOD Records Management Program.

Program Oversight:

Methods:
- Self-inspection
- Interviews

Purpose
- Measure success
- Assess quality and effectiveness
- Identify if additional training is needed

Performed
- On a regular schedule
- When there are administrative inquiries or reported security violations

Records
- Maintained in accordance with DODD 5015.2

**Review Activity 1**

Question (Survey true/false )

1. Only security experts should be involved in developing security education programs.

o True
o False

**Answer:** Security is everyone’s responsibility, and the target audience should be encouraged to participate in the development of security education programs.

2. Security education programs should be proactive rather than reactive.

o True
o False

**Answer:** An effective security education program is proactive rather than reactive.

3. Creative and fun components of security education programs can motivate employees to participate.

o True
o False

**Answer:** Creative and fun components of security education programs can motivate employees to participate.

4. Security education programs should be considered an expense, rather than an investment.

o True
o False

**Answer:** Security education is not an expense. It is an investment that will protect national security, save money, and is required by law.

5. Senior management should be involved in solving problems faced in the development of a security education program.

o True
o False

**Answer:** Senior management should be involved in solving problems faced in the development of a security education program.

**Review Activity 2**

Question (Multiple choice single response)

Which of the following is the most appropriate instructional method to use when you wish to quickly remind employees scattered in locations around the world of several security best practices.

- ○ Create posters and hang them up in office hallways and common areas.
- ○ Create an eLearning course.
- ○ Distribute an e-newsletter.
- ○ Hold a security awareness fair.

**Answer:** Newsletters are ideal for quickly communicating tips, reminders of security practices, and success stories. Electronic dissemination is best in this situation because employees are geographically dispersed.

**Review Activity 3**

Question (Multiple choice multiple response)

Which of the following are purposes of program oversight? Select all that apply.

- ○ Measuring program success
- ○ Informing employees of their security obligations
- ○ Identifying whether additional training is needed
- ○ Assessing program quality and effectiveness
- ○ Eliminating the need for individual reporting of security violations

**Answer:** The purposes of oversight of a security education program are to measure program success, identify whether additional training is needed, and to assess program quality and effectiveness. It does not eliminate the obligation for individual reporting of security violations.

**Summary**

In this lesson, you learned about instructional design methodology, the most appropriate instructional methods for your security education efforts, activities involved in implementing a security education program, and the components of program oversight.

Implementation:

- Get management buy-in
- Motivate your workforce
- Sell yourself
- Set overall goals

Program Oversight:

- Methods
- Purpose
- Performed
- Records

# Lesson 6: Course Conclusion

## Course Summary

Working with classified materials carries significant responsibilities. For this reason, it is essential that your security program includes a robust security education, training, and awareness effort to ensure those who have access to the information know how to protect it.

You should now know the policy requirements for a security education and training program, the best practices for developing and implementing such a program, and a variety of useful instructional strategies and methods.

## Lesson Review

Here is a list of the lessons in the course.

Lessons:

- Introduction to Security Education and Training Requirements
- Basic Security Briefing Requirements
- Special Briefings and Other Training
- Developing an Effective Security Education Program

## Course Objectives

Congratulations! You have completed the Developing a Security Education and Training Program course. You should now be able to perform all the listed activities.

You should now be able to:

- State the purpose of a security education and training program.
- Identify security education and training policy requirements for DOD and Industry personnel.
- Describe and define the types of required security briefings for all cleared personnel.
- Identify the various audiences of a security program.
- Discuss the training requirements for Industry and the DOD.
- Identify and define the types of briefings and other training required for specific roles/activities.
- Identify the various types of special briefings and recognize when they are required.
- Identify the characteristics of a successful security education program.
- Identify how each of the components of the ADDIE model help in selecting and developing appropriate instructional methods.
- Identify potential roadblocks to implementing a successful security education program and strategies for overcoming those roadblocks.
- Identify the components and purpose of program evaluation and oversight.