Student Guide

Course: DoD Security Policies, Principles & Programs

Lesson 1: Introduction and Background
Topic 1: Introduction

Course introduction

What governs Department of Defense (DoD) security programs?
- **Policies**
- **Principles**
- **Programs**
- **Governing documents**
- **Four overarching security disciplines**

The lessons you will be working through are:
- **Introduction and Background**
- **Role of the Federal Government**
- **DoD Security Responsibilities**

Narration Script: In this course, you will examine the policies, principles, programs, governing documents, and four overarching security disciplines that govern how the Department of Defense—or DoD—implements its security programs. In the United States, national security has been evolving since the Revolutionary War, and to this day, we still struggle over the methods and means to implement it. Our national security program developed slowly. The first formal system for the protection of information was not put into place until 1912. For additional historical perspective on the development of our national security program, please enroll in our Introduction to Information Security e-Learning course. Now, take your seat in time—modern-day America—and let's concentrate on security programs as they exist now. The lessons you will be working through include Introduction and Background, Role of the Federal Government, and DoD Security Responsibilities.

Overview of entire course

Introduction and Background **lesson topics:**
- **The importance of security programs**
- **An overview of basic security policies and principles**

Role of the Federal Government **lesson topics examine how security policies and principles are influenced by:**
- **Branches of government**
- **Executive Orders**

DoD Security Responsibilities **lesson topics:**
- **DoD security disciplines and roles**

- **Special types of information**
- **DoD security instructions, directives, and regulations**

Narration Script: Take a moment to familiarize yourself with the course's organization and content. Although you can work through the material in any order, we recommend you follow this sequence since the lessons and topics build upon one another. This lesson explores the importance of security programs and provides a brief overview of basic security policies and principles. In the *Role of the Federal Government* lesson, you will examine how security policies and principles are influenced by the three branches of the government as well as by Presidential Directives and Executive Orders. In the final *DoD Security Responsibilities* lesson, you will investigate DoD security disciplines and roles, special types of information, and DoD security instructions, directives, and regulations. After you have looked over the course topics, we will review the course objectives.

Course objectives

Course Objectives

After completing this course, you will be able to:

- **Identify the roles of the three branches of the Federal Government and the Executive Branch agencies responsible for security policies and direction**
- **Identify the responsibility of various DoD security offices and disciplines**
- **Identify Executive Orders relevant to security policy and their purpose**
- **Identify other types of documents that guide security policy**
- **Identify the two basic policies and three basic principles that provide a framework for security programs within the Federal government**

Narration Script: This course is designed to help you attain the overall course objectives. Take a few moments to familiarize yourself with the course objectives. The next topic includes general introductory information and works through specifics regarding why security programs are needed and how they are implemented. Let's get started.

Lesson 1: Introduction and Background
Topic 2: Importance of Security Programs

Topic introduction

Position of the United States without security:

- **The original colonies might not have been able to fight successfully for independence**
- **Spies and criminals might gain access to our nation's:**
  - **Protected technological advances**
  - **Industrial secrets**
  - **Diplomatic information**
- **Our citizens' personal information would be vulnerable**
- **Potentially greater danger from insider threats**

This topic explores:

- **Need for a security program**
- **Role of a security program**

Narration Script: Imagine current world events and then think about what might happen if the United States had no national security program. The position in the world of the United States without security is symbolized by the unlocked chain. In this scenario, our national assets would have no protection. The original 13 colonies might not have been able to plan for—and actualize—their fight for independence. Our country would not be able to protect itself from espionage and sabotage. Individuals who are determined to do harm to our national security could have access to our nation's technological advances, industrial secrets that support our nation's economy, or information, potentially providing our adversaries with a technological or strategic advantage over the United States. Aside from the risks to national security, individuals' personal information—Social Security numbers, health records, and credit information—would also be vulnerable to unauthorized access if no security were in place. And there's always the potential for insider threats—for example, Ana Montes, the Defense Intelligence Agency senior intelligence analyst who passed Top Secret information to Cuban intelligence for 16 years. In this topic, you will explore the need for a security program to protect our national assets—and just such a program has existed, in one form or the other, since America's colonial days. The role of our security program is to safeguard our assets, and the most important asset is the American people.

Topic objectives

Topic Objectives:

- **Define why a security program is necessary**
- **Identify the three goals of Federal security programs**

Narration Script: Your objectives for this topic include define why a security program is necessary, and identify the three goals of Federal security programs.

Need for security programs

United States assets to protect:

- **Our citizens**

- ***Classified Information***
- ***Controlled Unclassified Information***
- **Facilities and installations**
- **Employees and resources**

Common aspects of *security programs* **need to:**
- **Provide consistency in protecting all national assets**
- **Establish minimum security standards**
- **Ensure adequacy of protection**

Four overarching security disciplines that help attain these goals:
- **Information security**
- **Personnel security**
- **Industrial security**
- **Physical security**

Narration Script: The overall need for a security program is evident. Our country possesses all kinds of assets that require security for our citizens, for classified information, for certain types of controlled unclassified information requiring adequate protection at all levels, for facilities and installations, and for employees and other resources. To effectively implement the security programs, government branches need consistency in the procedures required to protect national security assets, and they need established common minimum security standards. The government needs a way to ensure adequacy of protection, thereby promoting the confidence of the American people that they are safe. The four overarching security disciplines provide a convenient way to categorize and organize the programs and activities required to attain our security goals. The four security disciplines are information security, personnel security, industrial security, and physical security.

Role of security programs

Uniform basis for safeguarding our national assets across all three branches of government are:
- **Consistency in protecting all national assets**
- **Observation of minimum security standards in all programs and activities**
- **Adequacy of provided protection**

Narration Script: Federal security programs seek to provide a uniform basis for safeguarding our national assets across all three branches of government—Executive, Legislative, and Judicial. To achieve this goal, government activities that implement security programs observe three aspects that help ensure commonality across the branches. These are first, consistency in the protection provided to all national assets; second, observation of minimum security standards in all programs and activities; and third, adequacy of protection provided. Systematic observation of these aspects is required because of the importance of security programs. Following these aspects helps to ensure confidence across the government and among citizens that the required resources are effectively and efficiently dedicated to national security.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

You've just examined the role of the nation's security program. Try out this question.

Identify THREE of the following common aspects that are observed in the implementation of national security programs in every branch of the government.

- ❑ **To provide consistency in protecting all national assets**
- ❑ **To establish minimum security standards**
- ❑ **To ensure adequacy of protection**
- ❑ **To provide a uniform basis for the government to gather information**
- ❑ **To provide a means for decoding gathered information**

The correct answers are:
To provide consistency in protecting all national assets
To establish minimum security standards
To ensure adequacy of protection

Topic summary

Importance of Security Programs Summary:

- **Need for a security program**
- **Three aspects of uniformity in security programs across the government**
    - **Consistency in protecting all national assets**
    - **Minimum security standards common to all programs and activities**
    - **Adequate protection provided**

Narration Script: This was a short but very important topic. It tried to help you answer the question—why does our nation need to establish security programs? Our nation's citizens and assets are too valuable to leave unprotected. Protecting them requires the establishment of security programs. To ensure national security, we cannot allow access to our security resources and information by individuals who are unauthorized or would do us harm. Because of the importance of our national assets, security programs need to be implemented with uniformity across the branches of government. Three aspects that contribute to uniformity of implementation have been established. These aspects help ensure consistency, minimum standards of security, and adequate protection. In the next topic, you'll take a more in-depth look at the security policies and principles used to implement these aspects of our important national security.

Lesson 1: Introduction and Background
Topic 3: Overview of Security Policy and Principles

Overview

Overview of Security Basic Policies and Principles

Two basic policies and three supporting principles underlie security programs.

Two basic policies provide a framework for all of the security principles:
- **Availability**
- **Economizing**

Three basic principles provide the basis for all of the security programs:
- **Prioritizing**
- **Consolidating**
- **Overlapping**

Begin by examining the policies.

Narration Script: There are two basic policies and three supporting principles within the Federal Government that provide a framework for security programs. This topic will provide an overview of these policies and principles. The two basic policies of availability and economizing provide a framework for all the security principles. In turn, the security principles of prioritizing, consolidating, and overlapping are the foundation for all the security programs.

Policies

Two basic policies:
- **Availability**
- **Economizing**

Read the following for more information.

Economizing

The policy of economizing means that using assets wisely is an inherent government responsibility:
- **The public pays for the assets.**
- **The public demands that the government spend wisely.**

Since the public pays for these assets, the government wants to ensure wise spending to get the most mileage out of the money and the most "bang for the buck."

Availability

Federal government assets belong to the public and consequently are available to the public with certain exceptions.

Examples of exceptions include:

- **Classified Information**
  - **Top Secret**
  - **Secret**
  - **Confidential**
- **Controlled Unclassified Information—For Official Use Only**

Some information is not available to the public because of security or privacy measures, or other restrictions and limitations that apply to government protected information.

Narration Script: Let's begin by examining the policies. Read each item for more information. After you investigate each of the basic policies, on the next screen we'll look at how they support the three foundational principles.

Principles

Three supporting security principles are:

- **Prioritizing**
- **Consolidating**
- **Overlapping**

Read about each principle to discover more.

Narration Script: As a result of the two basic security policies, availability and economizing, the three supporting security principles, prioritizing, consolidating, and overlapping, have evolved and are used throughout security programs. Let's look at how each principle complements the others while incorporating the two basic security policies. Read about each of the three security principles to find out more about how it affects security programs.

Prioritizing

Prioritizing:

- **Ranks Federal assets from the most important to the least important**
- **Is used to select, target, and apply security resources**

Narration Script: The principle of prioritizing incorporates the policy of economizing. Prioritizing is the act of identifying and ranking the most important—down to the least important—Federal assets. Prioritizing also determines where security resources are focused and subsequently applied. For example, Top Secret, Secret, and Confidential materials require different levels of protection. Since Confidential materials are not as sensitive as Top Secret materials, it wouldn't be cost effective to spend the same amount of money protecting Confidential information as you do for protection of Top Secret material. There are numerous other examples of

prioritizing, such as the level of protection provided to nuclear weapons as opposed to that given to small arms, or the protection of senior officials as opposed to that given to junior officials. The principle of prioritizing also incorporates the policy of availability: As you are prioritizing the Federal assets, you will also consider the sensitivity of the information. If the information is determined publicly releasable, it will be made available to the general public.

Consolidating

Consolidating:

- **Provides better protection by placing assets in a small number of locations**
- **Helps the government afford better protection of its assets**

Read the examples of the consolidating principle.

Top Secret

Because of the policy of economizing, not everyone or every office is going to have its own security container. In this instance, a security container may be used with different levels of classified material stored in each drawer, provided everyone with access to the container has the appropriate security clearance eligibility and access as well as the need to know. Another option would be to have a multidrawer container with the appropriate combination lock on each drawer. This ensures those who only have access to a certain drawer of information are prevented from accessing the information stored in the other drawers.

In other instances, a defined area may be constructed as a Sensitive Compartmented Information Facility (SCIF) or a Special Access Program Facility (SAPF). People requiring access into either of these facilities must possess the appropriate level of security clearance and access eligibilities as well as the need to know. The physical security requirements may be the same for both; however, require strict access control to meet the need-to-know criteria for each area. This is met through access control devices versus the construction of two separate areas.

Narration Script: The principle of consolidating incorporates the policy of economizing. Consolidating provides better protection by placing assets in a small number of locations rather than having them scattered over a large area. Consolidating also helps the government make better use of taxpayer dollars because fewer protection resources are required to provide adequate protection for all the assets. Fewer protection resources mean lower costs. That is why consolidating Classified Information is more cost effective. For example, instead of storing different levels of classified material in different containers in many locations, all levels of Classified Information can be placed in one container, as long as the container is approved for the highest level of information being stored and everyone with access to the information has the appropriate security clearance and access eligibilities as well as the need to know. Storing Confidential information with Secret and Top Secret levels is more cost effective than having separate containers for each level. One container is easier to protect, making it more economical. Read the examples of the consolidating principle. The government also employs the consolidation principle when it comes to supporting the availability to the public. For example, the availability policy is considered in the management of the Freedom of Information Act program, also called FOIA. It offers consolidated operations used by the public to gain access to publicly releasable government information.

Overlapping

Examples of overlapping:
- **Security discipline interrelationship**
- **Security-in-depth**

Read the examples of the overlapping principle.

Security Discipline Interrelationship

An example of the principle of overlapping is the interrelationship among the Personnel, Physical, Information, and Industrial Security disciplines:
- **The Physical Security discipline addresses the requirements for the physical protection of government assets.**
- **The Information Security discipline promotes the proper and effective classification, protection, and downgrading of official information requiring protection in the interest of the national security. It also promotes the declassification of information no longer requiring such protection.**
- **The Industrial Security discipline requires industry partners to protect classified information released or disclosed to them in connection with classified contracts under the National Industrial Security Program (NISP).**
- **The Personnel Security discipline requires individuals to meet and retain their security clearance eligibility and have the need to know for access to classified and sensitive information.**

All four security disciplines address requirements for protecting classified information.

Security-in-Depth

A good example of the principle of overlapping is security-in-depth. This term means security resources are deployed in layers of increasing intensity. The closer one gets to the asset being protected, the more stringent the safeguards become. For example:
- **An asset may have a fence as the first layer of security.**
- **The second layer of security may be an armed guard.**
- **The third layer could be a secure structure with a high-security lock and an alarm system.**
- **A fourth layer might comprise an entry controller and a badge exchange system controlling entry to the facility.**
- **A final layer could consist of securing the asset vault with a dedicated alarm system and protecting it with an armed guard.**

Narration Script: The principle of overlapping incorporates the policy of economizing. Overlapping is the process of using more than one security resource or discipline to protect national assets in an effort to provide the best and most cost-effective form of safeguarding. Overlapping can occur between the four security disciplines or between elements within a security discipline itself. The security disciplines interrelate or overlap each other to form a security umbrella that enhances asset protection. An example of the security umbrella is provided by the practice of security-in-depth measures, which integrates practices from the physical, information, industrial, and personnel security disciplines to provide stronger asset protection than any one of

the disciplines itself. Applying the overlapping principle ensures all security measures interrelate—or overlap—each other in an effort to provide stronger asset protection. Read the examples of the overlapping principle.

Knowledge check

Matching—match each item on the left with the selection you choose from the list on the right.

Federal Government security programs operate under two policies and three principles.

Match each policy and principle with the BEST definition.

Availability	**The policy that attempts to get the best value for the money**
Economizing	**The policy is based on the notion that government assets belong to the people**
Prioritizing	**The principle integrates the application of security disciplines to protect Federal government assets**
Consolidating	**The principle that determines where security resources are focused and applied**
Overlapping	**The principle that helps the government provide better protection for its assets at less cost**

The correct matches are as follows:

Availability	**The policy is based on the notion that government assets belong to the people**
Economizing	**The policy that attempts to get the best value for the money**
Prioritizing	**The principle that determines where security resources are focused and applied**
Consolidating	**The principle that helps the government provide better protection for its assets at less cost**
Overlapping	**The principle integrates the application of security disciplines to protect Federal government assets**

Topic summary

Overview of Security Policy and Principles

Basic policies and principles underlie national security programs.

Two basic policies:
- **Availability**
- **Economizing**

Three supporting principles:
- **Prioritizing**
- **Consolidating**
- **Overlapping**

Narration Script: To recap this topic, the two basic policies of availability and economizing provide guidance for the application of three supporting principles: prioritizing, consolidating, and overlapping. Prioritizing identifies assets from the most important to least important and determines where resources are going to be focused. After assets are prioritized, they are consolidated accordingly, allowing the best protection for the least

amount of money. And overlapping ensures that the protection offered is multilayered. In the next lesson, we'll explore additional details about information security and the Federal Government's role. That information will provide examples of the application of the policies and principles.

Lesson 1: Role of the Federal Government
Topic 4: Branches of Government

Topic introduction

This lesson examines the role of the Federal Government as it pertains to security programs.

Authority for Federal security policies and programs originates from the *Executive***,** *Legislative***, and** *Judicial* **branches of government. Each branch plays a different role in developing and implementing security policy.**

Let's explore the branches of the Federal Government:
- **Executive**
- **Legislative**
- **Judicial**

Continue reading to investigate each branch.

Narration Script: Welcome to the Role of the Federal Government lesson. As you can tell by the title, this lesson examines the role of the government as it pertains to security programs. The Executive, Legislative, and Judicial branches of government create the authority for Federal security policies and programs within our governmental system. Each branch is then responsible for developing and implementing security policy. Let's explore the three Federal branches and the role they play in security policy.

Executive Branch

The President:
- **Head of the Executive Branch of the Federal Government**
- **Responsible for the nation's security policies and procedures**
- **Issues Presidential Directives and Executive Orders (E.O.) to communicate policies and procedures**

Different terminology used to refer to Presidential Directives:
- **National Security Action Memoranda (NSAMs)**
- **National Security Decision Memoranda (NSDMs)**
- **Presidential Directives (PDs)**
- **National Security Decision Directives (NSDDs)**
- **National Security Directives (NSDs)**
- **Presidential Decision Directives (PDDs)**
- **National Security Presidential Directives (NSPDs)**
- **Homeland Security Presidential Directives (HSPDs)**
- **Presidential Memoranda (PMs)**

Narration Script: The President of the United States is the head of the Executive Branch. The President is responsible for the nation's security policies and procedures. The President issues security policy and guidance in the form of Presidential Directives and Executive Orders. Executive Orders are issued as a formal means

through which the President prescribes the conduct of business in the Executive Branch. (We'll cover Executive Orders more extensively in the Executive Orders topic later in this lesson.) Presidential Directives are developed by the National Security Council when they concern national security. They are signed or authorized by the President and are given various names by different Presidential administrations. For example, President John F. Kennedy and President Lyndon B. Johnson referred to their Presidential Directives as National Security Action Memoranda, while President Richard M. Nixon and President Gerald R. Ford referred to theirs as National Security Decision Memoranda. President Jimmy Carter called his Presidential Directives, while President Ronald Reagan called them National Security Decision Directives. President George H. W. Bush referred to his as National Security Directives, while President William "Bill" J. Clinton called them Presidential Decision Directives. President George W. Bush issued National Security Presidential Directives and also as a result of 9/11 created Homeland Security Presidential Directives. President Barack Obama refers to his Presidential Directives as Presidential Memoranda. Each administration approaches the issuance of its Presidential Directives based on world events and administrative styles and preferences.

Security policy advice to the Executive Branch

The President receives security policy advice and input for the Executive Branch from a variety of organizations:

- **National Security Council (NSC)**
- **Information Security Oversight Office (ISOO)**
- **Department of Defense (DoD)**
- **Office of Personnel Management (OPM)**
- **Department of Justice (DoJ)**
- **Department of Commerce (DoC)**
- **Office of Management and Budget (OMB)**
- **Department of Energy (DoE)**

Read about each organization for more information. Then visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to learn more about the Executive Branch.

National Security Council (NSC)
The NSC was established by the National Security Act of 1947 and amended by the National Security Act Amendments of 1949. Later in 1949, as part of the Reorganization Plan, the Council was placed in the Executive Office of the President. The NSC is the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and Cabinet officials. The Council also serves as the President's principal arm for coordinating those policies among various government agencies.

Members of the NSC: The NSC is chaired by the President. Regular NSC attendees are the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Chairman of the Joint Chiefs of Staff is the military advisor to the NSC, and the Director of National Intelligence (DNI) is the intelligence advisor. The heads of the other Executive Branch departments and agencies, as well as other senior officials, are invited to attend meetings of the NSC as appropriate.

National Security Council Staff: The NSC staff, headed by the Executive Secretary, serves as the President's national security and foreign policy staff within the White House. The staff receives its direction from the President, through the National Security Advisor. The Executive Secretary assists the President and the Assistant to the President for National Security Affairs in preparing for meetings with foreign leaders and in connection with the President's foreign travel. The staff performs a variety of activities in advising and assisting the President and the Assistant to the President for National Security Affairs, including participating in Presidential briefings, assisting the President in responding to Congressional inquiries, and preparing public remarks. The NSC staff serves as an initial point of contact for departments and agencies that wish to bring a national security issue to the President's attention.

Other offices/organizations within the NSC structure include:

1. Information Security Oversight Office (ISOO): Oversees the security classification programs in both government and industry, and reports to the President annually on their status. ISOO was originally established in 1978 under Executive Order 12065. It now operates under the authority of Executive Order 13526, and is currently a component of the National Archives and Records Administration (NARA). More details are provided under ISOO.

2. National Telecommunications and Information Systems Security Committee (NTISSC). Established by NSDD 145, under the NSC. The Executive Agent is the Secretary of Defense (SECDEF), and the National Manager is the Director, National Security Agency.

Information Security Oversight Office (ISOO)

Established by President Jimmy Carter, the ISOO is responsible to the President for policy and oversight of the government-wide security classification system and the National Industrial Security Program. ISOO comes under the National Archives and Records Administration (NARA) for administrative purposes only. Operationally, ISOO comes under the NSC.

The Assistant to the President for National Security Affairs, a member of the NSC, provides policy and program direction to the ISOO for the security classification program. The ISOO oversees the program for both government and industry and reports annually to the President on the status of those programs.

ISOO receives authority from Executive Order 13526, Classified National Security Information, and Executive Order 12829, National Industrial Security Program, and functions with three components:

- **Classification Management Staff**
- **Operations Staff**
- **Controlled Unclassified Information (CUI) Office**

Department of Defense (DoD)

Within the DoD, the Secretary of Defense has designated the Under Secretary of Defense for Intelligence, USD(I), as the Primary Security Advisor (PSA) and advisor to the Secretary and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters.

USD(I) develops, coordinates, and oversees the implementation of DoD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DoD Special Access Program (SAP) security as well as research and technology protection.

The USD(I) further serves as the DoD Senior Security Official pursuant to E.O. 13526, and advises the Secretary of Defense, secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the heads of DoD components on the development and integration of risk-managed security protection policies and programs (except for Nuclear Physical Security pursuant to DoD Directive O-5210.41).

For more information on the responsibilities and functions of the USD(I), refer to DoD Directive 5143.01, Under Secretary of Defense for Intelligence—USD(I).

Office of Personnel Management (OPM)

The OPM is the Federal Government's human resources agency, ensuring the nation's civil service remains free of political influence. The OPM oversees the fair, merit-based selection and treatment of Federal employees.

Federal employees are subject to security measures as provided by E.O. 10450, Security Requirements for Government Employment. OPM conducts personnel security investigations. OPM is also responsible for the monitoring and implementation of how the personnel security program is run by the Executive Branch agencies to ensure requirements of E.O. 10450 and E.O. 12968 are met.

Department of Justice (DoJ)

The DoJ is an executive department headed by the Attorney General, who represents the United States in legal matters and provides legal counsel to the President when requested.

Department of Commerce (DoC)

The DoC is an executive department responsible for fostering, serving, and promoting the nation's economic development and technological advancement. The DoC participates with other government agencies in the creation of national policy through the President's Cabinet and its subdivisions.

One of the ways the DoC executes its mission is by acquiring, analyzing, and disseminating information regarding the economy to help achieve increased social and economic benefit.

Office of Management and Budget (OMB)

The OMB oversees contracting and budget issues. Its mission is to assist the President in overseeing the preparation of the Federal budget and to supervise budget administration in Executive Branch agencies. The OMB:

- **Evaluates the effectiveness of agency programs, policies, and procedures**
- **Assesses competing funding demands among agencies**
- **Sets funding priorities**

Department of Energy (DoE)

One of the DoE's missions is to advance the national, economic, and energy security of the United States. Energy security is foremost in the Atomic Energy Act of 1954.

Now fundamental U.S. law, the Atomic Energy Act of 1954 addresses the development and regulation of nuclear materials. The law stipulates that the "development, use, and control of atomic energy shall be directed so as to promote world peace, improve the general welfare, increase the standard of living, and strengthen free competition in private enterprise."

Narration Script: The President is advised on security policy by numerous organizations and departments in the Executive Branch. These departments and agencies include the National Security Council, the Information Security Oversight Office, the Department of Defense, the Office of Personnel Management, the Department of Justice, the Department of Commerce, the Office of Management and Budget, and the Department of Energy. Other agencies, departments, and personnel may also advise the President on security matters as appropriate. Read about each organization for more information. Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to learn more about the Executive Branch.

Security executive order chain of command

Narration Script: The chart on this screen illustrates the chain of command governing the issuance of Executive Orders that prescribe security policy and procedures within the Executive Branch. The President signs the Executive Orders. The Executive Orders are then passed through the National Security Council, or NSC, which in turn passes the order to agencies within the Executive Branch. Keep in mind the Chairman of the Joint Chiefs of Staff is the military advisor to the NSC, and the Director of National Intelligence (or DNI) is the intelligence advisor. The issuance and implementation of Executive Orders may vary; some are issued directly to the Executive Branch agencies, and others may be issued through an implementation agency for uniformity. For example, the Director of Information Security Oversight Office—or ISOO—is designated, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, to issue implementing guidance for Executive Order 13526. Once the ISOO issues the ISOO directive number one, the directive goes to the executive agencies for implementation. Within the DoD, the Secretary of Defense receives the directive and passes it to the Under Secretary of Defense for Intelligence, who then issues DoD policy to the DoD components and organizations.

Legislative Branch

The Legislative Branch consists of the House of Representatives and the Senate. Together, they form the

U.S. Congress. Among the functions of this branch is passing the laws that directly and indirectly affect our national security programs.

The *Atomic Energy Act of 1954* **directly affected security by creating a security program regarding nuclear power and its associated information.**

The *Freedom of Information Act* **(FOIA) indirectly affects our national security program by forcing or preventing the release of certain types of information.**

The *Intelligence Reform and Terrorism Prevention Act of 2004* **directly affects the intelligence community and intelligence-related activities of the United States government.**

Other legislative examples dealing with national security include:

- *National Security Act*
- **Espionage statutes**
- *Military Critical Technologies List* **(MCTL)**
- *Classified Information Nondisclosure Agreement* **(SF 312)**
- **Hearings and investigations**

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html for additional information on the Legislative Branch.

Narration Script: The Legislative Branch directly and indirectly affects the nation's security programs. For example, the Atomic Energy Act of 1954 directly affected national security by creating a security program for nuclear power information. On the other hand, the Freedom of Information Act indirectly affects our national security program. The FOIA forces or prevents the release of certain types of information. The Intelligence Reform and Terrorism Prevention Act of 2004 directly affects the intelligence community and the intelligence and intelligence-related activities of the United States government, and for other purposes. This balance between protecting assets and releasing declassified information can be traced back to legislation enacted during the Constitutional Convention in 1787 when rules were adopted ensuring secrecy. All attendees had to sign a secrecy agreement before attending the convention, thus classifying convention proceedings. In 1820, statutes were enacted to remove those restrictions and simultaneously provide for the publication and distribution of convention records, declassifying the information. This is just one of many examples of the fine line between making information available to the people and securing information for the protection of national security. Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html for more information about the Legislative Branch.

Judicial Branch

The Judicial Branch of the Federal Government affects security programs through deciding legal challenges that come before the courts.

Examples of legal decisions affecting national security programs include:

- **Samuel Loring Morison case**
- **Drug testing**
- **Personnel security clearance limitations**

- **SF 312**

Read each example to learn more about these decisions. Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to learn more about the Judicial Branch.

Samuel Loring Morison Case

The Samuel Loring Morison case had an impact on our security program through legal challenges and decisions.

Morison was a Navy intelligence analyst with Top Secret clearance. He took three Secret satellite photographs from a co-worker's desk, cut off the classified control markings on the photos, and mailed them to *Jane's Defence Weekly*, the publication where he was a part-time contributor and editor.

Morison's outside activities presented a conflict of interest with his Navy intelligence job. The courts interpreted that the existing regulations at the time did not control conflict of interest. This case resulted in setting security clearance regulations, and "Outside Activities" was added to the Adjudicative Guidelines that are used to determine eligibility for security clearances.

Drug Testing

The Supreme Court has upheld decisions involving drug testing. In 1986, President Ronald Reagan signed Executive Order 12564, requiring Federal employees to be drug free on and off the job.

Four years later, the U.S. Supreme Court upheld Executive Order 12564 in the case of the *National Treasury Employees Union v. Von Raab*. In this decision, the Supreme Court agreed that employee drug testing does not violate the Constitution's Fourth Amendment protections against unreasonable searches.

Personnel Security Clearance Limitations

Personnel Security Clearance Limitations apply to any covered person. The term "covered person" means:

- **An officer or employee of a Federal agency**
- **A member of the Army, Navy, Air Force, or Marine Corps who is on active duty or is in an active status**
- **An officer or employee of a contractor of a Federal agency**

Absent an express written waiver, the head of a Federal agency may not grant or renew security clearance eligibility for a covered person who meets any of the following conditions:

- **Has been convicted in any court of the United States of a crime, was sentenced to imprisonment for a term exceeding one year, and was incarcerated as a result of that sentence for not less than one year**
- **Has been discharged or dismissed from the Armed Forces under dishonorable conditions**
- **Is mentally incompetent, as determined by an adjudicating authority, based on an evaluation by a duly qualified mental health professional employed by, or acceptable to and approved by, the United States Government and in accordance with the Adjudicative Guidelines required by subsection (d)**

Meritorious Waiver may be awarded if:

- **Consistent with mitigating conditions of Adjudicative Guidelines (Dec. 05)**
- **Conviction and incarceration for not less than one year**
- **Discharged or dismissed from the Armed Forces under dishonorable conditions**
- **Determined mentally incompetent**

Meritorious Waiver may not be awarded to an unlawful user of a controlled substance or a current addict.

SF 312

When Federal employees or contractors are granted security clearance for access to classified information, they must first sign Standard Form 312 (SF 312), a Nondisclosure Agreement required under Executive Order 13526.

The SF 312 form is issued by the ISOO and titled Classified Information Nondisclosure Agreement. It prohibits repeating or confirming classified information to unauthorized individuals, even if the information has already been leaked.

Narration Script: Security programs are affected by legal challenges and decisions made in the judicial court system. One example of legislation dealing with information security is the Morison case. Samuel Loring Morison leaked Secret information to a weekly publication. Because Morison worked as a Navy analyst in the government sector and an editor for a publication in the private sector, legislation was passed regarding the examination of conflicts of interest when authorizing security clearance. Other examples showing how the court system has affected our security programs through legal challenges and decisions are drug testing, personnel security clearance limitations, and, of course, Standard Form 312—the Classified Information Nondisclosure Agreement. Read each example to learn more. Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to learn more about the Judicial Branch.

Knowledge check

Matching—match each item on the left with the selection you choose from the list on the right.

Match the branch of the Federal Government with the best description or example. You may use each branch more than once.

Executive Branch	**This branch created a security program for the atomic energy program.**
Executive Branch	**This branch affected security programs by passing the FOIA.**
Legislative Branch	**Through the Morison episode, this branch gave rise to security clearance regulations.**
Legislative Branch	**As part of this branch, the USD(I) implements security policy in DoD.**
Judicial Branch	**This branch executes the nation's security policies and procedures.**

The correct matches are as follows:

Executive Branch	**This branch executes the nation's security policies and procedures.**
Executive Branch	**As part of this branch, the USD(I) implements security policy in DoD.**
Legislative Branch	**This branch affected security programs by passing the FOIA.**
Legislative Branch	**This branch created a security program for the atomic energy program.**
Judicial Branch	**Through the Morison episode, this branch gave rise to security clearance regulations.**

Topic summary

In summary, each branch of the Federal Government is responsible on some level for the development and implementation of U.S. security programs.

Executive Branch—Implements national security policy and procedures through:

- **Executive Orders**
- **Presidential Directives**

Legislative Branch—Passes laws that establish security programs

Judicial Branch—Affects security programs through deciding legal challenges that come before the courts

Narration Script: You've now completed the Branches of Government topic. In this topic, you learned about the role of the three branches of the Federal Government pertaining to national security. The Executive Branch is responsible for issuing Executive Orders reflecting the current administration's policies on security. The President makes informed security decisions based on input from a number of departments and organizations providing advice about such matters. The Legislative Branch passes the laws that establish our national security programs. The Judicial Branch interprets legal issues as they pertain to national security in accordance with the Constitution. Grievances heard and rulings issued support the nation's security programs while upholding justice. In the next topic, we'll take an in-depth look at Executive Orders. Let's dive right in.

Lesson 1: Role of the Federal Government
Topic 5: Executive Orders

Topic introduction

Ultimately, implementing the nation's security policies and procedures is the responsibility of the President.

Security policies are directed by the President through the issuance of:
- *Executive Orders*
- *Presidential Directives*—**developed by the** *National Security Council* **(NSC) when they concern national security**

These orders and directives provide the formal means to prescribe the conduct of business in the *Executive Branch.*

After completing this lesson, you will be able to:
- **Identify the purpose and characteristics of Executive Orders and Presidential Directives**
- **Identify current Executive Orders and Presidential Directives relevant to security policies**

Narration Script: Within the Executive Branch, the President is responsible for the nation's security policies and procedures. Security policies are directed by the President through the issuance of Executive Orders and various other Presidential Directives developed by the National Security Council. Executive Orders and Presidential Directives are the formal means the President uses to prescribe the conduct of business in the Executive Branch. Take a minute and review the lesson objectives on the screen before continuing with this topic.

Executive order characteristics

Executive Orders:
- **Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government**
- **The President uses Executive Orders to stipulate how the business of the Executive Branch is accomplished**

Changes in administrations may affect how business is conducted, potentially resulting in the issuance of new or amended Executive Orders.

Executive Orders also echo the administration's reaction to its environment:
- **Political philosophies**
- **World events**
- **Judicial actions**
- **Congressional actions**

Narration Script: Executive Orders are official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government. The President uses Executive

Orders to stipulate how the business of the Executive Branch is accomplished. Logically, with each change in administration, the way the government conducts business may also change. This has the potential to directly affect the Executive Orders resulting in the issuance of a new Executive Order or amendments to existing Executive Orders. Executive Orders also echo an administration's reaction to its environment. Political philosophies, world events, and judicial and congressional actions influence Executive Orders, potentially affecting the management and implementation of security programs across the Executive Branch.

Current Executive Orders affecting security policy

Key Executive Orders related to our national security:

- **Executive Order 10450, Security Requirements for Government Employment**
- **Executive Order 11935, Citizenship Requirements for Federal Employment**
- **Executive Order 12333, United States Intelligence Activities**
- **Executive Order 12829, National Industrial Security Program**
- **Executive Order 12968, Access to Classified National Security Information**
- **Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to National Security Information**
- **Executive Order 13526, Classified National Security Information**

Read each Executive Order for a brief description. Visit the resource links for job aids that summarize all of these Executive Orders.

Executive Order 10450

This order specifies responsibility of government departments and agencies to establish and maintain programs to ensure that their employment of civilian officers or employees is consistent with national security interests. It also lays out information about the scope of investigations, actions to take when employment is not consistent with national security interests, the purpose of investigations, and other provisions.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 11935

This E.O. stipulates that U.S. citizenship is required for permanent employment in competitive civil service positions.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 12333

This E.O. emphasizes that timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to U.S. national security. It establishes the goals, duties, and responsibilities to provide for effective conduct of U.S. intelligence activities and protection of constitutional rights.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 12829
E.O. 12829 establishes a National Industrial Security Program (NISP) aimed at safeguarding Federal Government classified information that is released to U.S. government contractors, licensees, and grantees.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 12968
This order establishes a uniform Federal Personnel Security Program for employees who will be considered for initial or continued access to classified information. It includes definitions as well as information regarding access to classified information and financial disclosure.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 13467
This E.O. establishes the policy, applicability, and definitions required to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability of a person to hold a sensitive position. It stipulates contractor employee fitness and eligibility for access to classified information.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Executive Order 13526
This E.O. substantially advances the goal for reforming the security classification and declassification process. It offers greater openness and transparency in the Government's legitimate interests. It further promotes new techniques to support declassification.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view this Executive Order in its entirety.

Narration Script: Although Executive Orders have been used since President George Washington, President Franklin Delano Roosevelt signed the first Executive Order to be published in the Federal Register as an Executive Order—Executive Order 8381—on March 22, 1940. This Executive Order formalized and provided a basis for existing classification systems then in use by the Army and Navy. Since then, Executive Orders have been added to and subtracted from, depending on the political context of the time. Executive Orders apply to all personnel within the Executive Branch. They are written in general terms, and each department, agency, or organization charged with implementation will need to specify implementation directives according to its missions and functions. Within the DoD for security policy, the Under Secretary of Defense for Intelligence, or USDI, will issue or update documents. The military components and other organizations will in turn issue or update documents at their respective levels. Read each bullet for a summary. Inside each area, you will see a link enabling you to view the Executive Order in its entirety. You should look at several of them and examine

the way they are written, what areas of the Executive Branch they apply to, and how they are to be implemented.

Presidential Directives

Presidential Directives affecting security policies and procedures within the Executive Branch are:

- **National Security Decision Directive (NSDD) 84—Safeguarding National Security Information (Investigating Leaks of Classified Information)**
- **NSDD 298—National OPSEC Program (http://www.cdse.edu/catalog/elearning/GS140-resources.html)**
- **NSDD 145—National Policy on Telecommunications and Automated Information Systems Security (Telecommunications and Computer Security)**
- **Homeland Security Presidential Directive (HSPD) 12—Policies for a Common Identification Standard for Federal Employees and Contractors (http://www.cdse.edu/catalog/elearning/GS140-resources.html)**

Click the links in parentheses to view these Presidential Directives to view it in their entirety. Please note that NSDD 84 and NSDD 145 are not available online at this time.

Narration Script: In addition to Executive Orders, Presidential Directives are decision-based directives, issued by a President and based on facts gathered by the NSC, the views of appropriate government agencies, analyses, and alternative choices. These Presidential Directives have the same substantive legal effect as Executive Orders and remain effective upon changes in administration, unless otherwise specified. You can view these Directives by clicking the corresponding link.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

Do you think you have a lock on what Executive Orders and Presidential Directives are?

Choose TWO correct statements about Executive Orders and Presidential Directives.

- ❑ **The President may issue Executive Orders and Presidential Directives.**
- ❑ **Executive Orders related to national security are developed by the NSC.**
- ❑ **Congress issues Directives related to national security.**
- ❑ **Executive Orders are developed by the Congress and signed by the President.**
- ❑ **The Department of Homeland Security develops the Presidential Directives.**

The correct answers are:
The President may issue Executive Orders and Presidential Directives.
Executive Orders related to national security are developed by the NSC.

Topic summary

In summary, Executive Orders and Presidential Directives are:

- **Used by the President to issue instructions to all personnel in the Executive Branch**

- **Directly affected by the presiding administration, world events, and the political philosophies of the time**

The next lesson:
- **Introduces the four security disciplines**
- **Special types of information**
- **Instructions, directives, and regulations that affect security programs**

Narration Script: In summary, the most important piece of information to take away from this topic is that Executive Orders and Presidential Directives are used by the President to inform all personnel within the Executive Branch about how business will be conducted. These orders and directives help to safeguard our country. In order to protect our national security, Executive Orders and Presidential Directives can change with administrations, world events, and political philosophies. In the next lesson, we will investigate the topics shown here.

Lesson 1: DoD Security Responsibilities
Topic 6: DoD Security Disciplines and Roles

Topic introduction

Why security programs are a must:
- **Increased frequency and magnitude of terrorist threats**
- **Proliferation of technologically savvy individuals with criminal intent**
- **Known and developing factors that threaten our national assets**

The *Department of Defense* **(DoD):**
- **Is a component of the** *Executive Branch* **of the Federal Government**
- **Is a target of threats to security**
- **Plays a critical and central role in safeguarding** *national security*

Keep reading for descriptions of DoD security activities.

DoD Security Activities

DoD security activities include:
- **Measures taken by a DoD unit, activity, or installation to protect itself against all acts designed to, or that may, impair its effectiveness**
- **Conditions resulting from the establishment and maintenance of protective measures that ensure a state of inviolability from adversarial acts or influences**
- **With respect to classified matter, conditions preventing unauthorized persons from having access to official information that is safeguarded in the interests of national security**

Narration Script: Today, more than ever, the need for security is a must at all levels of the government, including the Executive Branch and within the Department of Defense, or DoD. The increased frequency and magnitude of terrorist threats, the proliferation of technologically savvy individuals with criminal intent, and other developing factors that threaten our national assets make security programs a must. The DoD, as a component of the Executive Branch of the Federal Government, is often a target of threats to security and plays a critical role in safeguarding national security against these threats. Before we move ahead in this topic, read the descriptions of DoD security activities.

Topic objective

In this topic, you will explore the four core security disciplines and how they are implemented within DoD's security programs.

The four core security disciplines are:
- **Information**
- **Physical**
- **Industrial**
- **Personnel**

Read about each security discipline to examine its roles and responsibilities.

Narration Script: This topic examines the roles and responsibilities of four core national security disciplines and how they are implemented within DoD security programs. These four security disciplines are information security, physical security, industrial security, and personnel security.

Information security

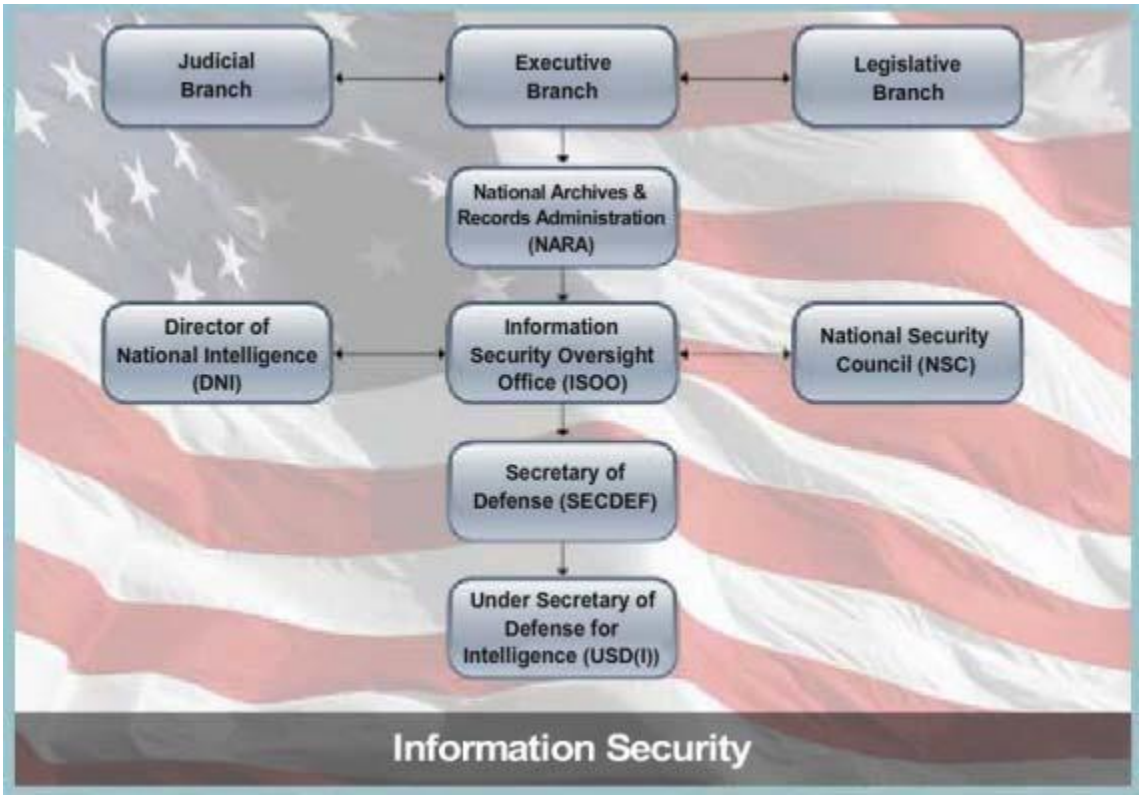
The purpose of the *Information Security Program* **is to:**

- **Promote the proper and effective way to classify, safeguard, protect, and downgrade classified information requiring protection in the interest of national security**
- **Promote the declassification of information no longer requiring such protection**
- **Promote uniformity in the handling of classified information:**
    - **Classifying**
    - **Safeguarding**
    - **Downgrading**
    - **Declassifying**

Protection:

- **Collateral**
- **Sensitive Compartmented Information (SCI)**
- **Special Access Programs (SAPs)**
- **Controlled Unclassified Information (CUI)**

Review the flowchart for the sequence of information security policy and program implementation.



Narration Script: The government of the United States owns or controls information that must be protected from unauthorized distribution. This information may be vital to protecting our national assets and interests, or it may be information the government is morally and legally bound to protect from unauthorized disclosure. In order to accomplish this, it's vital for our national security to have a uniform program providing direction and management for classifying, safeguarding, downgrading, and declassifying information. In addition to determining the policies and guidance, the program must also oversee the application of that guidance. The DoD Information Security Program established the protection for collateral; Sensitive Compartmented Information, or SCI; Special Access Programs, or SAP; and Controlled Unclassified Information, or CUI. The flowchart shows the sequence for developing and implementing information security policy and programs from the President through implementation in the Department of Defense. The President authors the Executive Order with the input of the National Security Council, or NSC. The signed Executive Order is passed through the National Security Council to the Information Security Oversight Office, or ISOO, which issues ISOO Directive no. 1. This implements the Order to all the executive agencies, including the DoD. Note that the ISOO is under the National Archives and Records Administration (or NARA) administratively and the NSC operationally.

Information security (continued)

Under Secretary of Defense for Intelligence [USD(I)]:

- **Appointed by the Secretary of Defense (SECDEF)**
- **Primary official responsible for issuing guidance for the information security program in DoD**
- **Issues DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information**
- **Issues DoDM 5200.01, DoD Information Security Program**

Sources and authorities regarding the Information Security Program:

- **USD(I)**
- **DoDI 5200.01 and DoDM 5200.01**
- **DoD components**
- **Component senior agency officials**
- **Security managers**

Read about each item in the list for more information.

USD(I)

The USD(I) is the primary office responsible for implementing DoD Information Security Program policies and procedures. Some information security responsibilities are shared with the Under Secretary of Defense for Policy [USD(P)].

The USD(I) forwards information security program policy through issuance of the DoDI 5200.01 and the DoDM 5200.01 to all of the DoD components and agencies. DoDI 5200.01 and DoDM 5200.01.

DoDI 5200.01 establishes the basic information security policies for the DoD and further authorizes the publication of DoDM 5200.01.

DoDM 5200.01 establishes the information security baseline requirements for all of DoD. It provides guidance and direction on classification management for both original and derivative classification. It also provides marking, protection, and handling requirements for classified information and CUI.

DoDI 5200.01 also authorizes the publication of DoDM 5105.21, Volumes 1–3, Sensitive Compartmented Information (SCI) Administrative Security Manual. The DoDM 5105.21 will not be discussed in this course.

You can access these documents at the following link: http://www.cdse.edu/catalog/elearning/GS140-resources.html

DoD Components

The DoD components include the:

- **Office of the Secretary of Defense (OSD)**
- **Military Departments (Army, Navy, Air Force)**
- **Chairman of the Joint Chiefs of Staff**
- **Combatant Commands**
- **Defense Agencies**

Each of these components adds its own requirements to the DoD standards to ensure security measures are effective for each unique mission and function.

These DoD components monitor the information security programs within their organizations and designate a senior agency official to oversee each program.

Component Senior Agency Officials

The individual DoD components designate a senior agency official to be responsible for monitoring and reporting on the status of the information security programs at all levels under them. Some agencies apply standards more stringent than the ones required in the DoDM 5200.01.

Security Managers

Security managers are responsible for the administration of effective information security programs within the component. Some of the important information security functions security managers deal with include:

- **Security education and training**
- **Assignment of proper classifications**
- **Downgrading and declassification**
- **Safeguarding**
- **Program monitoring**

Narration Script: Appointed by the Secretary of Defense, the USD(I) has the primary responsibility for providing guidance, oversight, and approval authority governing information security. The USD(I) is the governing authority for issuance of DoD Instruction 5200.01. Guidance is disseminated throughout the DoD components and agencies. From the components to the senior agency officials, and then from the senior agency officials to the security managers, the Information Security Program permeates the entire Department of Defense. These agencies, officials, and security managers and security officers have their own responsibilities to implement, uphold, and manage the Information Security Program. Now, read about each fact for more information.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

Let's see what you remember about the DoD Information Security Program.

Choose THREE correct statements about information security.

- ❑ **The Information Security Program's purpose is to properly classify, protect, declassify, or downgrade official information and safeguard classified information.**
- ❑ **The Information Security Program promotes the declassification of information no longer requiring protection.**
- ❑ **DoDI 5200.01 provides guidance for Information Security Program implementation within DoD.**
- ❑ **The Information Security Oversight Office (ISOO) issues information security Executive Orders to DoD.**
- ❑ **The national Information Security Program is headed by a security manager.**
- ❑ **Federal intelligence agencies created the Information Security Program.**

The correct answers are:

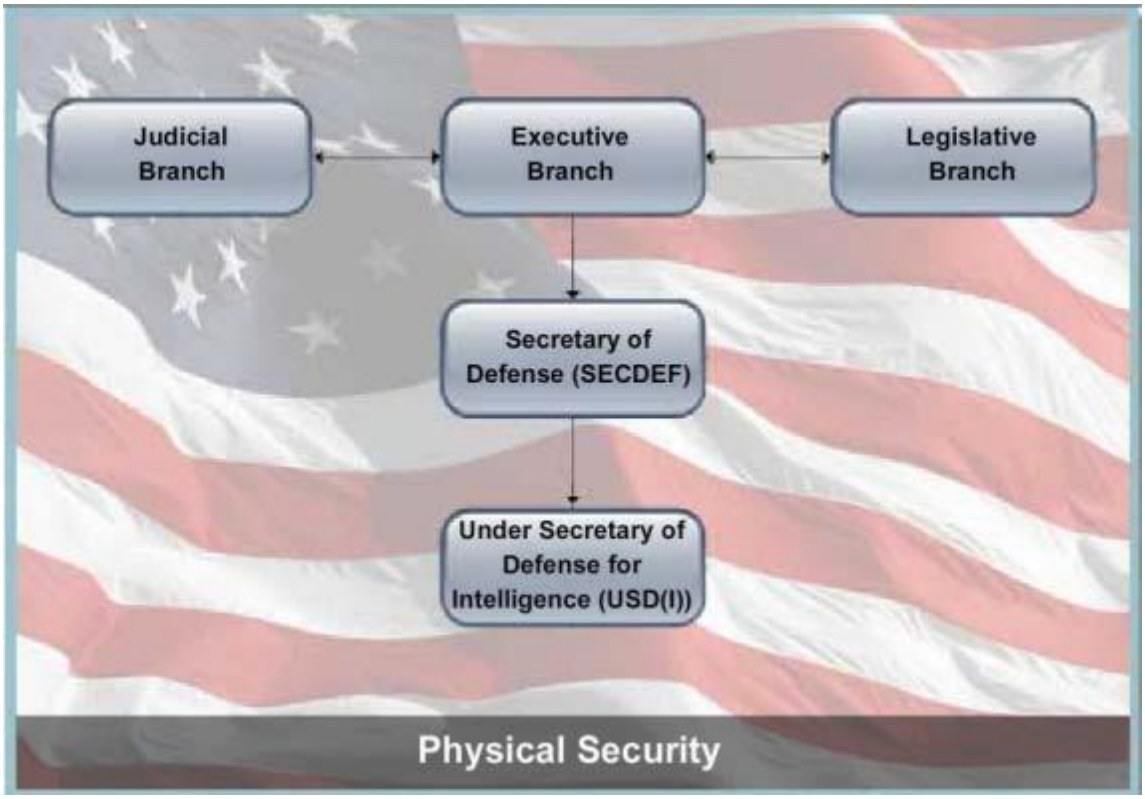
The Information Security Program's purpose is to properly classify, protect, declassify, or downgrade official information and safeguard classified information.
The Information Security Program promotes the declassification of information no longer requiring protection.
DoDI 5200.01 provides guidance for Information Security Program implementation within DoD.

Physical security

The two primary purposes of the *Physical Security Program* **are prevention and protection designed to:**

- **Safeguard personnel**
- **Prevent unauthorized access to equipment, installations, material, and documents**

Review the flowchart shown here to see the chain of command for national physical security programs, beginning with the President and other elements of the Executive Branch.



Narration Script: The two primary purposes of the national Physical Security Program are prevention and protection designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and to safeguard these assets against espionage, sabotage, damage, and theft. Properly designed and executed physical security programs should deter or prevent the loss, theft, or damage of assets, including people, information, equipment, facilities, activities, and operations. The flowchart here shows that the physical security program begins at the Executive Branch with the President and continues through the chain of command through the OSD and the USD(I).

Instruction and Regulation 5200.08

The commanders must ensure that appropriate measures are taken to minimize loss, theft, or damage to the assets they are responsible for protecting.

DoD Instruction 5200.08 and DoD 5200.08-R:

- **Implement policies and minimum standards for physical security to protect DoD personnel, installations, operations, and related resources**
- **Authorize installation commanders and facility directors to issue regulations for the protection and security of property or places under their command**
- **Authorize commanders to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property**

Narration Script: Commanders must ensure appropriate measures are taken to minimize loss. Deterrents such as fences, signs, dogs, and guards typically provide sufficient protection against general criminal activity, but deterring enemy force, terrorist, or insider threat activity may require more extensive countermeasures. DoD Instruction 5200.08 and DoD 5200.08-R implement policies and minimum standards for physical security to protect DoD personnel, installations, operations, and related resources. These documents authorize installation commanders and facility directors to issue policies for the protection and security of property or places under their command and to take reasonably necessary and lawful measures to maintain law and order and protect installation personnel and property.

Instruction and Regulation 5200.08 (continued)

Other DoD personnel responsible for the physical security of assets include:

- **Installation commanders/facility directors**
- **Antiterrorism officers (ATOs)**
- **Local, state, and Federal law enforcement officials**
- **Operations Security (OPSEC) Officers**
- **Physical Security Officers/Provost Marshals**

Read about each category of personnel for information on that position's physical security responsibilities.

Installation Commanders/Facility Directors

Under DoD Instruction 5200.08, commanders or directors serving in management or leadership positions are responsible for:

- **Safety and protection of the people and property under their command**
- **Planning, forming, coordinating, and integrating all physical security matters in their installation**
- **Identification of mission-essential capabilities**

Antiterrorism Officers (ATOs)

The ATO supports the physical security mission by managing the installation or facility antiterrorism program—a program using defensive measures to reduce the vulnerability of individuals and property

from terrorist attacks.

Local, State, and Federal Law Enforcement Officials

Effective liaison with local, state, and Federal law enforcement officials fosters cooperative working relationships that help coordinate handling of antiterrorism concerns and goals, emergency responses, and criminal incidents. Coordination activities support mutual understanding of jurisdiction and authority.

Operations Security (OPSEC) Officers

OPSEC Officers facilitate:

- **Identifying critical information**
- **Identifying threats to specific assets**
- **Assessing asset vulnerabilities**
- **Analyzing risk to specific assets and to national security as a whole**
- **Developing countermeasures against potential threats to national security and other DoD assets**

Physical Security Officers/Provost Marshals

The Physical Security Officer or the Provost Marshal is responsible for managing, implementing, and directing physical security programs. This person may also be responsible for developing and maintaining physical security plans, instructions, regulations, and standard policies and procedures.

Additional responsibilities include coordinating with local law enforcement agencies, antiterrorism officers, and loss prevention personnel.

Narration Script: Other personnel actively involved with physical security at DoD facilities include installation commanders and facility directors; antiterrorism officers; local, state, and Federal law enforcement officials; OPSEC officers, and Physical Security Officers and Provost Marshals. Read about each category of personnel for information on that position's physical security responsibilities.

Knowledge check

Matching—match each item on the left with the selection you choose from the list on the right.

What have you discovered about DoD's physical security program? Match

DoD physical security personnel with their area of responsibility. Facility

directors	**Maintenance of physical security plans and instructions**
ATOs	**Development of countermeasures against potential threats**
OPSEC officers	**Defensive measures to reduce vulnerability from terrorist attack**
Provost marshals	**Safety of people and property under their command**

The correct answers are:

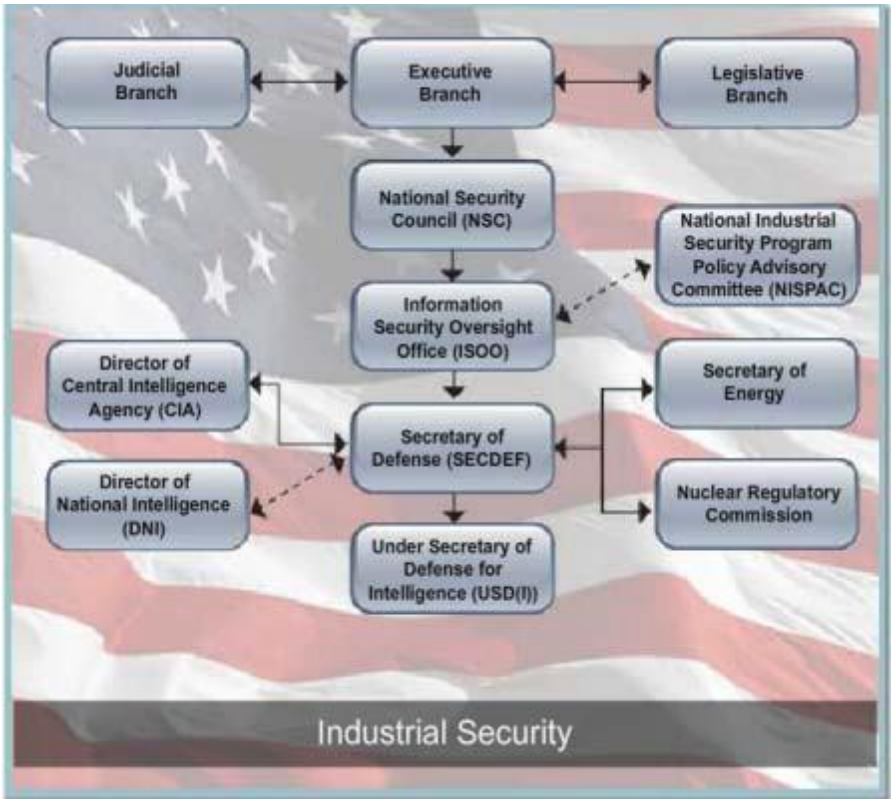
Facility directors	**Safety of people and property under their command**
ATOs	**Defensive measures to reduce vulnerability from terrorist attack**
OPSEC officers	**Development of countermeasures against potential threats**
Provost marshals	**Maintenance of physical security plans and instructions**

Industrial security

The *National Industrial Security Program* **(NISP):**

- **Was established by** *Executive Order* **12829 for the protection of information classified under Executive Order 13526, or its successor or predecessor orders, and the** *Atomic Energy Act of 1954***, as Amended**
- **Safeguards classified information in the hands of U.S. industrial organizations, educational institutions, and all organizations and facilities used as prime and subcontractors**

Review the flowchart to see the chain of command for NISP, starting with the President and moving on down to the USD(I).



Narration Script: The National Industrial Security Program—also called NISP—was established by Executive Order 12829. It establishes standards for contractors who have access to classified information, facilities, information systems, and equipment. The NISP defines the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information by these contractors. If contractors deal with unclassified but sensitive material, their contract may include additional guidance on what safeguards are required to protect that information. Contractors are also obligated to protect certain unclassified information in accordance with export regulations found in the International Traffic in Arms Regulations (or ITAR) and the

Export Administration Regulations (or EAR). Review the flowchart to see the chain of command for NISP.

Industrial security documents

Documents providing guidelines and authorities for DoD's implementation of the NISP are:

- **DoD Directive 5220.22**
- **DoD 5220.22-R**
- **DoD 5220.22-M**
- **Industrial Security Letters**

Read about each document for more information.

DoD Directive 5220.22

DoD Directive 5220.22 assigns overall responsibility for policy and administration of NISP to ensure that classified information released to industry is properly safeguarded.

In accordance with Executive Order 12829, the directive, titled National Industrial Security Program, authorizes the publication of DoD 5220.22-R, DoD 5220.22-M, and Industrial Security Letters. This directive defines the industrial security program responsibilities of the USD(I), Director of the Defense Security Service (DSS), and the heads of the DoD Components.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to access DoD Directive 5220.22. DoD 5220.22-R

DoD 5220.22-R, Industrial Security Regulation, sets forth policies, practices, and procedures of the DoD implementation of the NISP to ensure the safeguarding of classified information in the hands of U.S. industrial organizations, educational institutions, and all organizations and facilities used as prime contractors and subcontractors.

DoD 5220.22-R, Industrial Security Regulation, applies to the following organizations:

- **OSD (including all boards, councils, staffs, and commands)**
- **DoD Agencies**
- **Departments of the Army, the Navy, and the Air Force (including all of their activities)**

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to access DoD 5220.22-R. DoD 5220.22-M

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), and its supplements prescribe the specific requirements, restrictions, and other safeguards considered necessary in the interest of national security for industry to protect classified information.

Compliance with the NISPOM is incorporated into each contract that requires access to classified information by use of the Security Requirements clause required by Subpart 4.4 of the Federal

Acquisition Regulation and a DoD Security Agreement.

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to access DoD 5220.22-M.

Industrial Security Letters
Industrial Security Letters are issued by the Director of the DSS, with the approval of the USD(I), to provide guidance to contractors in administering their responsibilities under the NISP and to provide other security-related implementation guidelines. Industrial Security Letters provide updates and clarification of information contained in the NISPOM.

Visit https://www.dss.mil/GW/ShowBinary/DSS/isp/industrial_sec.html to access Industrial Security Letters.

Narration Script: Four documents provide the guidelines and prescribe responsibilities relative to DoD's implementation of the National Industrial Security Program (NISP).Visit **https://www.dss.mil/GW/ShowBinary/DSS/isp/industrial_sec.html** to discover more about them.

NISP key roles and responsibilities

Key roles in industrial security under the NISP are:
- **Secretary of Defense**
- **USD(I)**
- **DoD components**
- **Component senior agency officials**
- **Defense Security Service (DSS)**
- **Industrial Security Specialists**
- **Facility Security Officers (FSOs)**

Read about each key role for information about its NISP responsibilities.

Secretary of Defense

The Secretary of Defense serves as executive agent for the NISP. As the Executive Agency, the DoD publishes the NISPOM and coordinates NISP policy with the other Cognizant Security Agencies (CSA).

USD(I)

The Secretary of Defense designates the USD(I) as the primary office responsible for implementing industrial security program policies and procedures. The USD(I) forwards DoD 5220.22-R, Industrial Security Regulation, to all of the DoD components and agencies.

DoD Components

The DoD components include the:
- **OSD**
- **Military Departments (Army, Navy, and Air Force)**
- **Chairman of the Joint Chiefs of Staff**
- **Combatant Commands**
- **Defense Agencies**

DoD components add their own requirements to the DoD standards, ensuring security measures are effective for their unique missions and functions.

The DoD components monitor the industrial security program within their organizations.

Component Senior Agency Officials

The individual DoD components designate a senior agency official to be responsible for monitoring and reporting on the status of the industrial security program at all levels under them. Some agencies apply more stringent standards than the ones included in the DoD 5220.22-R.

Defense Security Service

The DSS serves as the DoD Cognizant Security Office (CSO):
- **Oversees the protection of U.S. and foreign classified information in the hands of industry**
- **Administers the NISP for DoD, to include issuance of security clearances to industry**
- **Supports the Office of Personnel Management (OPM) in the conduct of personnel security investigations for DoD**
- **Provides security education and training in core security disciplines to the DoD and NISP community**
- **Provides information technology services that support the industrial and personnel security missions of DoD and its partner agencies**

In support of its mission, DSS employs:
- **Industrial Security Representatives**
- **Information System Security Professionals**
- **Counterintelligence Specialists**
- **Foreign Ownership Control and Influence (FOCI) Specialists**
- **International Specialists**

Industrial Security Specialists

Some of the important industrial security functions these individuals deal with include:

- **Reviewing classified contracts to identify the level and kind of security work to be performed in the facility**
- **Working with subject-matter specialists in developing statements of need, descriptions of work, and other considerations relating to the security requirements under contractual arrangement**
- **Working with contracting officers to ensure bidders can meet security requirements of the contract**
- **Working with subject-matter specialists and contracting officers to provide classification and security guidance via the DoD Contract Security Classification Specification (DD Form 254)**
- **Conducting continuing inspections of facilities possessing sensitive information to ensure adherence to security requirements**

Facility Security Officers (FSOs)

Each contractor facility must appoint an FSO to supervise and direct security measures necessary for implementing applicable requirements of the NISPOM and related Federal requirements for classified information.

The responsibilities of the FSO include ensuring that security is implemented and maintained in accordance with the contract requirements defined by the government customer.

Narration Script: The National Industrial Security Program identifies officials and activities that have key roles to play. Key roles in the industrial security program are the Secretary of Defense; the Under Secretary of Defense for Intelligence; DoD components such as the branches of the military, combatant commands, the Chairman of the Joint Chiefs of Staff, and other defense agencies; DoD component senior agency officials; the DSS; industrial security specialists; and facility security officers. Take a few minutes to review the descriptions of the roles each plays.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

There's a lot to know about the National Industrial Security Program (NISP). Check out this question to see what you remember.

Choose FOUR correct statements about NISP.

- ❑ **DoD Directive 5220.22 assigns overall responsibility for policy and administration of NISP.**
- ❑ **The NISP objective is to safeguard classified information in the hands of U.S. industry.**
- ❑ **DSS issues security clearances to U.S. industry.**
- ❑ **Industrial contractors must appoint an FSO to supervise and direct security measures.**
- ❑ **DoD Directive 2220.55 assigns overall industry security to DSS.**
- ❑ **The Secretary of the Interior plays a key role in NISP.**
- ❑ **NISP was started in 1945 by the person serving as Secretary of War.**

The correct answers are:
DoD Directive 5220.22 assigns overall responsibility for policy and administration of NISP.
The NISP objective is to safeguard classified information in the hands of U.S. industry.
DSS issues security clearances to U.S. industry.
Industrial contractors must appoint an FSO to supervise and direct security measures.

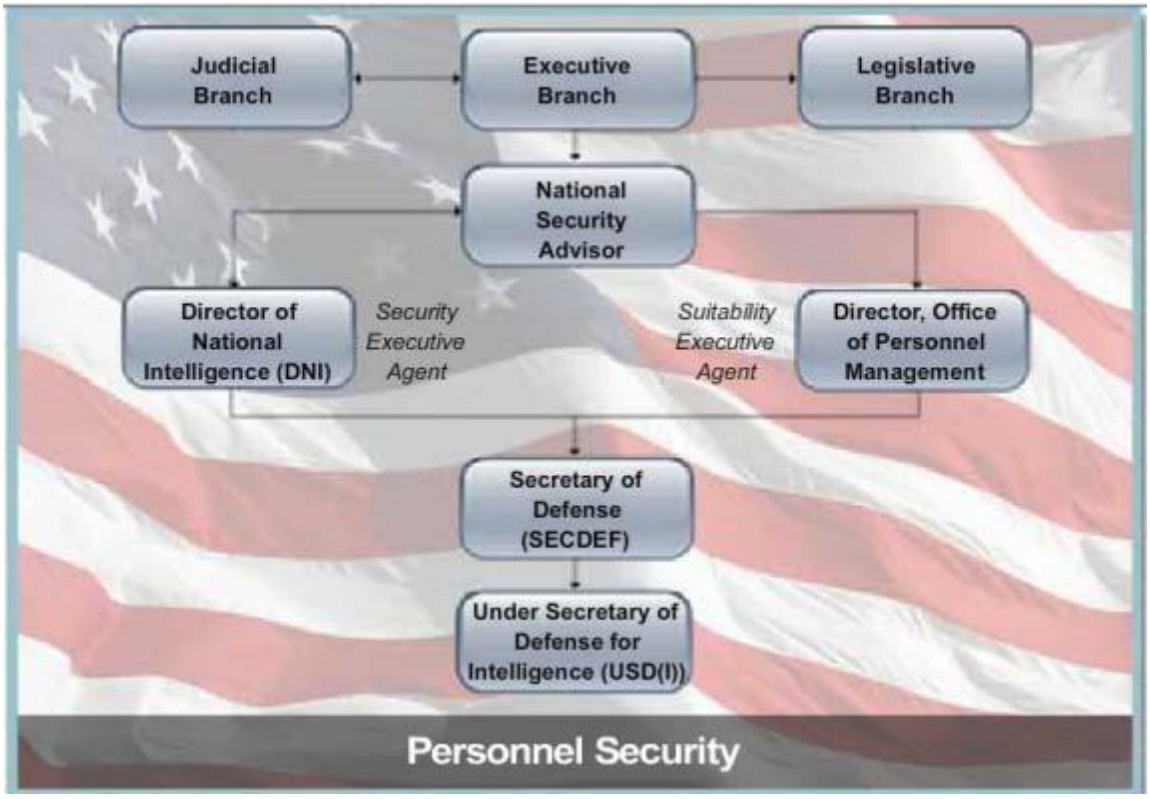
Personnel security

The purpose of the *Personnel Security Program* **is to protect national security by ensuring individuals granted access to classified information or assigned to sensitive duties are loyal, trustworthy, and reliable.**

The DoD Personnel Security Program:

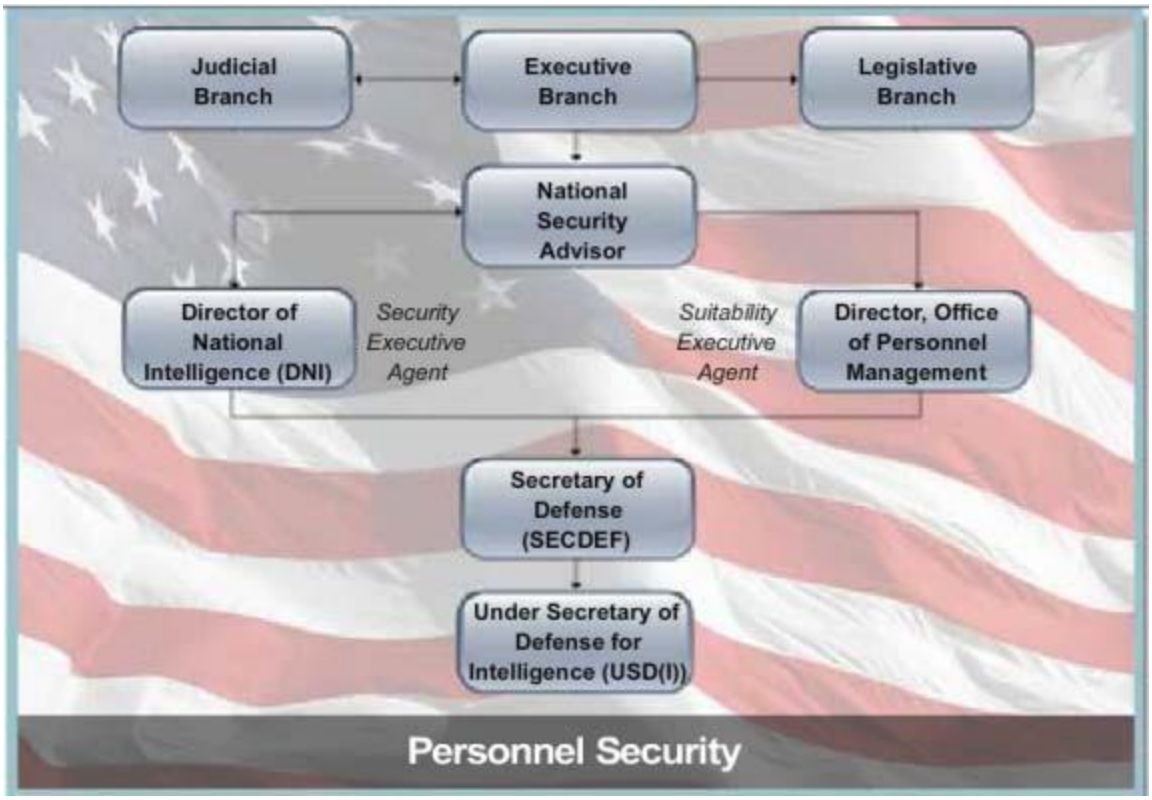
- **Establishes standards, criteria, and guidelines for making personnel security determinations, using a comprehensive background investigative process**
- **Applies its personnel security determinations to members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated individuals requiring access to classified information or assigned sensitive duties.**

Review the flowchart to see the chain of command for the personnel security program, beginning with the Executive Branch on down to the USD(I).



Narration Script: The purpose of the personnel security program is to protect national security by ensuring individuals granted access to classified information or assigned to sensitive duties are loyal, trustworthy, and reliable. Because of the extensive number of DoD personnel and contractors requiring security clearance to

perform their work, the Personnel Security Program is widespread. The DoD personnel security program establishes standards, criteria, and guidelines for basing personnel security determinations and applies these determinations to the Armed Forces, and to DoD civilian employees, contractors, and other affiliated individuals who require access to classified information or who are assigned sensitive duties. The flowchart illustrates the sequence of implementation for the national personnel security program from the Executive Branch to its implementation authority in the DoD.



Directive 5200.02

DoD Directive 5200.02 establishes the basic personnel security policies for the DoD and authorizes the publication of the Personnel Security Program regulation (DoD 5200.2-R).

This regulation:

- **Establishes the DoD personnel security policies and procedures**
- **Sets the standards, criteria, and guidelines upon which personnel security determinations are based**
- **Prescribes the kinds and scope of personnel security investigations required**
- **Details the valuation and adverse action procedures for making personnel security determinations**
- **Assigns overall program management responsibilities**

Narration Script: The DoD personnel security program is authorized by DoD Directive 5200.02 and DoD regulation 5200.2-R. This regulation establishes the policies and procedures for setting personnel security determinations and prescribes the types of security investigations required. The regulation also details the valuation and adverse action procedures for making personnel security determinations and assigns overall program management responsibilities.

Personnel security roles and responsibilities

DoD Regulation 5200.2-R assigns the overall personnel security program management roles:

- **USD(I)**
- **DoD components**
- **Component senior agency officials**
- **Security managers**
- **Personnel security adjudicators**

Read about each role to explore its personnel security responsibilities.

USD(I)

The USD(I) is the primary office responsible for implementing personnel security program policies and procedures.

The USD(I) forwards personnel security program regulation DoD 5200.2-R to all of the DoD components and agencies.

DoD Components

The DoD components include the:

- **OSD**
- **Military Departments (Army, Navy, and Air Force)**
- **Chairman of the Joint Chiefs of Staff**
- **Combatant Commands**
- **Defense Agencies**

DoD components add their own requirements to the DoD standards, ensuring security measures are effective for their unique missions and functions.

The DoD components monitor the personnel security program within their organizations.

Component Senior Agency Officials

The individual DoD components designate a senior agency official to be responsible for monitoring and reporting on the status of the personnel security program at all levels under them. Some agencies apply more stringent standards than the ones included in the DoD 5200.2-R.

Security Managers

Within the DoD components and agencies, the head of each component appoints an official to serve as its security manager. This person is responsible for the administration of effective personnel security programs within the department. Some of the important personnel security functions security managers deal with include:

- **Identifying and requesting personnel security investigations and security clearance eligibilities**
- **Managing the continuous evaluation program, including security education and training and evaluating continued access to classified information and sensitive duties**
- **Maintaining access in personnel security databases**

Personnel Security Adjudicators

The Department of Defense Consolidated Adjudications Facility (DoD CAF) handles adjudications functions only while ensuring uniform application of the requirements of DoD 5200.2-R.

Personnel security adjudicators administer the functions of this facility. Some of the important responsibilities of a personnel security adjudicator include:
- **Determining security clearance eligibility for access to classified information or assignment to sensitive positions**
- **Making unfavorable administrative determinations**
- **Maintaining security clearance determinations in personnel security databases**

Narration Script: DoD Regulation 5200.2-R also assigns the overall personnel security program management roles. These roles are the Under Secretary of Defense for Intelligence; the DoD components, including the Office of the Secretary of Defense, the departments of the Army, Navy, and Air Force; the Chairman of the Joint Chiefs of Staff; the combatant commands and other defense agencies; the component senior agency officials; security managers; and personnel security adjudicators. Read about each role to explore its personnel security responsibilities.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

Let's see what you remember about DoD's personnel security program.

Choose FOUR correct statements about the personnel security program.

- ❑ **Provides guidelines and criteria for personnel security determinations**
- ❑ **Is authorized by DoD Directive 5200.02**
- ❑ **Prescribes the roles and responsibilities for managing personnel security**
- ❑ **Authorizes personnel security adjudicators**
- ❑ **Is overseen by the Senate Subcommittee on Personnel Security**
- ❑ **Releases personnel security information to credit reporting bureaus**
- ❑ **Is authorized only for personnel serving in the Armed Forces**

The correct answers are:
Provides guidelines and criteria for personnel security determinations
Is authorized by DoD Directive 5200.02
Prescribes the roles and responsibilities for managing personnel security

Authorizes personnel security adjudicators

Counterintelligence support

There's one more functional area that is vital to supporting all areas of security—Counterintelligence (CI) Support.

This program is responsible for providing information about the capabilities, intentions, and threats of our adversaries. CI personnel must pay particularly close attention to those adversaries associated with foreign intelligence services.

CI is integrated into DoD security programs.

Narration Script: There's one more functional area that needs to be mentioned—Counterintelligence Support, or CI. CI works across all of the other functional areas: information security, physical security, industrial security, and personnel security. This program provides information about our adversaries—their capabilities, intentions, and the threats they pose. In particular, CI keeps a close eye on the activities of foreign intelligence services and is integrated into DoD security programs.

Topic summary

In this topic, you examined the four security disciplines and their associated programs, each pertaining to different facets of our nation's security:

- **The information security discipline protects information.**
- **The physical security discipline actively protects and prevents unauthorized access to assets.**
- **The industrial security discipline deals with contractors who have access to classified or sensitive information.**
- **The personnel security discipline establishes procedures for making security clearance determinations.**

Through time and experience, these disciplines have evolved—and continue to evolve—depending upon world events, innovations, and regulations.

In the next topic, we'll examine special categories of information.

Narration Script: In this topic, you've investigated the four main security disciplines: information security, physical security, industrial security, and personnel security. These disciplines and their associated programs, roles, and responsibilities all add up to one thing: continued safety and security of our country's assets. In the next topic, we will examine special categories of information.

Lesson 1: DoD Security Responsibilities
Topic 7: Special Categories

Topic introduction

This topic discusses special categories of classified information.

At the end of this topic, you will be able to identify various types of special categories of information and their:
- **Definitions**
- **Governing policy documents**
- **Purpose**

Narration Script: In this topic, we are going to briefly discuss some common special categories of information for which DoD has special responsibility. The collateral guidance provided in the core security disciplines topic explained the baseline safeguards for these special categories of information. However, because of additional policies, procedures, and laws, these special categories of information require additional or enhanced security practices, procedures, and safeguards. In this topic, we will identify the various types of special information categories and define each special category of information. We will discuss the governing policy documents for each special category of information and the purpose of each special category.

Special categories of classified information

The special categories of classified information are:
- *For Official Use Only* **(FOUO)**
- *Special Access Program* **(SAP) Information**
- *Communications Security* **(COMSEC) Information**
- *Sensitive Compartmented Information (SCI)*
- *TEMPEST*
- **Foreign Government Information**
- **Information subject to the** *Atomic Energy Act of 1954*

Narration Script: The special categories of information are For Official Use Only, or FOUO; Special Access Program, or SAP, information; Communications Security, or COMSEC, information; Sensitive Compartmented Information, or SCI; TEMPEST; Foreign government information; and information subject to the Atomic Energy Act of 1954.

For official use only

The designation For Official Use Only (FOUO) is applied to unclassified information that may be exempt from mandatory release to the public under the *Freedom of Information Act* **(FOIA).**

Two qualifications for FOUO information:
- **Fit one or more of the nine exemption categories**
- **Withholding it serves a valid government purpose**

Now, read about the exemption categories.

Nine FOUO Exemption Categories

The nine exemption categories from DoDM 5200.01-V4, February 24, 2012, Enclosure 3, pp. 11–12, are:

- **Exemption 1. Information that is currently and properly classified.**
- **Exemption 2. Information that pertains solely to the internal rules and practices of the agency, that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission.**
- **Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.**
- **Exemption 4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or protect the Government's interest in compliance with program effectiveness.**
- **Exemption 5. Interagency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision-making process and contain subjective evaluations, opinions, and recommendations. Other common privileges are the attorney-client and attorney work product privileges.**
- **Exemption 6. Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.**
- **Exemption 7. Records or information compiled for law enforcement purposes that:**
    - **(a) Could reasonably be expected to interfere with law enforcement proceedings.**
    - **(b) Would deprive a person of a right to a fair trial or impartial adjudication.**
    - **(c) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others.**
    - **(d) Disclose the identity of a confidential source.**
    - **(e) Disclose investigative techniques and procedures.**
    - **(f) Could reasonably be expected to endanger the life or physical safety of any individual.**
- **Exemption 8. Certain records of agencies responsible for supervision of financial institutions.**
- **Exemption 9. Geological and geophysical information (including maps) concerning wells.**

Narration Script: The designation For Official Use Only (abbreviated as FOUO) is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA is enacted by the Department of Defense under DoD Directive 5400.07, the DoD Freedom of Information Act Program, and DoD 5400.7-R, the DoD Freedom of Information Act Program. FOUO information must meet two qualifications. It must fit one or more of the nine exemption categories, and withholding it must serve a valid government purpose. The DoD Information Security Program: Controlled Unclassified Information (CUI) DoDM 5200.01, Volume 4 Enclosure 3 lists and explains the nine exemption categories. Now read about the nine exemption categories.

More about FOUO

Best practice: Mark FOUO information when documents are drafted

Disseminating FOUO information:

- **May be disseminated as necessary in the conduct of official business:**
  - **Within the DoD components**
  - **Between officials of the DoD components and DoD contractors, consultants, and grantees**
- **May be released to officials in other departments and agencies of the Executive, Legislative, and Judicial Branches in performance of a valid government function**
- **Special restrictions may apply to information covered by the** *Privacy Act*

Narration Script: Whenever possible, information determined to be FOUO status should be marked when the documents are drafted, promoting proper protection of the information. FOUO information may be disseminated as necessary to conduct official business within the DoD components, and between officials of the DoD components and DoD contractors, consultants, and grantees. FOUO information may also be released to officials in other departments and agencies of the Executive, Legislative, and Judicial Branches in performance of a valid government function. Special restrictions may apply to information covered by the Privacy Act. Simply because information is marked FOUO does not mean it automatically qualifies for exemption from release under FOIA. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released to the public. Some types of records (for example, personnel records) are not normally marked FOUO, but they may still qualify to be withheld under the Privacy Act.

Special Access Programs

Special Access Programs (SAPs)

- **Created or continued:**
  - **When vulnerability of, or threat to, specific information to be protected from unauthorized disclosure is exceptional, AND**
  - **Normal criteria for determining access to the assigned level of classification are not sufficient to protect the information from unauthorized disclosure, OR**
  - **Required by statute**

- **Approved:**
  - **Secretary of Defense or**
  - **Deputy Secretary of Defense**

- **SAP Policy and Guidance:**
  - **DoD 5205.07, Special Access Program (SAP) Policy**
  - **DoDI 5205.11, DoD Management, Administration, and Oversight of DoD Special Access Programs (SAPs)**

Continue reading for enhanced security examples.

Enhanced Security

Examples of enhanced security for SAPs include:

- **Use of special terminology, including code words, nicknames, and handling caveats to control information dissemination**
- **Personnel security requirements more stringent than those required for a comparable level of classified information**
- **Specialized Nondisclosure Agreements**

Narration Script: Any DoD program or activity employing enhanced security measures exceeding those normally required for collateral information at the same level of classification shall be established, approved, and managed as a DoD Special Access Program—or SAP. A SAP is established in accordance with DoDM 5200.01, Volumes 1–4, DoD Information Security Program, and may be created or continued when the vulnerability of, or threat to, the specific information to be protected from unauthorized disclosure is exceptional AND when the normal criteria for determining access to the assigned level of classification are not sufficient to protect the information from unauthorized disclosure OR when required by statute. DoD SAPs are approved by the Secretary of Defense or the Deputy Secretary of Defense. DoD SAP policy and implementation guidance are addressed in the DoD Directive 5205.07, Special Access Program Policy, and DoDI 5205.11, DoD Management, Administration, and Oversight of DoD Special Access Programs. DoD has further disseminated SAP guidance in various other manuals. Keep reading for enhanced security examples.

COMSEC

The definition of Communications Security (COMSEC) is:

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications.

COMSEC includes:

- **Cryptosecurity**
- **Emission security**
- **Transmission security**
- **Physical security of COMSEC material and information**

Narration Script: COMSEC stands for Communications Security. COMSEC is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information. The governing policy documents for COMSEC are identified in the National Security Telecommunications and Information Systems Security Instruction, or NSTISSI, 4000 series policies. Examples of COMSEC equipment are Secure Terminal Equipment, or STEs.

SCI

The definition of Sensitive Compartmented Information (SCI) is:

SCI is classified information concerned with or derived from intelligence sources, methods, or

analytical processes.

Handling:

- **Handled within formal access control systems established by the Director of National Intelligence (DNI)**
- **DNI establishes the policies, procedures, and controls for the dissemination and use of intelligence information**

Narration Script: Sensitive Compartmented Information, also known as SCI, is classified information concerned with or derived from intelligence sources, methods, or analytical processes. The Director of National Intelligence issues guidance and establishes formal access policies, procedures, and control systems to handle this information.

International programs

Foreign government and specialized treaty classified information:

- **Refers to information classified by a foreign government**
- **Considered a special category under the DoD Information Security Program**
- **Under Secretary of Defense for Policy (USD[P]) directs, administers, and oversees in coordination with the Under Secretary of Defense for Intelligence (USD[I])**
- **Defined in Executive Order 13526, Classified National Security Information**

Visit http://www.cdse.edu/catalog/elearning/GS140-resources.html to view Executive Order 13526.

Narration Script: The DoD Information Security Program handles foreign government and specialized treaty classified information as a separate and special category for security purposes. Unlike other portions of the DoD information security program, foreign government classified information security (including the North Atlantic Treaty Organization classified information) is directed, administered, and overseen by the Under Secretary of Defense for Policy (USD(P)) in coordination with the USD(I). Foreign Government Information is defined in Executive Order 13526, Classified National Security Information. Foreign government and specialized treaty classified information may require special safeguarding and dissemination controls because of its sensitivity and potential impact on our national security. To view Executive Order 13526, visit http://www.cdse.edu/catalog/elearning/GS140-resources.html

TEMPEST

TEMPEST.

Definition:

Investigation, study, and control of *compromising emanations* ***from telecommunications and information systems equipment.***

Narration Script: TEMPEST refers to the investigation, study, and control of compromising emanations from telecommunications and information systems equipment. Your activity TEMPEST advisor can provide additional guidance on this topic.

Atomic Energy Act information

Atomic Energy Act of 1954, as Amended:

- **Nuclear Weapons-Related Information**
- **Restricted Data and Formerly Restricted Data (RD and FRD)**
- **Managed by the Department of Energy (DoE)**
- **Joint Department of Energy & Department of Defense for FRD**
- **DoD Instruction 5210.02, Access to and Dissemination of Restricted Data and Formerly Restricted Data**

Narration Script: The Atomic Energy Act of 1954, as Amended, defines the protection and classification of Nuclear Weapons-Related Information. This information is defined as Restricted Data and Formerly Restricted Data—or RD and FRD. Because of the extraordinary importance of nuclear information, Congress passed the Atomic Energy Act of 1954, mandating special treatment for nuclear information. RD and FRD are governed by the Atomic Energy Act. The Atomic Energy Act is a statute, or public, law. Because atomic energy information is governed by statute, the requirements for protecting RD and FRD information extend to all U.S. citizens, not just government employees. The Department of Energy manages the government-wide RD and FRD classification and declassification system and has sole purview over any information that falls within the definition of RD. Any RD document that agencies generate must be based on a decision DoE has previously made. In the case of FRD, DoE and the DoD have joint responsibility. DoE and DoD jointly determine the declassification of FRD. All FRD classification decisions by other agencies must be based on a previous decision by DoE and DoD. DoD Instruction 5210.02, Access to and Dissemination of Restricted Data and Formerly Restricted Data, provides DoD policy and procedures governing access to and dissemination of Restricted Data by the Department of Defense. It implements the Atomic Energy Act of 1954, as Amended, and as modified by references to the Energy Reorganization Act of 1974.

Knowledge check 1

Matching—match each item on the left with the selection you choose from the list on the right.

Now take some time to check your knowledge of special types of information categories.

Match the special information type with the BEST definition.

FOUO	**A program created when the threat to or vulnerability of the information involved warrants added protection**
SAP	**Includes cryptosecurity and emission security**
COMSEC	**Applies to unclassified information that may be exempt from mandatory release to the public under FOIA**

The correct matches are as follows:

FOUO	**Applies to unclassified information that may be exempt from mandatory release to the public under FOIA**
SAP	**A program created when the threat to or vulnerability of the information involved warrants added protection**
COMSEC	**Includes cryptosecurity and emission security**

Knowledge check 2

Matching—match each item on the left with the selection you choose from the list on the right.

Here are some more matches to win.

Match the special information type with the BEST definition.

Foreign Government Information	**Applies to information derived from intelligence sources, methods, or analytical processes**
TEMPEST	**Deals with foreign classified information and specialized treaty information**
SCI	**Refers to investigations of compromising emanations**

The correct matches are as follows:

Foreign Government Information	**Deals with foreign classified information and specialized treaty information**
TEMPEST	**Refers to investigations of compromising emanations**
SCI	**Applies to information derived from intelligence sources, methods, or analytical processes**

Topic summary

In summary, special categories of unclassified and classified information include:

- **FOUO**
- **Special Access Program (SAP) Information**
- **Communications Security (COMSEC) Information**
- **Sensitive Compartmented Information (SCI)**
- **TEMPEST**
- **Foreign Government Information**
- **Information Subject to the Atomic Energy Act of 1954, as Amended**

Next topic: DoD Security Instructions, Directives, and Regulations

Narration Script: The public's right to know must be balanced against the need to protect the nation's security. Recognizing this obligation, the DoD attempts to meet these challenges to security by recognizing special categories of unclassified and classified information including FOUO, which protects sensitive, unclassified information; SAPs, which protect the nation's most sensitive assets and must be approved by the Secretary of Defense; COMSEC, which deals with transmission and cryptosecurity; SCI; TEMPEST; foreign government information; and Atomic Energy Act information. In the next topic, you'll have the opportunity to examine security instructions, directives, and regulations.

Lesson 1: DoD Security Responsibilities
Topic 8: DoD Security Instructions, Directives, and Regulations

Topic introduction

Modern Department of Defense (DoD) security policies can be traced to the 1947 *National Security Act* **that created the DoD.**

Since then, security policies have continually evolved in response to world events, political philosophies, administrations, and legislation.

Narration Script: The Department of Defense—or DoD—was established by the 1947 National Security Act. Since then, procedures, policies, and regulations have evolved in response to world events, political philosophies, administration policies, and legislation. From this topic, you'll be able to access actual documents on the Defense Security Service Academy Resource Tools site. If you need to review a document in the future, remember that this site will provide you with a handy reference library right at your keyboard.

Security policies documentation

This topic presents a consolidation of DoD documents providing security guidance for the protection of DoD assets.

Five categories of documentation related to DoD security policies:
- **DoD instructions**
- **DoD directives**
- **DoD regulations**
- **DoD manuals**
- **Information Security Oversight Office**

You can find these documents in Appendixes A through F of this Student Guide.

Narration Script: There are a number of documents that provide guidelines for the protection of DoD assets. Look in the Appendixes to access these documents.

Knowledge check

Multiple choice—check the box of the answer(s) you choose.

Identify the DoD information security guidance described below:

"This policy implements Executive Order 13526 and establishes the DoD Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of national security. It also promotes the declassification of information no longer requiring protection."

- ❑ **DoDM 5200.01**
- ❑ **DoD 5220.22-M**
- ❑ **DoDD 5220.22**
- ❑ **DoDI 5205.11**

The correct answer is DoDM 5200.01.

Topic summary

This topic provided you with the DoD security policies adhering to the regulations and guidelines contained in various documents, including:

- **DoD instructions**
- **DoD directives**
- **DoD regulations**
- **DoD manuals**
- **DoD correspondence**

When needed, these resources are accessible for your review at http://www.cdse.edu/catalog/elearning/GS140-resources.html.

Narration Script: DoD has published a wide variety of documents concerning security policies and programs in order to safeguard national security, respond to changing guidelines and requirements, implement policies published in Executive Orders, and comply with legal requirements for protecting private information and observing the right of the American people for access to information. This topic has introduced just a few of the most important documents that apply to DoD security disciplines. You will have many opportunities to consult these documents as you perform your security duties. You can find these documents in Appendixes A through F of this document.

Course conclusion

You have successfully completed the training portion of this course. You should now be able to:

- **Identify the roles of the three branches of the Federal Government in making or implementing security policies and programs**
- **Identify the Executive Orders and Federal policies applicable to security programs**
- **Identify the two basic policies and the three principles of the DoD security program**
- **Identify the roles of DoD agencies and offices responsible for security policy, direction, and oversight**
- **Define the four security disciplines—Information, Physical, Personnel, and Industrial—and their purpose**

To receive course credit, you MUST take the Security Policies, Principles & Programs examination.

Please use STEPP to register for the online exam.

Narration Script: Congratulations. You have now completed the Security Policies, Principles, and Programs course. You should now be able to identify the roles of the three branches of the Federal Government in making

or implementing security policies and programs; identify the Executive Orders and Federal policies applicable to security programs; identify the two basic policies and the three principles of the DoD security program; identify the roles of DoD agencies and offices responsible for security policy, direction, and oversight; and define the four security disciplines—Information, Physical, Personnel, and Industrial—and their purpose. To receive credit for this course, you must take the Security Policies, Principles, and Programs Examination. Please use STEPP to register for the online exam.

DSSA Security Policies, Principles & Programs Master Glossary

Use this resource to look up definitions of the glossary terms throughout the main document. Glossary terms appear in regular italicized text—for example, *Classified Information.*

Term	Definition
Atomic Energy Act of 1954	The U.S. Federal law creating a security program prescribing the civilian and military uses of nuclear materials and development and regulation of the uses of U.S. nuclear materials and facilities.
Classified Information	Any sensitive information or material that the U.S. government has determined according to Executive Order, statute, or regulation to require protection against unauthorized disclosure to particular classes of people for reasons of national security.
Classified Information Nondisclosure Agreement	Requires every individual who is granted a Top Secret security clearance or access to a specially controlled access category or compartment to conform to the conditions and responsibilities imposed by law or regulation related to such clearance.
Cognizant Security Agencies	Agencies that have been authorized by Executive Order 12829 to establish an industrial security program for the purpose of safeguarding classified information disclosed or released to industry.
Communications Security (COMSEC)	An abbreviated form of COMmunications SECurity, a set of measures to prevent unauthorized users from intercepting a radio message.
Compromising Emanation (CE)	Unintentional intelligence-bearing electrical, mechanical, acoustical, or other signals that if transmitted and subsequently intercepted and analyzed could disclose the information contained in them.
Controlled Unclassified Information	Unclassified information not meeting standards for National Security Classification under Executive Order 13526, but that is pertinent to U.S. national interests, requires protection from unauthorized disclosure, and is subject to limited dissemination.
Department of Defense (DoD)	Created in 1947, the Federal department responsible for safeguarding U.S. national security.
Executive Branch	The branch of Federal Government consisting of the President of the United States, the Vice President, the Cabinet, and other executive departments and agencies.
Executive Order (E.O.)	A formal means through which the President directs U.S. security and prescribes the conduct of business in the Executive Branch.

Term	Definition
For Official Use Only (FOUO)	Applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The Department of Defense (DoD) uses the FOUO designation on unclassified information or material that may not be appropriate for release to the public.
Freedom of Information Act (FOIA)	The FOIA indirectly affects U.S. national security by forcing or preventing the release of certain types of information. Under the FOIA, any person has the right to request access to Federal agency records or information. All U.S. government agencies are required to disclose such records when they receive a written request unless the records are protected from disclosure based on nine exemptions and three exclusions.
Information Security Program	Created by the requirements of an Executive Order, the Information Security Program provides a uniform basis for classifying, safeguarding, and declassifying national security information.
Intelligence Reform and Terrorism Prevention Act of 2004	This act was enacted to reform U.S. government intelligence and related activities.
Judicial Branch	The branch of government that manages the court system and explains, interprets, and applies U.S. laws. Members of the Judicial Branch are appointed by the President and confirmed by the U.S. Senate.
Legislative Branch	Consists of the House of Representatives and the Senate, which make up the U.S. Congress. The U.S. Congress has sole constitutional authority to enact legislation and declare war, possesses the right to confirm or reject Presidential appointments, and conducts miscellaneous investigations.
Military Critical Technologies List (MCTL)	A compendium of technologies deemed by the Department of Defense (DoD) to be critical to the military.
National Defense	The U.S. government's use of military, economic, and political power to protect the nation's people, assets, and interests.
National Industrial Security Program (NISP)	This program, which applies to all Executive Branch departments and agencies, establishes standards and safeguards classified information in possession of government contractors, licensees, or grantees.
National Security	The national defense or foreign relations of the United States.
National Security Act	Enacted in 1947, this act created the U.S. Department of Defense and established procedures, policies, and regulations related to U.S. security.

Term	Definition
National Security Council (NSC)	Established in 1947, the NSC is the principal forum for Presidential consideration of foreign policy issues and national security matters.
Personnel Security Program	Ensures that individuals granted access to classified information or assigned to sensitive duties are loyal, trustworthy, and reliable by establishing the standards, criteria, and guidelines on which personnel security determinations are based.
Physical Security Program	That part of security concerned with active, as well as passive, measures designed to prevent unauthorized access to personnel, equipment, installations, materials, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.
Presidential Directive	A form of Executive Order issued by the U.S. President and based on the advice and consent of the National Security Council.
Privacy Act	U.S. public law enacted in 1974 prescribing how personally identifiable information is collected, maintained, used, and disseminated.
Security-in-Depth	Deploying security resources in layers of increasing intensity.
Security Program	Established standards and consistency in procedures designed to protect a country's people and national security assets.
Sensitive Compartmented Information (SCI)	Classified information that is so sensitive that the measures used to protect it extend beyond those used for Top Secret information.
Special Access Program (SAP)	Any program requiring additional security protection and special handling, reporting, and clearance procedures.
TEMPEST	Investigation, study, and control of compromising emanations from telecommunications and information systems equipment.